Florida Department of Transportation Research

# Identify Sources and Risks on Cybersecurity for Connected Vehicle Infrastructures

November 2022

**Project Number**
BDV25-977-70

**Project Manager**
Megan Arasteh
*State Traffic Engineering and Operations*

**Principal Investigator**
Dr. Pei-Sung Lin
*University of South Florida*

## Current Situation

When it comes to highway safety, we typically think of vehicles and people. But with a growing connected transportation system, the Florida Department of Transportation (FDOT) is eyeing another kind of crash – cyber.

Connected vehicles (CV) are equipped with a range of technologies that enable them to communicate with external devices like other vehicles, roadside infrastructure, and the Internet . However, innovations that make CV information sharing easier and faster also present vulnerabilities for cyberattacks. These CV attacks can have real-world physical consequences – cyberattacks that mitigate safety mechanisms which in turn cause physical damage and harm – but can also result in costly slowdowns, service disruptions, or traffic congestion.

*A member of the University of South Florida's Center for Urban Transportation Research showcases a cyberattack on a connected vehicle roadside unit (potentially a traffic signal system) via an onboard unit.*

At the time of this research project, it was not clear what measures and precautions state DOTs and local transportation departments should take to prepare for managing CV cyberattacks.

## Research Objectives

FDOT and University of South Florida researchers aimed to identify and examine known and potential cyber vulnerabilities and demonstrate CV cyberattack scenarios. The team also made recommendations to bolster cybersecurity and provided mitigation measures and recommendations on practices that could decrease the likelihood of a successful cyberattack by rogue actors.

## Project Activities

Following an extensive literature review and interviews of subject matter researchers FDOT and USF's Center for Urban Transportation Research (CUTR) researchers assessed the cybersecurity of six different traffic controllers commonly used at Florida intersections. The team demonstrated in real-time how cyberattacks could be successfully performed on each controller. The team then demonstrated an attack on traffic control systems, exposing several vulnerabilities of the infrastructure. Due to the sensitive nature of the information, the details of the findings are not available in the final report.

The team used the demonstration to develop mitigation methods and recommendations to reduce the likelihood of such attacks. One notable finding: researchers found that similar attacks could create traffic incidents at intersections 23% worse than if no traffic control system had been deployed at all.

## Project Conclusions and Benefits

Researchers found that all CV tests for this project exposed the vulnerabilities of current intelligent transportation infrastructure. As FDOT continues to lead the way in cybersecurity for its transportation system, it will be more equipped with the appropriate safeguards to manage potential attacks on its infrastructure and mitigate their impacts if they do happen.

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