Florida Department of Transportation Research

Enhancing Cybersecurity in Public Transportation

December 2019

Project Number
BDV25-977-51

Project Manager
Gabrielle Matthews
FDOT Public Transportation Office

Principal Investigator
Sean Barbeau
Jay Ligatti
University of South Florida

Current Situation

"Hacking" has become a common story. As computers and wireless communications become more central to our daily lives, preventing unauthorized access and the possibility of unauthorized control is a subject of intensive study. In transportation, many technologies are being deployed that require communication among mobile devices, vehicles, and transportation infrastructure. These technologies offer improved services and convenience, but they also create cybersecurity vulnerabilities. Florida agencies of all sizes face challenge as new technologies become more common.

Paying a bus fare with using a phone app requires wireless communication, information exchange, and data storage, all of which present cybersecurity issues.

Research Objectives

University of South Florida researchers developed guidance to identify and mitigate transit cybersecurity liabilities and to facilitate ongoing information exchange among Florida transit agencies, vendors, and cybersecurity researchers.

Project Activities

The intensity of the research into transportation technologies has created a rich research literature. In the first task of the project, the research team reviewed this literature for both equipment and protocols to provide an overview of vulnerabilities and defenses. Both currently deployed technologies and those under consideration for deployment were reviewed.

In the second project task, Florida transit agencies were surveyed to collect information on transportation technology, vulnerabilities, and cybersecurity concerns, covering four areas: current and planned technologies; current deployment of automated or connected vehicles; data management policies and procedures; and issues in cybersecurity and implementing good security. The survey found extensive use of technology; for example, most agencies reported use of onboard WiFi, and many more were using CCTV security cameras and communication systems.

The researchers categorized transportation technologies used by public agencies based on five aspects: extent of deployment in Florida; transportation mode for which the technology if used; what the technology is used for; who owns, controls, or maintains the technology; and liabilities of the technology, including the likelihood and severity of loss of control or data.

The third project task continued the team's outreach efforts by facilitating cybersecurity information exchange among Florida transit agencies, their vendors, and researchers. Ten working group meetings were held for various stakeholders. Two hands-on workshops were also held in which students explored mobile fare payment applications and traffic cabinet technologies. The project also coordinated a conference at which faculty from Florida universities presented and discussed their research relating to cybersecurity in public transportation.

The researchers concluded their report with analysis and recommendations for securing two widely used technologies: mobile fare payment applications and traffic cabinets. They also considered Florida's Rule 14-90, "Equipment and Operational Safety Standards for Bus Transit Systems," and revisions to that rule that promote cybersecurity.

Project Benefits

Advanced technologies promise so many benefits for road users. Preventing misuse of these systems helps assure that they will successfully and safely deliver these benefits.

For more information, please see www.fdot.gov/research/.