National Center for Transit Research
Center for Urban Transportation Research
College of Engineering
University of South Florida

For more information,
contact: Robert L. Bertini, Ph.D.
NICR Director
Email: rbertini@usf.edu

Project: Enhancing Cybersecurity in Public Transportation

Authors: Sean Barbeau, Ph.D.

Summary

As transportation infrastructure continues to expand from isolated nodes to large interconnected networks, cybersecurity is a critical concern for transit agencies. This project aims to improve the cybersecurity of public transportation systems in Florida. More specifically, the objectives of this project are to identify and mitigate transit cybersecurity liabilities and to facilitate ongoing cybersecurity information exchange among Florida transit agencies, their vendors, and cybersecurity researchers. To meet these goals, the research team reviewed the existing literature for known vulnerabilities in transportation technologies, performed a survey of transit agencies in Florida, created a taxonomy of technologies and liabilities, hosted ten working group meetings, organized three workshops, and conducted hands-on analyses of several technologies. Known vulnerabilities were discovered in literature for connected vehicles, autonomous vehicles, electronic ticketing systems, traffic signal controllers, traffic signal priority, and dynamic message signs.

No known vulnerabilities were found in the literature for automatic vehicle location and computer-aided dispatch systems, online trip planners, mobile fare payment, onboard Wi-Fi, closed-circuit television, and automated passenger counters, but given their complexity, their wide attack surfaces, and the known vulnerabilities in related technologies, the research believes that it is reasonable to expect that security vulnerabilities do exist in these technologies as well. The survey of 25 transit agencies across the state of Florida revealed that the greatest perceived challenge to implementing good security practices was employee training, with lack of funding as the next most perceived challenge. The survey also revealed four agencies that have deployed autonomous vehicles and five agencies considering deployment in the next five years. The working group meetings discussed a wide variety of security topics, including security for mobile fare payment applications, safety policy, and certificate management for connected vehicles. Several members expressed support for security guidelines and sample policy, suggesting an increasing awareness of the importance of cybersecurity in public transportation.

The taxonomy classifying transportation technologies developed during the project partitions technologies based on five dimensions: extent of deployment in Florida, mode of transportation, functionality, responsible organizations, and liabilities. Communication systems and information technology (IT) systems such as email and agency networks are highly deployed, have many liabilities, and are operationally critical. However, these technologies are well researched, and many defenses for these systems currently exist. Less researched technologies such as computer-aided dispatch (CAD), automatic vehicle location (AVL), and mobile fare payment are also widely deployed and have critical liabilities. vii Two hands-on student-focused workshops and an academic workshop were held to further encourage cybersecurity awareness in the field. Students were instructed on the tools needed to

analyze mobile fare payment applications for Android devices and were given the opportunity to interact with the technologies inside of a traffic light controller cabinet.

For the academic workshop, faculty from Florida universities were invited to present and discuss their research and how it relates to cybersecurity in public transportation. The research team discovered a vulnerable Application Programming Interface (API) endpoint for a mobile fare payment application deployed in Florida that failed to authenticate the user. This vulnerability allowed a malicious user to collect personally identifiable information, including name, phone number, and partial credit card numbers. Additionally, because the vendor also provides parking payment solutions, the team was also able to access data for parking users, including license plate number and parking history. The research team followed a responsible disclosure process to present the vulnerability to the transit agency and vendor, and the issue was fixed by the vendor within six weeks of being reported. Because the application was a "white-labeled" solution with the same software serving multiple clients, 40 organizations were potentially affected by this vulnerability.

This report includes cybersecurity recommendations for transit agencies, including providing cybersecurity-related training for employees, conducting internal cybersecurity reviews, keeping systems up-to-date with the latest patches, securing and authenticating communications between system components (along with strong, non-default passwords), and having established policies for reporting and addressing vulnerabilities. The research team has provided suggested policy language for vulnerability disclosures for the security program plan additions for Rule 14-90 under consideration by the Florida Department of Transportation. Agencies should also comply with the Florida Information Protection Act of 2014, which outlines required activities of government agencies and their vendors in case of a data breach.

There are multiple areas of potential future work for cybersecurity in public transportation based on lessons learned in this project. Given the intersection of revenue collection for the agency and transit rider payment information on privately-owned devices, as well as the discovery of a vulnerability in the app examined by the research team during this study, mobile fare payment apps are a critical technology to examine further in detail. Onboard Wi-Fi, used for both public Internet access and critical communications (e.g., syncing schedules and offloading security video), is an important technology to analyze further as well. Based on the initial evaluations performed during this project, traffic signal controller equipment should also be further examined given its critical integration into transportation infrastructure and its network connectivity both to public (e.g., public transit, emergency response) and private vehicles (e.g., connected vehicles) as well as traffic management centers and other traffic controllers. In addition to creating template documents to assist agencies in implementing the suggested additions to Rule 14-90 in this project, future work should also examine adding cybersecurity components to the existing management plan processes (e.g., policies, training, reporting, emergency management, incident investigation, documenting drills and exercises, monitoring contractors) currently established for safety and security in Florida.

VIEW FULL REPORT: scholarcommons.usf.edu/cutr_nctr/12