Project Summary

Overview

Transportation systems have seen a rapid transformation in recent years, with an explosive infusion of autonomous features driven by the integration of a variety of new sensors, actuators, compute elements, communication protocols, and software. An unfortunate upshot of this trend is the increasing vulnerability of these systems to cyber-attacks. Recent research has demonstrated the feasibility of performing cyber-attacks on vehicular systems with potential for catastrophic impact. However, in spite of such compelling demonstrations, awareness of cybersecurity challenges in vehicular electronics remains limited. Existing curricula across the universities in United States do not provide adequate insight into the spectrum of security threats in transportation, with only glimpses of the issue sprinkled across research seminars. In a recent survey by the world's second-largest reinsurer Munich Re, 55% of the surveyed corporate risk managers named vehicular security as their top concern for autonomous vehicles.

We propose to address this problem by developing an infrastructure for disciplined dissemination of vehicular security concepts. We propose a comprehensive hands-on experimental platform to enable understanding of unique security challenges at vehicular hardware, sensor, compute, network, and full platform levels. The platform will target multi-disciplinary undergraduate students across STEM areas relevant to transportation and will additionally facilitate training of transportation engineers, designers of vehicular electronics, and practitioners in security of hardware and cyber-physical systems. We will conduct design-based research to investigate role of hands-on experiment infrastructure in learning and the discipline-specific challenges for students across subjects to learn vehicular security. The materials will be made accessible to educational institutions in Florida and subsequently across the nation.

Intellectual Merit

The proposed teaching platform will be one of the first comprehensive pedagogical platforms for vehicular security across the nation, covering the roots of security from the hardware, software, and sensor building blocks to platforms. A unique feature is the design of an extensive collection of experiments to provide a unique, hands-on understanding. The experiments will make novel use of a variety of vehicular simulators as well as a virtualized platform environment to facilitate effective comprehension of security challenges in current and emergent autonomous vehicles. Students will be able to exploit the environment to explore different cyber-attacks and design countermeasures, both in a physical lab environment and remotely through the Internet. The approach is targeted towards encouraging students not only to learn known attacks but also come up with novel threats and defenses. The project will contribute to cybersecurity education research, producing knowledge on how to design technological environments for vehicular security, expanding our understanding of specific challenges and difficulties for students across disciplines to learn vehicular security, and enabling exploration of strategies for interdisciplinary learning.

Broader Impacts

This project will have transformative technical and societal impacts through a comprehensive, unfragmented, hierarchical view of transportation security to undergraduate students. Given the criticality of the topic and the dearth of awareness in this area, the curricular materials give students a strong competitive edge in a highly promising, emergent market, and help them assume leadership roles in academia, industry, and public sector. It will also stimulate their interests in security research. The platforms developed will also benefit graduate students performing research in the area as well as K-12 students attending summer camps each year. The online infrastructure will allow multiple institutions to access the unique resources and infrastructure developed for the course. The project will provide a distinct opportunity for exposing minorities and female students to critical, emergent issues in transportation security and stimulating their interest in higher education and research.

Keywords: Cybersecurity Education; Cyber-Physical Systems