Identify Sources and Risks on Cybersecurity for Connected Vehicle Infrastructures

Project Number

BDV25-977-70

Executive Summary

PREPARED FOR

Florida Department of Transportation

November 2022

Identify Sources and Risks on Cybersecurity for Connected Vehicle Infrastructures

Project No. BDV25-977-70

Submitted to:

FDOT Research Center

Ms. Megan Arasteh, P.E. (PM)
TSM&O Program Engineer
Florida Department of Transportation, District 7 Traffic Operations
11201 McKinley Drive, Tampa, FL 33612
E-mail: megan.arasteh@dot.state.fl.us

Dr. Raj Ponnaluri, P.E, PTOE, PMP (Co-PM)
Connected Vehicles and Arterial Management Engineer
Florida Department of Transportation
605 Suwannee Street, MS 90, Tallahassee, FL 32399
Email: raj.ponnaluri@dot.state.fl.us

Prepared by:

University of South Florida

Center for Urban Transportation Research

Dr. Pei-Sung Lin, P.E., PTOE, FITE (PI), Program Director
Dr. Achilleas Kourtellis (Co-PI), Assistant Program Director
Dr. Sean Barbeau (Co-PI), Senior Research Associate

Computer Science and Engineering

Dr. Jay Ligatti (Co-PI), Professor
Dr. Xinming (Simon) Ou, Professor
Kevin Dennis, Graduate Research Assistant

Civil and Environmental Engineering

Dr. Xiaopeng (Shaw) Li (Co-PI), Associate Professor
Zhaohui Liang, Graduate Research Assistant

November 2022

Disclaimer

The opinions, findings, and conclusions expressed in this publication are those of the authors and are not necessarily those of the Florida Department of Transportation.

Acknowledgments

The authors sincerely thank project managers Ms. Megan Arasteh, Mr. Daniel Buidens, and co-manager Dr. Raj Ponnaluri for their guidance and support throughout the project period. In addition, the authors thank Mr. Ronald Chin, FDOT District 7 Traffic Operations Engineer, and Mr. Derek Vollmer and Matthew DeWitt, FDOT Traffic Engineering Research Laboratory (TERL) for their valuable input and support and City of Tampa staff for their help in communicating with vendors and manufacturers and providing the traffic cabinet for testing and demonstration.

Executive Summary

Background

The transportation industry continues to adopt new technologies, and transportation systems are becoming increasingly connected. One of the latest innovations is the development and deployment of Connected Vehicles (CVs). CVs are vehicles equipped with a broad range of technologies that enable them to communicate with external devices such as other vehicles, roadside infrastructure, and the Internet. The different types of communication have been classified into the categories of Vehicle-to-Infrastructure (V2I), Vehicle-to-Vehicle (V2V), Vehicle-to-Cloud (V2C), Vehicle-to-Pedestrian (V2P), and Vehicle-to-Everything (V2X). CVs offer many benefits, such as significantly improved safety and mobility with cooperation between vehicles and infrastructure. Connected infrastructure includes Roadside Units (RSUs) and anything connected to those such as traffic controllers or other sensors that provide messages to broadcast.

Although CVs bring many benefits due to increased communication between vehicles and infrastructure, they also greatly increase the risk and likelihood of cyberattacks. Cyberattacks related to vehicles via onboard units (OBUs) have been investigated extensively, but the sources and risk levels from possible cyberattacks on CV infrastructure have not been investigated in detail. It is not clear what measures and precautions State, and local Departments of Transportation (DOTs) should take to prepare for managing incoming CV infrastructure.

This study provides a literature review of known vulnerabilities to transportation infrastructure, especially traffic signal controllers and RSUs deployed by transportation agencies around the world. This study also provides an examination of potential cyber vulnerabilities and a demonstration of possible attack scenarios on the transportation systems used in the field today.

Cyber Security Frameworks

According to the literature, there are three existing security frameworks for CVs. The first framework, the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, defines five key functions to ensure vulnerability analysis and cover all aspects of improving an agency's security posture—Identify, Protect, Detect, Respond, and Recover.

The second framework, the Open Web Application Security Project (OWASP) Application Security Verification Standard, provides three levels of application security and metrics that applications at each level should satisfy. As CVs and the technology supporting them are considered critical infrastructure, these technologies are expected to fall into Level 2 and Level 3. Level 2 applications contain some sensitive or private data, such as a mobile application with

a rider's travel history, and Level 3 applications are the most sensitive applications and perform critical actions, such as the malfunction management unit of a traffic signal controller.

The third framework, the Center for Internet Security (CIS) Critical Security Controls, provides a list of 20 key security controls, the majority of which are relevant for TMCs and agencies; many also apply to CV technologies directly. This list was used to ensure that all potential attack avenues were considered during analysis in the project.

Assessment of Vulnerabilities

During the first phase of the project, the research team conducted risk assessment on one traffic signal controller to identify existing cyber vulnerabilities. The team also used a CV OBU to perform cyber-attacks on a RSU and a traffic signal system. The identified vulnerabilities were shared with the Florida Department of Transportation (FDOT) Project Managers (PMs) as well as selected FDOT personnel. Following the successful demonstration, the research team worked with the FDOT PMs and officials to identify additional controllers commonly used at signalized intersections throughout Florida and acquired five of these controllers from different manufacturers. The team tested vulnerabilities on each controller and presented findings to FDOT project managers and staff.

The research team investigated common cyber vulnerabilities, threats, and liabilities in the industry to assess how strong the various traffic signal controllers are to cyber threats. Some of these vulnerabilities investigated included the following:

1. Arbitrary Code Execution
2. Privilege Escalation Attacks
3. Denial of Service and Jamming Attacks
4. Misconfiguration
5. Missing or Broken Authentication
6. Man-in the Middle Attacks
7. Missing or Broken Encryption
8. Others

Expert Interviews

In addition to researching vulnerabilities, the team conducted interviews with researchers, TMC operations and IT managers, as well as equipment vendors and OBU manufacturers. The team established a set of questions pertaining to the topic and held personal interviews via a virtual platform with representatives from these three groups. The team was able to interview six researchers from various universities with a wide range of expertise including V2V and V2I

security, cyber-physical systems, Denial of Service (DoS), embedded hardware systems, wireless networking and security including 5G for CVs, and machine learning. In addition, three interviews with six participants from different TMC operations and IT managers were conducted representing agencies that have a wide range of experience, including managing ~1,000 OBUs and 40 RSUs, smaller pilots with cellular-based CV technologies, and over 25 years of experience in the industry in Traffic Operations and IT support. Finally, four interviews with vendors and manufacturers were conducted with seven participants that covered a wide range of areas and products, including experience with V2I, V2X, Dedicated Short Range Communications (DSRC), Bluetooth, Wi-Fi, Advanced Traffic Management System (ATMS), Signal Phase and Timing (SPaT), and Cellular V2X (C-V2X).

Although participant responses varied based on their backgrounds, several key ideas appeared across each of the three groups. When discussing vulnerabilities, DoS and jamming were mentioned by all six researchers, two of the three TMC and IT managers, and two of the four vendors or manufacturers. In addition, spoofing was mentioned by four of the six researchers, two of the three TMC and IT managers, and by two of the four vendors/manufacturers.

When discussing known attacks on CVs, only one participant could describe an attack in practice that targeted CV technologies—a ham radio operator was broadcasting on the same frequency as their DSRC in an area near their operations, interrupting their communications. They had to locate the operator and stop their broadcasts. The participant described how it may be a challenge to scale this technology up for an entire city. A handful of rogue radio operators could interrupt normal operations.

Some interview participants mentioned that the lack of known cyberattacks on CV technologies was likely due to the lack of broad deployment of such systems. Many described attacks on related technologies and how those may be transferable to CVs. The most popular example was the Jeep Cherokee attack presented at Black Hat 2015 by Charlie Miller and Chris Valasek. The duo was able to remotely hack the vehicle and take control of many systems, including steering, which resulted in the recall of 1.4 million vehicles by Fiat Chrysler.

Increased communication and coordination among security experts and agencies was a common recommendation by researchers and all TMC and IT managers. Vendors did not explicitly mention increased security expert involvement, but three of the four noted the importance of including security as a goal when designing and planning.

Mitigation Measures

Mitigation measures were recommended for all vulnerabilities found for agencies and for manufacturers of the devices. A high-level, non-comprehensive list of recommended mitigation measures is as follows:

1. Assume that all communications on networks, even those considered closed and private, can be monitored (as is the case on the general Internet).

2. Segregate networks as much as possible to avoid an attacker being able to easily pivot from taking over a single system to attacking many other systems on the network. For example, use of virtual private networks (VPNs) for communication between Traffic Management Centers (TMCs) and field cabinets can secure communications.
3. Monitor network traffic and log access attempts.
4. Use intrusion detection systems to identify anomalous behavior in a network.
5. Strengthen the physical security of transportation systems at access points (e.g., traffic cabinet).
6. Use modern password and authentication techniques (e.g., strong passwords, hashing, multifactor authentication, or co-authentication).
7. Participate in information-sharing organizations for real-time assessment and knowledge of threats.
8. Prioritize security in the design process of traffic controllers (e.g., creating easy-to-use and secure access controls).
9. Require secure design principles from vendors of ITS devices approved for use.
10. Perform software and firmware updates as soon as they are released from vendors.
11. Participate in and follow vulnerability databases for up-to-date information on common software components used in traffic controllers.
12. Use and require secure credential management systems for CV applications (both OBU and RSU).
13. Establish a cybersecurity review process to examine traffic signal controllers for commonly-identified cybersecurity issues prior to approving them for field use.
14. Create and support a clear vulnerability disclosure system or program that can expedite disclosure of vulnerabilities from third parties (e.g., researchers) who are not part of the manufacturer or agency teams.

Detailed findings and recommendations can be found in the confidential supplemental reports submitted to the FDOT PMs. DOTs, cities, counties, controller vendors and manufacturers, and other stakeholders who have a legitimate interest in the cybersecurity of traffic controllers should review these confidential reports, in particular Deliverable 4, Part 2, to address vulnerabilities identified in their systems. These parties may request access to the confidential reports by contacting the FDOT Research Center.

Due to the sensitive nature of the findings, detailed results and specific mitigation strategies or recommendations are presented in three confidential supplemental reports:

1. **Deliverable 3, Part 2: Demonstration of Cyberattack on Traffic Signal Controller and Recommended Mitigation Measures.** This report describes in detail the methods and scenarios for a cyberattack on a traffic controller being used in the field, highlights the

vulnerabilities, and provides mitigation measures. These findings were showcased at a demonstration to FDOT officials in June 2021.

2. **Deliverable 3, Part 3: Demonstration of a Cyberattack on a Roadside Unit and Potential Mitigation Measures.** This report describes in detail methods and scenarios for a cyberattack on an RSU via a rogue OBU, highlighting vulnerabilities and providing mitigation measures. These findings also were showcased at a demonstration to FDOT officials in June 2021.

3. **Deliverable 4, Part 2: Assessment of Additional Traffic Controller Types.** This report provides detailed findings on vulnerabilities discovered in five additional traffic controllers identified by FDOT for the project and provides an update on the traffic controller previously examined in Deliverable 3, Part 2. These findings supplement the work showcased in Task 3.

Demonstration

The demonstration of cyber vulnerabilities for CV infrastructure was conducted at the Center for Urban Transportation Research (CUTR), at the University of South Florida (USF) and also in the field on the USF Tampa campus. Figure 1 shows participants representing the research team, FDOT staff, and City of Tampa staff.

Figure 1. Participants at the demonstration.

Figure 2 shows pictures from the demonstration.

Figure 2. Demonstration of vulnerabilities at CUTR-USF.