Intersection Management and Cybersecurity: Applications, Issues, and Scheme

Executive Summary

Kimberly Collins, Yunfei Hou, Monty Van Wart, and Paul Suino

Introduction

Safeguarding against cybersecurity attacks is quickly becoming a prevalent issue facing local government agencies. Recent cyber-attacks, such as the 2018 SamSam ransomware attack that affected the City of Atlanta, have demonstrated the capacity to wreak havoc on city networks by paralyzing daily operations. Concerning transportation and technology, Traffic Management Systems (TMS) are becoming more vulnerable and susceptible hacking targets as they rapidly develop to become more connected and "intelligent".

With the support of the Western Riverside Council of Governments (WRCOG), the briefing paper was written to bring awareness to the possible cyber threats to the transportation system in the Inland Empire and to craft recommendations or next steps to addressing any shortfalls. Key findings included educating current local government leaders and employees on the current risks, increasing the interaction of CSUSB faculty and students to help address the issues, developing a comprehensive planning project increasing the interest and participation of local university level students and faculty to help alleviate the burden of cybersecurity threats felt by local governments.

Local Government Cybersecurity Incidents

Forty-four percent of local governments experience daily cyberattacks. The actual rate is much higher as less than 60.1% count how often they are attacked. Incidents range from mischievous attacks (ex.: road signs) to the interruption of daily activities (ex.: infected servers). Today, cybersecurity threats to ITS systems may be single acts or a combination of discrete steps threaded together, immediate and ongoing or evasive-by-design software attacks, intentional or unintentional physical manipulation/exploitation of hardware, and internal or external attacks by bad actors. These threats can include:

- Denial-of-Service, such as jamming Wi-Fi signals or blocking user access
- Traffic congestion, such as wrongly rerouting/timing vehicles
- Individual/multiple traffic signal control, such as changing all lights green
- Autonomous/connected vehicle manipulation, such as seizing command of a vehicle's braking system
- Spear phishing, such as targeted online attempts to steal sensitive information, either directly from a credible actor/employee or from the system itself
- Privacy issues, such as bad actors tracking specific vehicles via different sensors in different positions

Overview of Traffic Management Systems/Elements and Challenges

Sensors like the induction loop are buried and used for vehicle detection. Microwave, radar, and ultrasonic sensors are used for special applications. **Traffic signal controllers** are locked in roadside cabinets and responsible for light timing patterns at intersections. **Communication and network devices** are both hard-wired and wireless systems that communicate with each other and with traffic management centers. **Malfunction Management Units (MMU)**, aka conflict monitor units (CMU), are hardware-level, fail-safe mechanisms that monitor/override the outputs of the controller. **Advanced traffic management systems (ATMS)** consist of management centers, field infrastructure, and mobile units communicating in real time. **Dynamic Message Signs**, aka Variable Message Signs, are large electronic signs used to display information. **Adaptive and Coordinated Signal Control** refers to technologies that capture traffic demand data using sensors to optimize flow. **Transit Signal Priority and Emergency Vehicle Priority (TSP)** are operational improvements that modify signal timing to favor transit vehicles. **Eco-Signal** offers drivers accurate information about upcoming signal status. **V2V/V2I Communication** is the ability to wirelessly exchange information between vehicles. **Bluetooth/Wi-Fi Traffic Probes** scan for other enabled devices and store data for future analysis. **Third Party Traffic Data** is collected by companies to be used to improve traffic.

Challenges for intersection management are that:

- Devices frequently have low, or no level of cybersecurity built into them
- The industry has been slow to respond and be proactive in providing security
- Cyber threats are introduced through individual devices and the amalgamation of devices
- Federal guidance on cybersecurity has tended to be generic to date
- Agencies using intersection management are the smallest, most financially stretched
- Smaller agencies cannot compete for cybersecurity experts in an extremely tight market
- Building cybersecurity awareness is an aspect of the larger local government problem

Specific Vulnerabilities of Traffic Signal Systems

Controller attacks target privileged access to the light controller. When successful, lights could be changed, denial-of-service (DoS) may be initiated, or the malfunction management unit could take over, causing lights to enter a suboptimal state. While an attack can be triggered remotely, MMUs can only be reset manually. **Sensor data attacks** are assaults on the data being communicated to the controller. A malicious party can send bogus packets, leading the controller to operate with misinformed information. Additionally, an attacker can modify firmware with corrupted data which will cause the sensor to no longer function. **Physical attacks** directly tamper with the hardware. Vandalism and graffiti are common problems with public infrastructure, and traffic signal systems are designed with resiliency to handle physical system failures. However, coordinated attacks performed through a combination of cyber and physical attacks present a significant threat to the systems. For instance, if the MMU (a hardware fail-safe device) is damaged or removed, a coordinated cyberattack can trigger dangerous light timing patterns, leading to potential massive damage and/or traffic disruption.

The Current Regulatory Framework for Intersection Management

National level strategy has focused on providing rules or guidance about cybersecurity practices to be used by public agencies, and by providing legal standards or guidance about equipment to vendors and public agencies. To improve resilience and reduce cyber threats, rules have focused on consistent use of traffic control devices via the Manual on Uniform Traffic Control Devices (MUTCD). While these rules are national in scope, *cybersecurity of intersection management is not federally regulated.* The federal government is likely to issue initial rules and guidance on connected and autonomous vehicles cybersecurity in the near future.

States have the best resources to provide qualified, preferred traffic control systems lists. California's TEES guidance is used by most states in the country, as well as local governments in California. Use of the TEES list is not mandated, but frequently voluntarily adopted. The state is aggressive on cybersecurity at an enterprise level with a Security Operations Center in the Department of Technology's Office of Information Security. While this resource will likely bolster prevention, it seems unlikely to have much effect in the near future on state or local intersection management issues.

Local governments do not seem to understand the scope of their problems, let alone have much in place beyond generic cybersecurity protocols. Striking shortages of IT and cybersecurity personnel have been widely reported. Internal practices and policies with existing personnel create tremendous gaps in local government's cyber responses. Further, local governments are cash-strapped and aren't easily convinced, for example, that they must manually update every signal controller to thwart vulnerabilities at intersections.

Status of Local Government Cybersecurity Implementation and Recommendations for Future Actions

This study collected 18 questionnaires, conducted six Zoom interviews spanning 14 city/county transportation agencies, and talked to two consulting companies in the area. A typical intersection management team consists of 2 to 4 engineers and technicians who manage daily operations for 100-400 signals. Over 90% of surveyed intersections were found to be using McCain systems.

Our key findings are:

1) *Connected devices are named the top threats*. Among the 1157 traffic signals surveyed in this study, 67.6% of them are connected;

2) *Cities lack cybersecurity support*. Most professionals said they are not aware if their agencies follow standardized security practices. 67% believe lack of trained personnel is a major obstacle to adopting advanced security processes/technology; and

3) *Cities need to plan for future technology*. Nearly 80% of the agencies said that they are underfunded for their transportation needs. Authorities need to be able to recruit, compensate, and retain the type of high-caliber talent necessary to protect critical infrastructure.

Next Steps

<u>Outreach to Local City Officials</u>

1. Presentation of initial results from this study to the WRCOG City Managers' Council and other groups identified by staff at the WRCOG.
2. One-day conference on Transportation Cybersecurity in the IE, showcasing programs at CSUSB, local government work, and regional experts, highlight new research findings, and bring in equipment vendors who represent the higher rated companies.

3. Conduct cybersecurity audits and assessments for local cities. In collaboration with the WRCOG, teams of students, led by CSUSB faculty, will conduct cybersecurity audits of local jurisdictions. The project team will develop best practices and standard operating practices for local cities.

Information Technology Master Plan for Western Riverside Counties

1. CSUSB faculty and students will assist in the development of the WRCOG's IT Master Plan. Assistance will focus primarily on cyber, but other assistance will be offered as needed.

Education and Internship Programming

1. Provide training seminars for current local government personnel to better understand cybersecurity issues and develop security plans based on current resources.

As part of the current WRCOG Fellowship program, a specific fellowship for CSUSB cybersecurity students to work in local government or for contractors working for governments will be developed.

The full study with references is offered upon request. Publication pending.

Kimberly Collins, PhD, Executive Director, Leonard Transportation Center and Professor of Public Administration, CSUSB – kimberly@csusb.edu