Final Report CUTR-2019-09

Enhancing Cybersecurity in Public Transportation

Deliverable 7: Final Report

Project Number

BDV25-977-51

Prepared For

Florida Department of Transportation

September 2019

2019

CUTR CENTER FOR URBAN TRANSPORTATION RESEARCH

USF UNIVERSITY OF SOUTH FLORIDA

CUTR.USF.EDU

DISCLAIMER

The contents of this report reflect the views of the authors, who are responsible for the facts and the accuracy of the information presented herein. This document is disseminated under the sponsorship of the Department of Transportation University Transportation Centers Program and the Florida Department of Transportation, in the interest of information exchange. The U.S. Government and the Florida Department of Transportation assume no liability for the contents or use thereof.

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

Metric Conversion

SI* Modern Metric Conversion Factors as provided by the Department of Transportation, Federal Highway Administration http://www.fhwa.dot.gov/aaa/metricp.htm

Length

SYMBOL	WHEN YOU	MULTIPLY BY	TO FIND	SYMBOL
in	inches	25.4	millimeters	mm
ft	feet	0.305	meters	m
yd	yards	0.914	meters	m
mi	miles	1.61	kilometers	km

Area

SYMBOL	WHEN YOU	MULTIPLY BY	TO FIND	SYMBOL
in^2	square inches	645.2	square	mm^2
ft^2	square feet	0.093	square meters	m2
yd^2	square yard	0.836	square meters	m2
ac	acres	0.405	hectares	ha
mi^2	square miles	2.59	square	km^2

Length

SYMBOL	WHEN YOU	MULTIPLY	TO FIND	SYMBOL
mm	millimeters	0.039	inches	in
m	meters	3.28	feet	ft
m	meters	1.09	yards	yd
km	kilometers	0.621	miles	mi

Area

SYMBOL	WHEN YOU	MULTIPLY BY	TO FIND	SYMBOL
mm^2	square	0.0016	square inches	in^2
m2	square meters	10.764	square feet	ft^2
m2	square meters	1.195	square yards	yd^2
ha	hectares	2.47	acres	ac
km^2	square	0.386	square miles	mi^2

*SI is the symbol for the International System of Units. Appropriate rounding should be made to comply with Section Four of ASTM E380.

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle Enhancing Cybersecurity in Public Transportation		5. Report Date September 2019
		6. Performing Organization Code
7. Author(s) Sean J. Barbeau, Jay Ligatti, Kevin Dennis, Maxat Alibayev		8. Performing Organization Report No.
9. Performing Organization Name and Address National Center for Transit Research Center for Urban Transportation Research University of South Florida 4202 E Fowler Avenue, CUT 100, Tampa, FL 33620-5375		10. Work Unit No. (TRAIS) 11. Contract or Grant No. BDV25-977-51
12. Sponsoring Agency Name and Address Florida Department of Transportation 605 Suwannee Street, MS 30 Tallahassee, FL 32399		13. Type of Report and Period Covered Draft Final Report 1/31/18-7/1/19 14. Sponsoring Agency Code
15. Supplementary Notes		

16. Abstract

As transportation infrastructure continues to expand from isolated nodes to large interconnected networks, cybersecurity is a critical concern for transit agencies. This report provides recommendations and suggested policies for transit agencies that may help reduce cybersecurity liabilities. The recommendations are informed by a literature review of existing vulnerabilities, a survey of Florida transit agencies, a taxonomy of transit technologies, outcomes of cybersecurity working groups and workshops, and hands-on analyses of several technologies, all of which were conducted as part of this project. Existing vulnerabilities were discovered in literature for connected vehicles, autonomous vehicles, electronic ticketing systems, traffic signal controllers, traffic signal priority, and dynamic message signs. Survey participants ranked employee training as the biggest challenge to implementing good cybersecurity practices. The taxonomy of transit technologies was based on five dimensions: extent of deployment in Florida, mode of transportation, functionality, responsible organizations, and liabilities. The report also includes the results of the cybersecurity working group meetings and workshops held during the project and provides a detailed analysis of a vulnerability discovered in a Florida mobile fare payment application by the research team. Important areas of future work include further examining mobile fare payment apps, onboard Wi-Fi, and traffic controller equipment, as well as adding cybersecurity components to the existing management plan processes currently established for safety and security in Florida.

17. Key Word	18. Distribution Statement
cybersecurity, transit, public transportation, fare payment, security, safety, vulnerability	No restrictions.

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified.	Unclassified.	173	

Form DOT F1700.7 (8-72) Reproduction of completed page authorized

Acknowledgements

The research team would like to thank the City of Tampa for generously donating a traffic cabinet to the Center for Urban Transportation Research and Mission Secure for providing traffic cabinet equipment for further analysis. The team would also like to thank everyone who participated in working group meetings and attended the workshops, with a special thank you to those who presented at the various events.

This work was supported by the National Center for Transit Research, a program of the Center for Urban Transportation Research at the University of South Florida and funded by the U.S. Department of Transportation and Florida Department of Transportation.

FDOT Project Manager
Gabrielle Matthews, Transit Planning Research Administrator, Florida Department of Transportation

Executive 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.

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.

Table of Contents

List of Figures

List of Tables

Abbreviations and Acronyms

API	Application programming interface
AV	Autonomous vehicle
CCTV	Closed-circuit television
CUTR	Center for Urban Transportation Research
CV	Connected Vehicle
FTP	File transfer protocol
GPS	Global positioning system
IDS	Intrusion detection system
IT	Information technology
JTA	Jacksonville Transportation Authority
MMU	Malfunction management unit
MSi	Mission Secure
NFC	Near-field communication
OT	Operational technology
OWASP	Open Web Application Security Project
QR	Quick response
SPP	Security program plan
SSH	Secure shell
TMC	Traffic management center
USF	University of South Florida

CHAPTER 1: INTRODUCTION

1.1 Introduction

Cybersecurity is a significant concern in all industries. Given the rapid adoption of technology in the area of automated and connected vehicles, transportation infrastructure is a particularly attractive target. The concern is so great that in 2013 the Florida Legislature requested the formation of the Florida Center for Cybersecurity [1], which named transportation as a key focus area. *Protection of Transportation Infrastructure from Cyber Attacks: A Primer* says:

> "The sheer numbers of suddenly visible, interconnected, increasingly vital cyber components now deployed in transportation system and transit operations have created enormous, underappreciated complexity and significantly greater vulnerability across the entire system… This situation is poorly understood by transportation system executives, program managers, employees, elected officials and regulators." [2, p. iv]

Public transportation vehicles (e.g., buses) are perhaps the most-exposed component of transit infrastructure—they carry a large number of individuals that are continuously entering and exiting and contain a constantly increasing number of different technologies (including wirelessly connected systems) that can be leveraged as potential attack vectors. Transit agencies are also deploying an increasing number of technologies outside of the vehicle, including mobile apps for fare payment and real-time arrival information, automatic vehicle location, traffic signal priority, and onboard Wi-Fi.

The goal of this project is 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.

1.2. Project Overview and Report Structure

The report is organized into seven parts. This section, Chapter 1, provides an overview of the project and the structure of the report.

Chapter 2 reviews the literature about transit technologies, including equipment and protocols, for known vulnerabilities and defenses. Chapter 2 focuses on technologies deployed at Florida transit agencies and covers not only technologies currently deployed, but also those known to be considered for future deployment.

Chapter 3 describes a survey that was created and distributed to Florida transit agencies to collect information on security-relevant technologies, known and potential vulnerabilities, and cybersecurity concerns. The results of the survey are provided and analyzed.

Chapter 4 describes the working group meetings held throughout the project. The working group meetings exchanged cybersecurity information, including concerns and mitigations, between various stakeholders in Florida's transportation cybersecurity. The major discussion points and results of each meeting are described.

Chapter 5 provides a taxonomy of transit technologies, based on information gathered during the work conducted for Chapters 2, 3, and 4. The technologies are classified based their deployment, mode of transportation, functionality, responsible organizations, and potential liabilities.

Chapter 6 describes three workshops that were held throughout the project. The first two workshops were hands-on student-focused workshops, allowing students to explore mobile fare payment applications and traffic cabinet technologies. The third workshop brought together faculty from Florida universities to present their research and how it relates to cybersecurity in public transportation.

Chapter 7 provides recommendations for reducing cybersecurity liabilities, including suggested policies and processes for ongoing monitoring and improvement of transit cybersecurity. Technology analyses conducted during the project are included in this part, as well as final conclusions from the project and important areas of future work.

Chapter 8 concludes the report with a review of the major findings from the project and describes potential opportunities for future work.

CHAPTER 2: LITERATURE REVIEW

2.1. Introduction

This section reviews existing transit technologies, including equipment and protocols, for known vulnerabilities and defenses. The review focuses on technologies deployed at Florida transit agencies and covers not only technologies currently deployed, but also those known to be considered for future deployment. This literature review is informed by a survey conducted concurrently, as part of the same project, that collected transportation system deployment information from Florida transit agencies. Technologies of interest include fare payment (on-vehicle and mobile), onboard Wi-Fi, Automatic Passenger Counters (APC), Traffic Signal Preemption (TSP), autonomous and connected vehicles, and general information technology systems such as email (due to vulnerabilities to, for example, spear phishing attacks).

Existing reports [1, 2] have focused on implementing effective cybersecurity policies in public transportation management. This paper takes a more technical approach and evaluates the current state of technologies used in public transit and their vulnerabilities by reviewing known vulnerabilities discussed in a variety of technical venues. This report also presents the estimated costs of attacks on transit technology when the information is available in the literature. The remainder of this section provides a brief background of the field and presents major related works, which cover both cybersecurity policy and technology.

2.1.1. Background

Transit agencies have improved their operational and financial processes and services with the deployment of modern computing machines and technologies, such as mobile applications, autonomous vehicle location, connected vehicles (CVs), autonomous vehicles (AVs), and other devices in the field. The achieved advantages include improved fleet management, increased ridership and rider satisfaction through bus tracking and other mobile apps, more easily accessible fare payments, and more [3, 4]. These achievements highlight the continued growth in transportation technologies, which have significantly developed in recent years from individual nodes to large, interconnected networks of devices, similar to those seen in modern IT systems. With this rapid development comes security concerns that have typically been constrained to classical computer systems. The transportation sector is a particularly attractive target for adversaries seeking to have a wide area of impact.

Operational Technology (OT) is defined by Gartner as “hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise” [5]. While IT and OT are converging, the differences between them are greater than the similarities [6]. The term “Cyber-physical systems” refers to the integration of computation, networking, and physical processes [7]. IT and OT are compared in greater detail in Section 1.2.2.

Transportation agencies have already suffered from cyber-attacks. On February 22, 2018, the Colorado Department of Transportation shut down 2,000 employee computers after the SamSam ransomware virus infected their systems and stole files [8]. With help from their antivirus software provider, CDOT was able to remove the virus from their computers. In addition, CDOT did not pay the ransom because their files were backed up before the attack. Nevertheless, a week later, the same ransomware struck them again. It mutated into a new virus and re-infected the computers. A spokeswoman for the state's Office of Information Technology, Brandi Simmons, said:

> *"We had 20 percent of the computers up and running when our security tools detected malicious activity. And sure enough, the variant of SamSam ransomware just keeps changing. The tools we have in place didn't work. It's ahead of our tools."* [8]

This example shows that even well-known cyber-attacks keep evolving, and it is crucial to learn how to effectively mitigate them. Cybersecurity researchers and attackers are constantly finding new ways to exploit systems.

2.1.2. Related Reports

This section provides an overview of two major reports that are related to security in transit environments.

2.1.2.1. Securing Control and Communications Systems in Transit Environments

The *Security for Transit Systems Standards Program* [9] from the American Public Transportation Association consists of multiple documents that address transportation cybersecurity from different perspectives. These perspectives include: control and communications security, emergency management, enterprise cyber security, infrastructure security, and security risk management.

Securing Control and Communications Systems in Transit Environments [2] is a four part document from the *Security for Transit Systems Standards Program* [9] designed to provide additional guidance for transit agencies seeking to implement stronger security policies related to control and communication security. The following paragraphs summarize the first two sections of this document. The final two sections focus on attack modeling for transit agencies and are distanced from the technology itself, so they are not presented here.

Part I: Elements, Organization and Risk Assessment/Management [2] briefly introduces a wide range of technologies, with a focus on rail technology. In addition, several generic network layouts are described, which provides a useful overview of the potential attack surface that may be present at an agency. The last two sections cover creating a security plan for transit agencies, and how agencies can perform risk assessment and management.

Part II: Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones [10] describes security zones, how they can be used to protect critical infrastructure, and a variety of related topics. While the paper focuses on rail transit, the zoning scheme is based on zones described by the Department of Homeland Security for industrial control systems and can be generalized to other areas of public transit.

2.1.2.2. Protection of Transportation Infrastructure from Cyber Attacks: A Primer

Protection of Transportation Infrastructure from Cyber Attacks: A Primer [1] provides a deep review of cybersecurity policy making and cybersecurity fundamentals, written specifically for the transit professional. The primer aims to assist professionals seeking to write strong policy for their agencies and to harden their technologies.

Notably, the primer begins by dispelling seven common cybersecurity myths, such as "Nobody wants to attack us" [1, p. 4]. The primer argues that the few number of catastrophic attacks on transit agencies has lulled them into a false sense of security. While in the past cyber risks were low and mainly required physical access, with the increasing connectivity of transit technologies the risk of attack also increases and must be perceived as such. Dispelling these myths allows agencies to more effectively implement high-quality security policy.

The primer also provides a comprehensive comparison between IT systems and Industrial Control Systems (ICS), a subset of OT. ICS prioritizes availability above all other concerns, followed by integrity, and finally confidentiality, while IT systems prioritize confidentiality, then integrity, and finally availability. This distinction reflects ICS's time-critical nature, compared to IT's traditionally greater prioritization of correctness and security over availability.

2.2. Information Technology Security

Many IT systems are used in the day-to-day operations of a transit agency, including email, databases, web applications, and networking equipment [11]. Maintaining these systems is critical to an agency's operation. IT systems also may contain sensitive internal or customer data. For cyber incidents in the transportation industry, the average cost is $121 for each record involved in the incident [1, p. 2].

Exercising proper network security is critical to reducing the security vulnerabilities present at an agency. Fok [12] provides an analysis of vulnerabilities that may be present in a typical Traffic Management Center (TMC) and offers suggestions for mitigating attacks by securing the network. Security technologies such as firewalls and intrusion detection systems should be installed, and correctly configured.

As defined by US-CERT, *phishing* "is an attempt by an individual or group to solicit personal information from unsuspecting users by employing social engineering techniques" [13]. Phishing is often conducted by sending emails with urgent requests for information or tempting

offers that aim to convince the victim to provide information at a web link provided in the email. From the 2017 survey [14] results released by the Florida Center for Cybersecurity [15], phishing attacks were considered the greatest security risk by stakeholders in government, academia, and business. Spear phishing is a phishing attempt that is crafted to target a specific organization or person [16].

The Anti-Phishing Working Group (APWG) [17] provides advice on how to avoid phishing. APWG collects suspected phishing attempts for analysis, and releases quarterly reports on trends in phishing.

Ransomware is a form of malware that prevents the normal operation of a computer system and typically demands payment in virtual currencies (e.g., Bitcoin) to restore functionality [18]. The techniques used to prevent operation vary, but malware typically locks the display to a ransom screen demanding payment, and/or encrypting the files on the system [19]. Ransomware is often distributed in phishing attempts; 93% of phishing emails contain ransomware [20].

The potential damage due to ransomware attacks varies greatly but can be reduced with proper preparation. A ransomware attack in Paris, Tennessee cost the city approximately $20,000 [21]. Another ransomware attack in Atlanta, Georgia cost approximately $2.6M [22]. The US Computer Emergency Readiness Team (US-CERT) [18] lists several preventative measures, including developing and executing proper backup and data recovery plans, and staying up-to-date with system updates.

2.3. Transit Technologies

This section reviews, with a focus on cybersecurity, transit technologies in the following categories: online trip planners and real-time passenger information, electronic ticketing and fare collection systems, field devices, operations and fleet management, and emerging technologies.

2.3.1. Online Trip Planners and Real-time Passenger Information

Overview

Online trip planners assist riders by creating step-by-step directions to a given location using a source and destination provided by the user. Online trip planners ease the learning curve associated with planning a trip using a traditional paper transit schedule, and many provide the real-time status of vehicles [23]. The term *Real-time Arrival Information* "refers to up-to-the-minute tracking of transit vehicles by automatic vehicle location systems or track circuit systems" [24, p. 2]. Real-time arrival information may increase passenger satisfaction, ridership, and perception of personal security, and reduce time spent waiting [4, p. 1816, 24].

Access to online trip planners and real-time passenger information systems come in a variety of forms, including mobile phone apps, websites, smartwatch apps and virtual assistants.

OneBusAway [25] lists eight different modes for accessing real-time information, including smartphone applications, a smart watch app, virtual assistant, and a web page. Several mobile apps (Transit App, OneBusAway) provide multimodal trip planning, further improving the accessibility of transit to users. The proliferation of applications powered by transit data was largely made possible by the development of the *General Transit Feed Specification* (GTFS), an open data format [26].

Implementation

The General Transit Feed Specification (GTFS) developed by Google and TriMet in 2006 defines a common format for public transportation schedules and associated geographic information [27]. A GTFS feed is composed of several comma-delimited data files that contain information about the different aspects of the routes: stops, routes, trips, stop times, etc. These files, when made available over the Internet as a zip file hosted on the transit agency's servers, allow third party applications to download and process the information to provide trip planning services to riders. These files must be updated regularly (typically around 3-4 times per year, but not more frequently than every seven days) to ensure that riders are provided accurate information. The official documentation can be found at Google's GTFS reference page [28].

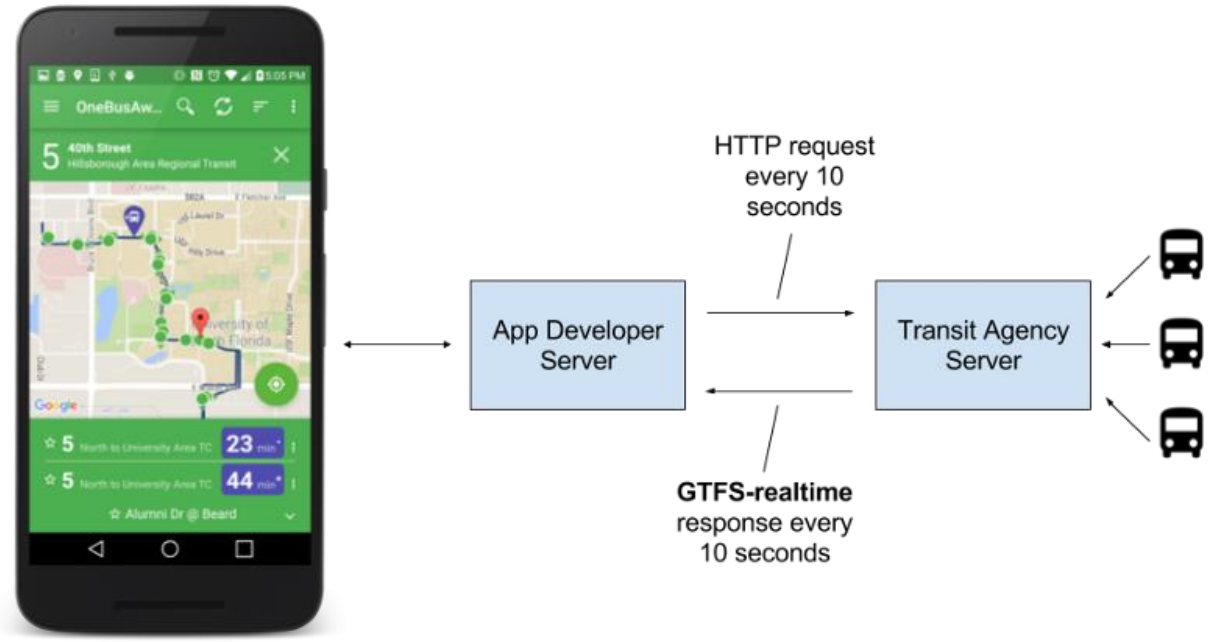

Figure 2.1 Typical real-time information flow from a transit agency to a mobile app

A real-time counterpart to GTFS is GTFS-realtime [29]. GTFS-realtime has recently emerged as a de facto standard for real-time arrival prediction, vehicle positions, and service alerts [30]. GTFS-realtime feeds are hosted on the transit agency's server in the protocol buffer binary format [31]. GTFS-realtime information changes rapidly (e.g., every 10 seconds), so consuming applications must frequently request updated information from the transit agency's server to ensure that real-time data shown to riders is current. Figure 2.1 shows the typical real-time information flow from a transit agency to a mobile app.

Transit agencies typically share their GTFS and GTFS-realtime data with third-party applications such as Google and Apple. In this case, the transit agency application servers are data-distribution mechanisms for the GTFS zip file as well as the GTFS-realtime protocol buffer files (e.g., via an HTTP request/response model), but the agency's servers do not provide a direct service to the transit rider. Instead, the third party maintains the application that the transit rider uses.

Transit agencies are increasingly hosting their own trip planning or real-time information services as well. The application servers can be hosted on the transit agency's internal IT network or on cloud services (e.g., Amazon Web Services, Google Kubernetes Engine), either managed directly by the transit agency or by a contractor/vendor on the agency's behalf. These application servers can provide data to many potential platforms including native smartphone applications, web pages, text messages, touchtone, and virtual assistants.

Online trip planners have been moving toward open-source solutions in recent years. Popular examples include OpenTripPlanner [32] and OneBusAway [25]. Open-source solutions offer a wide range of benefits to agencies looking to establish their own services for transit riders. While managing and setting up an open-source solution may initially be more work for the agency or its contractor, the open-source solution provides a wide range of features that can be configured for the agency's deployment, reduces vendor lock-in (i.e., the solution can potentially be maintained by any qualified third party), pools resources from many agencies to maintain and enhance the same application, and avoids any ongoing licensing fees for data or services. Both OpenTripPlanner and OneBusAway provide Application Programming Interfaces (APIs), streamlining application development and offering significant flexibility for developing future solutions [23, 33].

Security Considerations

Because GTFS and GTFS-realtime data distribution platforms, online trip planning, and real-time information applications typically consist of a web server maintained by the transit agency or their contractor, the vulnerabilities and defense strategies for these technologies are well documented. Organizations such as the Open Web Application Security Project (OWASP) [34] provide a wealth of information on this subject. This paper instead focuses on the risks these technologies may present to the transit agency. Cloud-hosted or contractor-provided servers are susceptible to attacks similar to those described below. A compromised cloud server that communicates with the internal network may still be used to attack an internal network.

If successfully compromised, a web server may be a valuable pivot to attack other machines on the same network, and these other machines may contain more sensitive information or controls. Outward-facing machines such as the web server should be placed in a *Demilitarized Zone* (DMZ): a section of the network separated from the rest of the internal network by a backend firewall. Fok [12] discusses tecniques agencies may implement to better

secure a network, such as establishing a DMZ, and *Protection of Transportation Infrastructure from Cyber Attacks: A Primer* describes in detail the benefits of proper zoning for transit agencies.

A unique risk for online trip planners that is not present for IT web servers is the nature of the service provided by online trip planners and the real-time information apps provide. Online trip planners, if compromised, could trick riders into following incorrect directions, possibly leading them into dangerous areas, driving the wrong way on a one-way street, etc. A news article from 2016 [35] suggests that people are willing to follow wrong directions from Google Maps regardless of physical signs warning them of the error. Similarly, real-time information apps could be compromised to indicate that delays exist on routes that are clear, and vice versa, changing the actual travel path or vehicle of users accordingly.

The growth of open-source software brings with it interesting security concerns, as the bug-discovery process for both attackers and defenders is improved. Open-source software may be more secure since any eyes looking at the same code are more likely to find and patch a bug. However, open-source software may also present a risk, as attackers have an easier time discovering and exploiting the vulnerabilities. Payne [36] provides a more in depth review of the benefits and risks presented by open source software.

2.3.2. Electronic Ticketing and Mobile Fare Payment Systems

2.3.2.1. Electronic Ticketing

Overview

Electronic ticketing, or e-ticketing, is a broad term for ticketing systems that rely on any form of electronic device to provide proof of ticket purchase. Four generations of ticketing systems exist, often co-existing in the same city or agency, with the last three categorized as electronic ticketing: paper tickets or tokens, magnetic ticketing systems, contactless tickets, and mobile ticketing systems [37]. Due to the expected growth of mobile fare payment [38], mobile ticketing systems are discussed separately, in Section 3.2.2.

A survey from 2016 [3, p. 28] reports that 54% of the Florida agencies surveyed make use of magnetic stripe tickets or farecards and 15% use smart cards. Electronic ticketing systems “offer a large range of possibilities to make public transport easier to use, to manage and to control” [37, p. 8].

Implementation

Electronic ticketing systems can be either contact or contactless systems. Contact systems require the user to touch the ticket to a validation, typically by swiping or inserting a magnetic strip or contact smart card. Contact systems are mainly based on the ISO 7816 communication standards [37, p. 9].

Contactless systems allow a user to verify their ticket from a distance, and with little physical manipulation. Communication between the card and validation device is established via protocols such as Radio Frequency Identification (RFID), Near Field Communication (NFC) [39] or Bluetooth Low Energy (BLE) [40].

Security Considerations

Most attacks against electronic ticketing systems consist of breaking the device's cryptographic implementation, if the device uses cryptography, and copying or changing the values stored in the card. Students at MIT [41, 42] demonstrated such attacks on the magnetic swipe and RFID cards used by the Massachusetts Bay Transportation Authority (MBTA) fare collection system. The students discovered that the value of a ticket was stored locally on the card and could be changed, allowing an attacker to use the system free of charge.

Due to the widespread deployment of smart cards in fields such as payment, there are numerous papers reviewing the vulnerabilities of smart card technology. Smart cards employ cryptographic ciphers in their communications, for example using DES, AES, or RSA [43]. Abbott [44, p. 4] lists vulnerabilities that may be exploited to break the cryptographic implementations in smart cards, such as differential power analysis [45], timing attacks, reverse engineering of the embedded microprocessor, or flaws in the design or implementation of the card.

User privacy is also a concern in electronic ticketing systems. Kerschbaum et al. [46] describe how an attacker can retrieve a rider's travel records from the EZ-Link smart cards by scanning the card from a short distance. Kerschbaum et al. also present a privacy-preserving billing protocol. Sadeghi et al. [47] further describe potential attacks against electronic ticketing systems, such as impersonation and tracing, and analyze existing electronic ticketing systems.

2.3.2.2. Mobile Fare Payment and Ticketing Systems

Overview

Mobile fare payment is a form of contactless electronic ticketing that enables riders to purchase a ticket and validate the purchase using their mobile device. Mobile fare payment is typically added as an additional, more convenient fare payment option, rather than replacing existing options entirely [3, p. 36].

Mobile fare payment may reduce production and cash-handling costs [48, p. 6]. Passenger Transport [49] reported that First Bus' mobile fare payment system reduced boarding times by up to 75%.

Some mobile fare payment apps integrate trip planning and real-time information. The implementation details and security considerations presented in Section 3.1 apply to these systems as well.

Implementation

Mobile fare payment is commonly implemented using one, or a combination, of the following technologies: visual validation, *Quick Response* (QR) codes, *Near-Field Communications* (NFC), or *Bluetooth Low Energy* (BLE).

In a visual validation scheme, the user is provided an image on their mobile device that is shown to agency staff to verify their ticket purchase. Visual validation requires no additional equipment on the vehicle or station, and instead uses the data connection of the user's device for any necessary communication with a remote server [3]. Figure 2.2 shows an example of a screen from Token Transit [50], a mobile app used by some agencies for visual validation. The screen shows an image to the driver, as well as the time and word of the day, so they can visually authenticate the ticket.

QR codes [51] require QR scanners to be available on the vehicle or at the station and require a method for communicating with a remote server, such as Wi-Fi or cellular, for verification [3]. In a QR code system, a QR code is provided to the user on their mobile device upon purchase of their ticket. This ticket is then held under a QR scanner for verification [48].

Figure 2.2 Example of a visual validation screen from Token Transit [50]

NFC provides short range radio communication between the user's mobile device and the NFC device [52]. Unlike visual validation or QR codes, NFC requires the mobile device to support it with specific hardware. NFC is a contactless payment form in which users bring their devices into close proximity to the sensors, similar to RFID.

BLE is a low-energy implementation of Bluetooth [53]. BLE provides a larger communication range than NFC or RFID. This increased range allows mobile fare payment to be conducted in a *Be-In/Be-Out* (BIBO) style by detecting the device when the user passes through the gates or boards the vehicle [3], avoiding the constraint of passing the device by a sensor as in NFC.

Mobile fare payments are a relatively new technology, and little seems to have been published on their security concerns. However, related studies in other forms of payment may be relevant. Mobile fare payment shares the privacy concerns present in other forms of electronic ticketing described in Section 3.2.1. Kieseberg et al. [54] analyze the attack vectors generally present in QR codes. These include command injection, phishing, and other social engineering attacks.

Visual validation is potentially subject to replay attacks where an attacker records the screen and plays it back when showing the vehicle operator the ticket. Vendors implement animations to try to prevent such attacks, including showing a ticking clock with the time of day or additional information known by the vehicle operator, such as the color or word of the day. Implementation of the color or word of the day systems require daily information sharing with vehicle operators so they know the current color or word of the day. This information sharing can be accomplished via a display in a log-in screen used by vehicle operators, radio communication with a dispatcher, email, text message or other mode of information sharing. In any case, sophisticated attackers could create apps to run on mobile devices that would mimic any required animations, clocks, colors, or words, perhaps obtained from seeing other riders tickets or talking with operators.

Trojan horse applications, or applications that mislead users by masking their true intent, are another means of attacking mobile fare payment. Symantec researchers [55] have found malware that was spoofing Uber's Android application. When the users launched the malware and went through user authentication (e.g., entering a password), their account credentials were passed to the attacker. This malware attack prevents the user from easily discovering that their device has been compromised by redirecting the user to the page from the legitimate Uber app that shows their location. Given that there are increasing integration options between apps (e.g., Transit App links both to Uber for booking rideshare trips and fare systems for payment), the number of opportunities for malicious apps to capture data by masquerading as linked applications are also increasing.

2.3.3. Field Devices

Field devices are technologies that are found near roadsides or located outside a transit agency's building. Technologies reviewed here include traffic signal controllers and traffic signal preemption/priority, dynamic/variable message signs, closed circuit television and surveillance equipment, and onboard Wi-Fi.

2.3.3.1. Traffic Signal Controllers and Traffic Signal Preemption/Priority

Overview

Traffic signal controllers are responsible for managing traffic signals at intersections. Traffic signal controller security has been the subject of many research endeavors in recent years, possibly due to the criticality of these systems.

Traffic Signal Preemption and *Traffic Signal Priority* (TSP) decreases the time transit vehicles, such as buses, spend waiting at traffic lights by facilitating movement through the intersection [56]. TSP may reduce transit delay and travel time, and improve reliability.

Implementation

Traffic signal controllers store pre-programmed timing controls programmed by an operator using an interface on the front of the controller. This interface typically consists of a screen and several buttons that allow the operator to interact with the controller and update the timing. The pretimed controls consist of a series of fixed phases that define the currently active signals at any given time, which continuously run in a cycle [57]. Many modern traffic signal controllers also allow for actuated control based on data received from a variety of sensors, potentially allowing for more efficient traffic flow.

Modern traffic controllers are becoming increasingly operator friendly, with colored displays and touch screen support, Web browser-based interfaces allow remote programming and observation and may support connected-vehicle technologies [58]. Traffic controllers are also becoming increasingly connected [59], communicating over private networks back to the agency monitoring the intersection and to other traffic signal controllers in the area.

Traffic Signal Preemption and Traffic Signal Priority, while often addressed together, are different processes [56]. Traffic Signal Preemption interrupts the normal traffic cycle (e.g., changing a light to red for a train approaching an intersection), while Traffic Signal Priority modifies the normal cycle (e.g., reducing the time until a bus waiting at a traffic light gets a green signal). However, the equipment used to implement these technologies is the same at a high level and this paper does not distinguish between them further.

TSP often consists of the following equipment: detector units located on the utility poles, *Priority Request Generation* (PRG) equipment, and the *Priority Request Server* (PRS) located in the traffic signal cabinet [60]. The most common triggering method seen in the literature is an infrared detector unit and *mobile infrared transmitters* (MIRTs). These requests are processed by the PRS and passed to the traffic signal controller. TSP may use GPS and AVL systems to detect oncoming transit vehicles or a combination of GPS and infrared. GPS offers better information regarding bus trajectory [61, p. 3]. Wireless cellular phones are also seen in the literature as an alternative to infrared [62].

Security Considerations

Field devices, such as traffic signal controllers, are met with unique physical cybersecurity challenges. Physical access to the equipment can be readily obtained by an attacker willing to take the risk to do so (tampering with traffic control devices is a criminal violation by Florida Statute 316.0775 [63]). Keys for the traditional #2 key/lock cabinet standard can be purchased online, and a duplicated key has been used in Florida to change traffic signal timings [64].

With the new connected features discussed earlier, physical access to the equipment presents a cybersecurity risk. While entirely preventing physical access is infeasible, there are several mechanisms that can be employed to prevent or detect access, such as locks, alarms, and cameras. Electronic locks, which use RFID or similar technology, provide more management over access to the traffic cabinets than traditional locks by allowing contractors to be given temporary access and logging access information such as time and the accessor's ID [65].

Traffic signal controllers are also susceptible to remote attack. Ghena et al. [66] created a program that allows an attacker on the network to remotely trigger any of the buttons on the controller and display the output. With this capability, an attacker can insert malicious logic statements or modify light timings. Ghena et al. discovered this attack by reverse engineering the communication protocol used by the traffic controller configuration software. The protocol required no authentication and did not use encryption. Default usernames and passwords were used on the devices, allowing attackers to gain access to the devices.

Due to the lack of authentication and encryption, traffic signal controllers are also sensitive to falsified data. Cerrudo [67, 68] showed that fake traffic detection data can be sent to traffic signal controllers to influence their behavior and cause them to accept incorrect options when setting the configuration. By conducting a simulation, Ghafouri et al. found that severe congestion can be caused by falsified data and compromised sensors [69]. Laszka et al. developed a "polynomial-time heuristic algorithm for computing approximately optimal attacks" [70, p. 1], that is, an algorithm for efficiently identifying the critical signals that have the greatest impact for creating congestion.

The most frequently cited concern for TSP in the literature is the unauthorized triggering of the TSP sensors. The TSP sensors may be triggered by unauthorized personnel who have purchased or created their own MIRT. Newer TSP sensors are being designed to only respond to signals that transmit an authorized serial number and provide logging capabilities to track misusage [71]. As new methods for TSP, such as GPS/AVL or mobile, become more prominent, other concerns may begin to surface in the literature.

2.3.3.2. Dynamic/Variable Message Signs

Overview

A Dynamic Message Sign (DMS) serves as the primary means of communication between agencies and en route motorists. DMSs are used by transit agencies to display estimated arrival times and delays at transit stations [72]. The information is often displayed in real-time, and updates may be scheduled by operators. While many DMSs are permanent installations found beside or above highways, some are temporary and transported to various locations to provide communication [73, 74].

Implementation

The hardware behind a DMS depends on several aspects, including the matrix display type and the display technology. A student handbook created by the Washington State Department of Transportation [73] provides an introduction to the hardware inside a DMS.

A typical DMS offers several different methods for locally and remotely updating the message being displayed. Updating the DMS locally can be performed through two primary means: a laptop brought by the operator and connected via a RS-232 serial port, or a user interface on the DMS that provides a display screen and input controls to the operator [73]. Providing a user interface lessens the need for manufacturer software that would be installed on a laptop, but a user interface may not always be present in older DMS devices.

A DMS device may be accessed remotely through a variety of connection types, such as radio, cellular dial up lines, or by dedicated lines. DMS devices that support cellular dial up have a dedicated phone number that can be used to access them [73]. Some DMS devices are now Internet-enabled over IP, allowing any device with Internet browser support to login and manage the DMS device [75].

Security Considerations

Florida is one of the top states in term of number of DMS intrusions, alongside other high-population states including Texas and California [76]. Attacking a DMS and modifying the message has become a popular prank. Online guides [77] have been published on the Internet giving detailed instructions on how a layperson can change the message of these signs. These issues still persist today [78] and reflect the lax security practices expressed in *Protection of Transportation Infrastructure from Cyber Attacks: A Primer* [1].

Figure 2.3 A compromised DMS from an online guide on exploiting DMSs [77]

The online guide [77] lists a number of security issues present with DMS devices and how they can be taken advantage of. Figure 2.3 presents a compromised DMS found in the online guide's gallery of compromised DMSs [77]. These issues include unused locks on the DMS trailer or cabinet, unused or default passwords, and the ability to easily reset the sign to the factory default password with a simple sequence of keystrokes. DMS devices have also been attacked remotely over an Internet connection [79, 80].

2.3.3.3. Closed-Circuit Television

Overview

Closed-circuit television (CCTV) provides agencies the ability to monitor their equipment and assists in incident response. Many CCTV systems are combined with other technologies such as Automatic Vehicle Location, silent alarms and radio communications [81]. CCTV cameras can be found in a variety of locations, including on vehicles, stops, stations, and at ticketing machines.

CCTV and video surveillance offer several benefits to transits agencies, such as deterring and detecting crimes, risk management for fare evasion, and providing information to investigate reported crimes or complaints [82]. CCTV may reduce transit worker assaults and "was considered the most effective technology by survey participants in the prevention of operator assaults" [83, p. 39].

Implementation

CCTV may be monitored in real time or used for forensic investigation [82]. The American Public Transportation Association (APTA) created a recommended practice [84] for the use of CCTV systems by transit agencies. The recommended practice reviews functional requirements, camera specifications, screen image specifications for personal identification, and maintenance. CCTV may be combined with AVL systems or GPS to determine exact locations of incidents.

Many CCTV systems support wireless connections and may be accessed remotely, providing real-time streaming via cellular networks. Cameras may be managed from this remote

connection via web applications, allowing viewing and management from a variety of platforms, including smartphones. Some CCTV solutions provide the ability to wirelessly transfer video files to storage upon return to the vehicle depot or other designated location [82].

Security Considerations

Costin [85] provides a review of the threats, vulnerabilities and mitigations related to CCTV and surveillance cameras. The different attacks described include visual-layer attacks, covert-channel attacks, denial-of-service attacks, and jamming attacks. Costin also discusses vulnerabilities in online video surveillance systems. Default credentials were used by 39.72% of online cameras [86], allowing attackers to gain access to these systems.

Shodan [87], an online search engine for *Internet of Things* devices, can be used by attackers to quickly discover systems connected to the Internet. These devices could then be scanned for vulnerabilities. Costin [85, p. 49], using Shodan, revealed more than 2.2M Internet-connected surveillance systems produced by more than 20 distinct vendors.

CCTV and surveillance systems that allow users to manage their systems through web applications may be susceptible to typical attacks found in web applications. Users should ensure that default credentials are not used on this system. Organizations such as the Open Web Application Security Project (OWASP) [34] provide a wealth of information on vulnerabilities in web applications.

Researchers from Google [88, 89] found a vulnerability in computer-vision systems, such as transit security cameras, that have “smart” analytics to detect objects or people within video streams. The Google team was able to create stickers with patterns that can deceive *artificial intelligence* (AI) algorithms used in computer vision. These pictures and patterns are known as adversarial images. The stickers can be downloaded and printed out with ease. Security systems could potentially be rendered inert and fail to detect objects or individuals.

2.3.3.4. Onboard Wi-Fi

Overview

Onboard Wi-Fi offers transit passengers the ability to wirelessly connect to the Internet using a mobile device, such as a smartphone or laptop. This addition makes transit options more attractive to riders.

Implementation

Internet connection for onboard Wi-Fi is often established using cellular data networks, which is extended to users via a wireless access point on the bus [90]. Due to the increased usage and resulting deterioration of the quality of service of cellular networks, the cellular connection may be supplemented by accessing other Wi-Fi access points when they are available [91].

Security Considerations

The survey of Florida agencies conducted as part of this project revealed that agencies perceive onboard Wi-Fi to have the highest susceptibility of attack but on average was also considered one of the least critical systems deployed in public transit, presumably because most agencies offer Wi-Fi as an amenity to transit riders but that same Wi-Fi is not used in operations. However, two agencies indicated that Wi-Fi was critical to their operations, indicating that it was used for a purpose other than passenger access to the Internet (e.g., loading new schedule and headsign data onto vehicles when they are in the yard, transferring APC data from the vehicle to agency servers). The agencies did not specify if the same Wi-Fi system used for critical operations was also used for passenger Internet connectivity, or if these were two separate systems.

User privacy is the primary concern for public Wi-Fi expressed in the literature. Gupta and Jha [92] provide an analysis of the potential attacks that a wireless network may be susceptible to, including Man-in-the-Middle (MITM) attacks and rogue access points. These techniques allow an attacker to eavesdrop on a user's connection, or masquerade as the user.

If the onboard Wi-Fi is physically connected to a system with access to the *Controller Area Network* (CAN) [93] of the vehicle, an attacker could potentially gain access to CAN [94]. However, no references in existing literature were found that presented a successful attack on a transit vehicle CAN via onboard Wi-Fi.

2.3.4. Operations and Fleet Management

Transit agencies may improve the efficiency of operations and fleet management by employing Computer Aided Dispatch, Automatic Vehicle Location, and Automated Passenger Counters.

2.3.4.1. Computer-Aided Dispatch and Automatic Vehicle Location

Overview

Automatic Vehicle Location (AVL) systems allow transit agencies to track the location of a vehicle in real time. AVL technology serves two primary purposes for transit agencies: providing internal fleet management and sharing vehicle information with riders. Potential benefits of such technology include an increase in ridership and providing better customer satisfaction by increasing the perception of service reliability [24].

Computer Aided Dispatch (CAD) systems work closely with AVL technologies to provide transit agencies the ability to manage their fleets in real time, including tracking transit routes, trip orders and vehicle assignments. CAD systems provide similar benefits to AVL technologies, increasing the reliability of the service and performance tracking [95, 96].

CAD and AVL systems are often distributed as a single package by vendors [97] and are often referred to as CAD/AVL systems. CAD/AVL systems may also be packaged with components of real-time passenger information systems for the benefit of riders in addition to the agency. In this case, the implementation and security considerations discussed in the Real-time Passenger Information Systems section could also apply to a "CAD/AVL" package deployed at an agency.

Implementation

AVL systems in the past made use of a variety of techniques to determine the current location of the vehicle such as dead-reckoning, but modern AVL systems primarily rely on Global Positioning Systems (GPS). The data from the GPS is communicated to the transit agency, often in conjunction with the Computer Aided Dispatch. AVL systems consist of onboard computers, the GPS and mobile data communications [1]. The mobile data communications may be through the area's cellular network through standards such as the *Global System for Mobile communications* (GSM) or through local user-based radio.

Security Considerations

Researchers were able to successfully take complete control of the *Controller Area Network* (CAN) of a passenger vehicle, granting the researchers complete control of the vehicle [94]. The researchers attacked the cellular communication features available in the van. The vulnerabilities described are viable at a large scale, and the cost of discovering and exploiting such a vulnerability was classified as "Medium-High" [94]. Theoretically, onboard WiFi could also be used in place of cellular communications to gain access to the vehicle network if the systems are physically connected. No prior research was found exploring the possibility of such an attack on transit vehicles, but similar vulnerabilities may exist in the mobile communication systems used in CAD/AVL systems and onboard vehicle network (i.e., the CAN standard is used across both commercial and consumer vehicles [93]). Due to the similarities, such an attack is believed to be theoretically possible, although there appears to be no public evidence of successful attacks.

CAD/AVL systems have been affected by other vulnerabilities seen in IT systems. In Baltimore, Maryland, the police CAD system was brought down for 17 hours after being attacked with ransomware. Attackers entered the network after changes were made to the firewall during troubleshooting unrelated to the CAD system. The IT team in Baltimore were able to isolate and contain the ransomware, limiting the spread to other systems on the network [98].

2.3.4.2. Automated Passenger Counters

Overview

Automated Passenger Counters (APCs) record the number of passengers that board and disembark from a vehicle. A survey conducted in 2008 [99] found that APCs are primarily used to collect ridership data for a given route (including tracking ridership changes), but many agencies also use this data to evaluate performance at individual stops as well as adjusting schedules

based on ridership [99, p. 1]. APCs may be integrated with other technologies such as the Automatic Vehicle Location system to provide additional benefits (e.g., tracking the exact time and location of boardings and alightings) [100].

Implementation

APC devices collect ridership data using several methods, including infrared beams, treadle mats, passive thermal, digital cameras with three-dimensional vision technology software, thermal imaging, ultrasound, and light beam [100]. Regardless of the collection method, APCs will typically consist of a standalone sensor or a microcomputer that processes and stores the data from a series of sensors located at each of the entrances to the vehicle.

For a standalone sensor, data is retrieved locally from the sensor using standard connections such as USB or Ethernet. In a more sophisticated APC system, data may be stored and retrieved locally or transmitted via a Wi-Fi or cellular connection to a remote destination, such as the agency or a cloud provider.

Security Considerations

No papers were found that discussed the security of APCs in detail. This may be due to the APC not being directly accessible via wireless connection; APCs are commonly connected to the Wi-Fi or GPRS module by Ethernet, and it may be simpler to attack the Wi-Fi or GPRS module directly. APC devices that provide these modules or support wireless connections to these modules may be susceptible to attack, including indirectly over a connected vehicle network.

The raw sensors used by APCs (e.g., infrared) could also theoretically be attacked (e.g., jammed to prevent counting, or intentionally triggered even when passengers are not boarding or alighting to erroneously over-count riders). Because federal funding is allocated to transit agencies based in part on ridership data [101], and agencies must validate their use of APC data for National Transit Database ridership reporting every three years, corrupted APC data could potentially force the agency to use an alternate means of reporting ridership until the APC data could be proved to be reliable again when the next validation year arrives [102].

2.3.5. Emerging Technologies

Connected and autonomous vehicles are emerging technologies that could potentially revolutionize the transportation system, but are not yet widely deployed.

2.3.5.1. Connected Vehicles

Overview

Connected vehicle (CV) technology is a broad range of technologies that enable vehicles to communicate with other vehicles, the road infrastructure, and the Internet. CVs improve the driving experience by providing advanced knowledge of the environment to the driver.

Applications include Intelligent Driver-Assistance Systems (IDAS) [103], Vehicle-to-Infrastructure (V2I) safety, and Vehicle-to-Vehicle (V2V) safety [104].

In September 2016, the USDOT initiated the Design/Build/Test phase of the Connected Vehicle (CV) Pilot Deployment Program [105], providing over $45 million to Wyoming [106], New York City [107], and Tampa [108] to begin building connected vehicle programs. The Tampa Connected Vehicle Pilot aims to provide services such as rush hour collision avoidance, wrong way entry prevention, improved pedestrian safety, traffic-flow optimization, bus priority, and streetcar safety.

The survey of Florida agencies conducted as part of this project also revealed that CVs are deployed in the Lakeland Area Mass Transit. The Gainesville Regional Transit System, Jacksonville Transportation Authority, Hillsborough Area Regional Transit Authority, Palm Tran, and Bay County Transportation Planning Organization are considering deploying CVs.

Implementation

There are a variety of communication classifications for CVs, such as Vehicle-to-Infrastructure (V2I), Vehicle-to-Vehicle (V2V), Vehicle-to-Cloud (V2C), Vehicle-to-Pedestrian (V2P), and Vehicle-to-Everything (V2X) [109]. Connected vehicles communicate using a variety of protocols including IEEE 802.11p Wireless Access in Vehicular Environments (WAVE) [110, 111], GPS, cellular, Bluetooth [53], and Wi-Fi. Kenney [112] describes in detail the WAVE protocol, a dedicated short-range communications (DSRC) standard for V2V communications in the United States.

Security Considerations

CV wireless communications may become a key target of cyber attacks on CV deployments. Attackers may use their own vehicles and infrastructure or the vehicles and infrastructure of others to connect to transit-agency equipment.

Hausermann [113] created an infographic that summarizes all of the potential attack surfaces into one image. Mobile applications, infotainment systems, and the onboard diagnostics (OBD) port are marked as high-threat areas. This marking aligns with the reports by Koscher et al. [114] and Checkoway et al. [94], which describe how these systems can be exploited to gain full control of the vehicles.

Koscher et al. [114] found several vulnerabilities that allowed the researchers with physical access to CVs to gain full control of the vehicles. Checkoway et al. [94], in a continuation of the previous paper, provide an analysis of several *remote* attacks that can be used to gain full control of the vehicles. While agencies may not have direct control over the CV implementations in vehicles that they procure, agencies should be aware of these attacks due to their potential for abuse, both from an agency's own transit vehicles and from public vehicles that communicate

with agency equipment. Additionally, any equipment and networks connected to networks accessed by the CV could also be vulnerable.

Researchers from the University of Michigan [115] analyzed congestion attacks on traffic-signal controls based on connected vehicles. Their attack model assumes that attackers can send malicious messages from the connected vehicle to the *Intelligent Traffic Signal System* (I-SIG). Under this assumption, they found that congestion attacks, in which an attacker attempts to create congestion by sending falsified data to the I-SIG system, were highly effective, increasing the delay by as much as 68.1% [115, p. 2].

Privacy concerns are also present in connected vehicles. Elmaghraby and Losavio [116] present a range of privacy issues present in smart cities, many of which are relevant to connected vehicles. Location data is remarked as being a potential key security concern [116, p. 494]. In February, 2016, security researcher Troy Hunt posted on his blog [117] a detailed analysis of a vulnerability in the Nissan Leaf. This vulnerability allowed an attacker to retrieve information about a vehicle over the Internet, as well as allowing the attacker to change conditions in the vehicle, such as temperature. This information included start and stop times and was caused by an insecure web application programming interface (API).

2.3.5.2. Autonomous Vehicles

Overview

Autonomous vehicles (AVs) are vehicles that provide automated control over at least one safety-critical control function, such as steering, without user input [118]. There are various levels of automation, ranging from not automated to fully automated.

Litman [119] provides an analysis of the potential benefits and costs of autonomous vehicles. While a detailed description of the benefits and costs are outside the scope of this paper (especially as the benefits are often contested in the literature), relevant areas considered in Litman's document include driver stress, productivity, cost, and safety.

Autonomous vehicles have been deployed in Florida by transit agencies. An autonomous shuttle is being tested in downtown Gainesville and is currently performing mapping of the streets [120]. Autonomous shuttles are also under consideration by Tampa [121] and Babcock Ranch [122]. The survey of Florida agencies conducted as part of this project revealed that AVs are deployed in the Gainesville Regional Transit System, Jacksonville Transportation Authority, and Miami Bridge Youth & Family Services. In addition, the Collier Area Transit, Pinellas Suncoast Transit Authority, Hillsborough Area Regional Transit Authority, University of South Florida (USF), and Broward County Transit are considering deploying AVs.

Implementation

SAE J3016 [123] was chosen as the official reference for the levels of vehicle autonomy by the USDOT [124]. The five levels are: no automation (Level 0), driver assistance (Level 1), partial automation (Level 2), conditional automation (Level 3), high automation (Level 4), and full automation (Level 5) [123].

An AV is composed of many onboard sensors, enabling the vehicle to navigate in an environment with unknown obstacles. These sensors include "laser, radar, *light detection and ranging* (LiDAR), GPS and computer vision systems" [125, p. 82].

The range of sensors and computer vision systems in an AV allow the vehicle to develop detailed 3D maps of the environment and track static and dynamic objects. The unknown environment, and the vehicle's location in that environment, is mapped by the system in a process known as *Simultaneous Localization and Mapping* (SLAM) [126]. The initial mapping provides the system with a base to compare future data against, enabling the system to better distinguish between static and dynamic objects and make smart decisions about the environment around it [127].

Security Considerations

As with connected vehicles, AVs may have vulnerabilities similar to those discovered by Checkoway et al. [94] if wireless access to the vehicle is enabled, allowing an attacker to gain remote control of the vehicle. Wyglinski et al. [125] provide an analysis of the attack surface present in an autonomous vehicle and rate the importance of the systems in the vehicle. The Navigation Control Module (NCM) is rated as the most critical system, followed by the engine and electronic brake control modules.

As discussed earlier in the CCTV section, Google researchers [88, 89] found a vulnerability in computer vision systems. The Google team was able to create stickers with patterns that can deceive artificial-intelligence algorithms used in computer vision with adversarial images. If adversarial images (e.g., stickers) were placed on traffic signs or other objects or people in the vehicles line-of-sight, autonomous vehicles using computer vision systems could potentially take unexpected actions (e.g., hard braking, swerving, or ignoring traffic signs, objects, or people).

The underlying sensors used by AVs are also vulnerable to *spoofing*, where signals are falsified or modified to confuse the vehicle into detecting an object or person where one doesn't actually exist. Security researchers demonstrated that a LiDAR system on an AV could be forced to falsely detect pedestrians and cars using off-the-shelf equipment costing around $60 [128]. These spoofed signals could force an AV relying on LiDAR to sit still to avoid hitting the phantom object or potentially perform evasive actions at high speeds to avoid a collision that would not actually occur [129]. Considering that LiDAR is considered a vital ingredient in most AV systems [130], LiDAR-based vulnerabilities may prove to be a primary cybersecurity concern in AV deployments. Petit et al. also demonstrated spoofing and blinding attacks on the cameras

present in autonomous vehicles and provide countermeasures for spoofing and blinding attacks, including by building redundancy into the sensors and their control systems [128]. GPS is also susceptible to spoofing [131].

2.4. Summary

A review of the literature related to technologies deployed in public transportation found known vulnerabilities in CVs, AVs, electronic ticketing systems, traffic signal controllers, traffic signal priority, DMS. No known vulnerabilities were found in the literature for AVL/CAD systems, online trip planners, mobile fare payment, onboard Wi-Fi, CCTV, and APCs, but given their complexity, their wide attack surfaces, and the known vulnerabilities in related technologies, we believe that it is reasonable to expect that security vulnerabilities do exist in these technologies as well.

CHAPTER 3: SURVEY

3.1. Background and Objectives

Transit agencies have improved their operational and financial performance with the deployment of modern technology, such as mobile applications, AVL, and onboard Wi-Fi. Because increasingly more functions in public transportation rely on connected computers, attackers have a larger attack surface to exploit. This section of the report summarizes the results of a survey designed to capture information about technologies deployed and being considered by Florida transit agencies.

The survey questions can be categorized into four areas:

1. **Existing Transit Technologies in Use** – The technologies transit agencies have deployed and are considering deploying.
2. **Planned Deployment of AVs/CVs** – Whether agencies have deployed, or are considering deploying, Autonomous Vehicles (AVs) and Connected Vehicles (CVs).
3. **Data Storage and Security** – The types of data agencies collect, whether and how that data is backed up, and whether that data is shared with other organizations.
4. **Real and Perceived Risk of Breaches of Security** – Agencies' experience in, and concerns about, cyber-attacks.

Section 3.2 describes the methodology of the survey design, Section 3.3 presents the results, and Section 3.4 discusses the results. Section 3.5 concludes and discusses how the survey results serve the larger research project.

3.2 Survey Design and Methodology

3.2.1. Survey Design

The survey was designed as an online survey using SurveyMonkey. Conditional logic was used so that respondents only had to answer follow-up questions relevant to information they had already provided. Appendix B contains the compilation of the 25 questions from the study.

After preliminary questions about participants' contact information (Questions 1-2), the survey addresses the following four areas:

1. **Technologies deployed by the agency (Questions 3 and 6-13)** – These questions sought information about deployed technologies (Question 3), their vendors (Question 6), and technologies being considered for deployment (Question 7). There were also questions

asking participants to evaluate the likelihood of the technologies being attacked and the technologies' operational and financial importance (Questions 8-13). Appendix B shows the initial order of the questions. Although the survey went live on May 7, 2018, Question 6 was moved to the end of the survey on May 9, 2018 because six of 13 initial participants stopped the survey on that question. The research team hypothesized that individuals stopped completing the survey because they did not know the answer to Question 6. Moving this question to the end of the survey may have encouraged respondents to complete more of the survey before stopping.

The responses to these questions help identify the most common technologies used by Florida transit agencies, and those technologies' vendors. The obtained information will help facilitate information exchange between transit agencies and cybersecurity researchers to help identify and mitigate vulnerabilities in transit systems.

2. **The current scope of AV and CV deployment (Questions 4-5 and 14-17)** – Questions 4-5 asked whether the responding agencies have deployed AVs or CVs.

   An attack on these technologies may have a more significant impact than on other technologies. Therefore, the survey paid special attention to this area.

   If the agencies have not deployed AVs or CVs, they were asked whether they are considering deploying AVs or CVs in the future. If they were considering deploying AVs or CVs, they were asked to estimate when that deployment may occur.

3. **Agencies' data-management techniques (Questions 18-23)** – The transit agencies were asked to identify the types of data they keep, where the data is kept, and how frequently the data is backed up.

   The goal of these questions was to assess the availability of back-up data for the agency, as backups are needed to recover from many phishing and ransomware attacks.

4. **Agencies' experience in encountering cyber-attacks and their concerns (Questions 24-25)** – The agencies were asked to identify any known attacks and the challenges for implementing good computer-security practices.

3.2.2. Survey Methodology

The priority group for the survey were technical staff at Florida transit agencies who are responsible for cybersecurity. The research team identified 33 individuals across 33 agencies as technical contacts for those agencies. The team compiled this list by combining contact information of IT personnel retrieved from general contact information provided by CUTR's bus

safety and security review team and from a contact list provided by each FDOT District Office of Modal Development. A master list containing the technical contact list along with the member lists of the Florida Transit Safety and Operations Network (FTSON) and Florida Rural Transit Assistance Program (RTAP) groups was created. Individuals affiliated with an organization outside of Florida were removed from the list, as were individuals affiliated with any organization that did not operate transit service, which left a total of 318 email addresses on the master list.

The Florida Department of Transportation (FDOT) sent an initial email with a link to the survey (Appendix A) on May 7, 2018, to the master list as well as to the Florida Transit Planning Network (FPTN) email list. The original deadline for completing the survey was May 18, 2018. Due to a low response rate (14 individuals), FDOT sent a reminder email (Appendix A) on May 21, 2018, to the master list, extending the deadline until May 25, 2018. The USF research team also followed up with personally addressed email to the agency personnel who were on the technical contact list who had not yet replied. In the case of emails that returned a response saying the email address was no longer valid, the research team found alternate contacts for those agencies from CUTR staff who have worked with those agencies in the past and forwarded the reminder to those new email addresses.

3.3. Results

A total of 37 Florida transit agencies responded to at least one question in the survey. Twelve responses were omitted from consideration for the following reasons: duplicating another response from the same agency (four responses were in this category; only the most recent response was kept), originating from a non-transit agency (three responses were in this category), or providing contact information but no responses to technical questions (eight responses were in this category). Three responses were in multiple categories; one response was a duplicate with no responses to technical questions, two were from non-transit agencies who didn't respond to technical questions.

Of the remaining 25 agencies, 23 agencies completed the survey, and another two answered at least one technical question (specifically regarding the technologies deployed at the agency). The remainder of this report discusses the responses from these 25 agencies. Of the 25 responses, 18 were from the agencies on the technical contact list, while the remaining seven were from the other emails lists (FTSON, RTAP, or FTPN). The 25 agencies who responded to at least one technical question in the survey were:

- Bay County TPO
- Broward County Transit
- Calhoun County Senior Citizens Association, Inc.
- Citrus County Transit
- Collier Area Transit
- Council on Aging of Clay County
- Gainesville RTS

- Hillsborough Area Regional Transit
- Hernando County Transit Management, Inc.
- Jacksonville Transportation Authority
- Key West Transit – City of Key West
- Lake County
- Lakeland Area Mass Transit
- Lee Tran
- Martin County BOCC
- Miami Bridge Youth & Family Services, Inc.
- Ocala/Marion TPO/SunTran
- Palm Tran
- Pasco County Public Transportation
- Pinellas Suncoast Transit Authority
- Sarasota County Area Transit
- South Florida Regional Transportation Authority
- Space Coast Area Transit
- StarMetro
- University of South Florida

3.3.1. Transit Technologies in Use

Figures 3.1-3.9 and Tables 3.1-3.4 show results of the first group of questions that discussed deployed technologies. The value of N (shown in the figures or their captions) is the number respondents who answered the given question.

Figure 3.1 shows the percentage of agencies that have deployed each technology (Question 3). Here CAD/AVL stands for Computer Aided Dispatch/Automatic Vehicle Location; APC for Automatic Passenger Counter; TSP for Traffic Signal Preemption/Priority; and SPAT for Signal Phasing and Timing.

Two agencies entered technologies in the “Other” answer field for deployed technologies:

- Automatic Vehicle Monitoring (AVM)
- GPS and Rastrack S.A.S

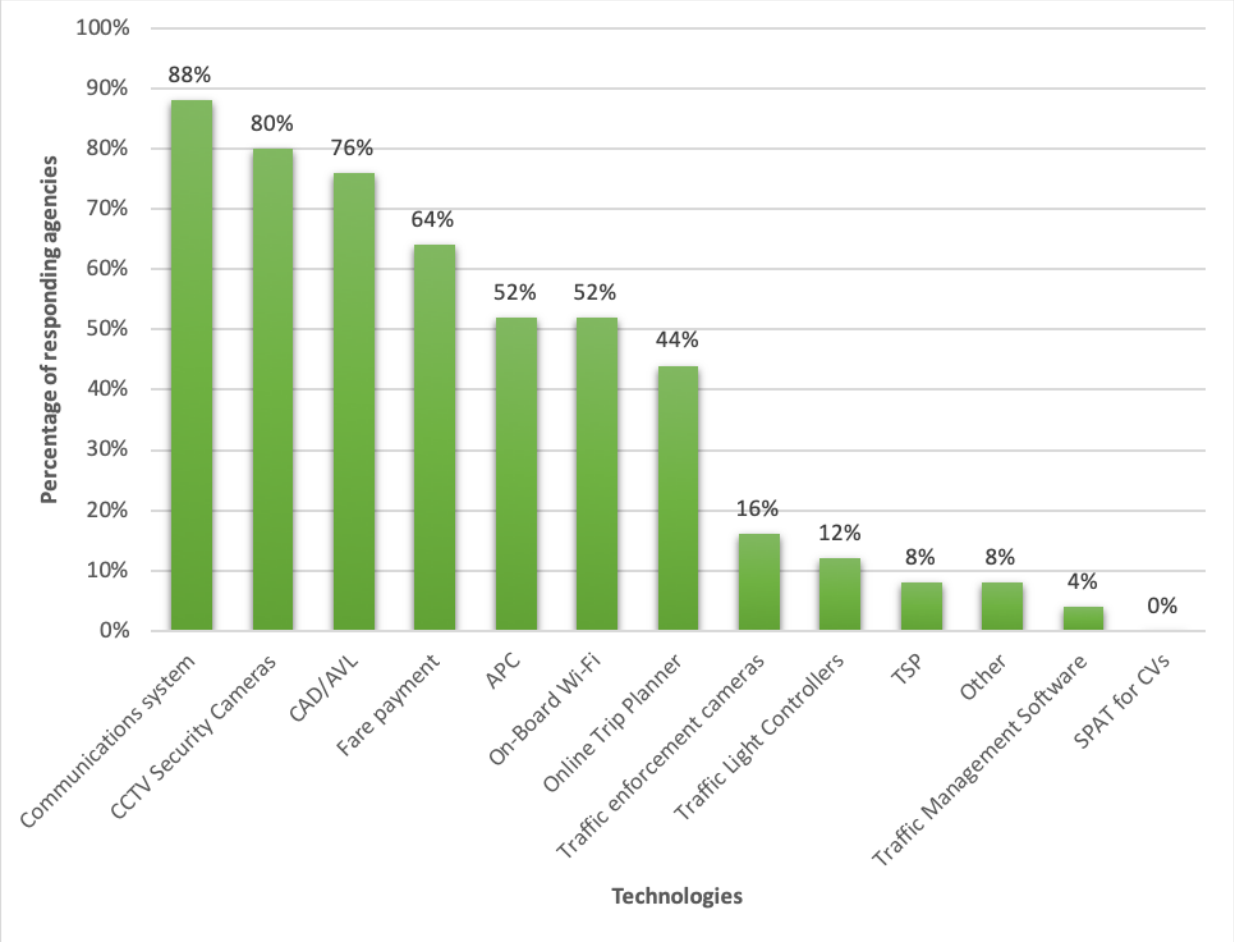

Figure 3.1 Technologies deployed at participating agencies (Q3). N = 25

Figure 3.2 illustrates which vendors supply the participant agencies with the technologies selected in Question 3. The vertical axis shows how many times each vendor was mentioned in the answers. There were in total 30 vendors for the 19 agencies who responded to this question.

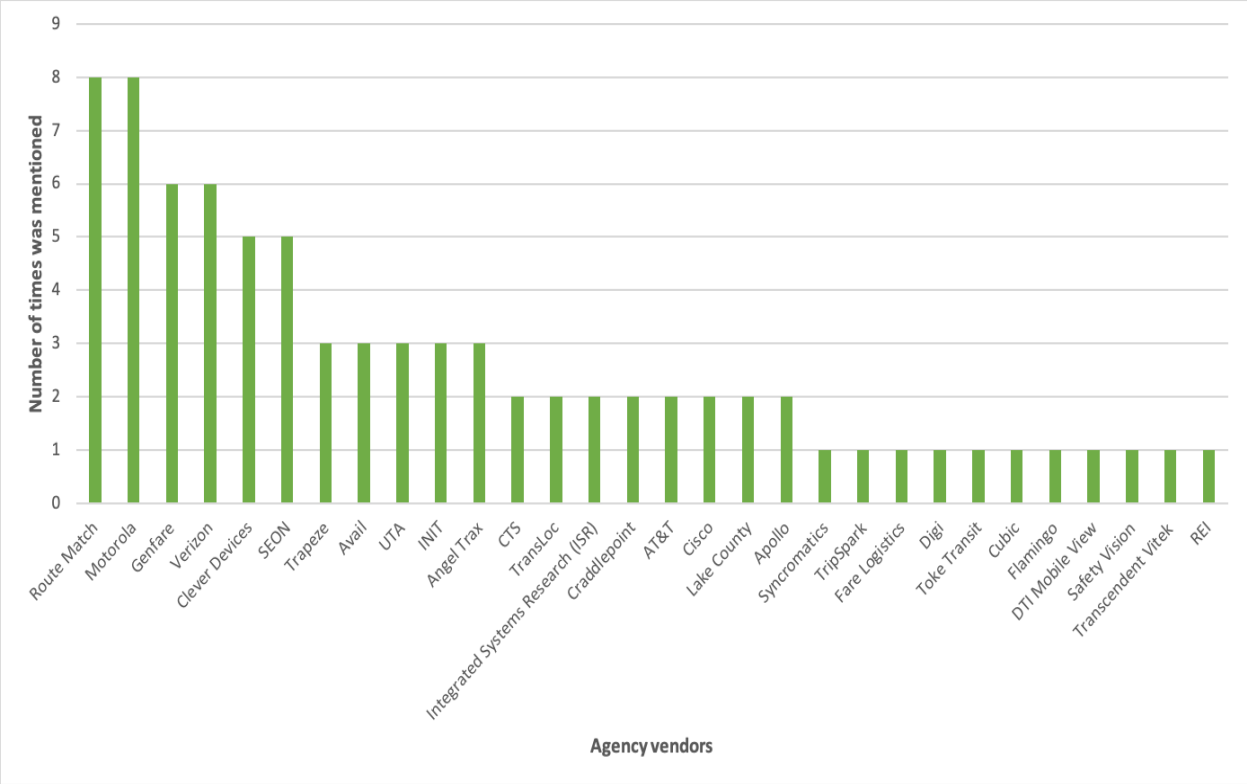

Figure 3.2 Florida transit agency vendors (Q6). N = 19

Table 3.1 The most-deployed technologies by transit agencies and their vendors

Technology name	Response rate	Vendors
Communication systems (such as regular radio, VoIP)	88%	Motorola, Verizon, Cisco, Lake County
CCTV Security Cameras (such as on-vehicle cameras)	80%	SEON, Angel Trax, Apollo, DTI Mobile View, Safety Vision, Transcendent Vitek, REI
CAD/AVL	76%	Route Match, Clever Devices, Trapeze, CTS, Integrated Systems Research, Syncromatics, TripSpark, Verizon, TransLoc, Avail
Fare payment (such as on-vehicle and/or mobile app, ticket vending machine)	64%	Genfare, INIT, Toke Transit, Cubic, Flamingo, Avail
Onboard Wi-Fi	52%	Verizon, AT&T, Cradlepoint, Cisco, Digi, Route Match
APC	52%	UTA, Route Match, Genfare, Avail, Fare Logistics

Table 3.1 shows the vendors for the most widely deployed technologies. Figure 3.3 shows the technologies that are under consideration by agencies for deployment (Question 7). Respondents were only able to choose from technologies they have not yet deployed when answering this question. Three agencies entered values in the "Other" field:

- Annunciators
- Mobile ticketing for fare payment
- New fare solution

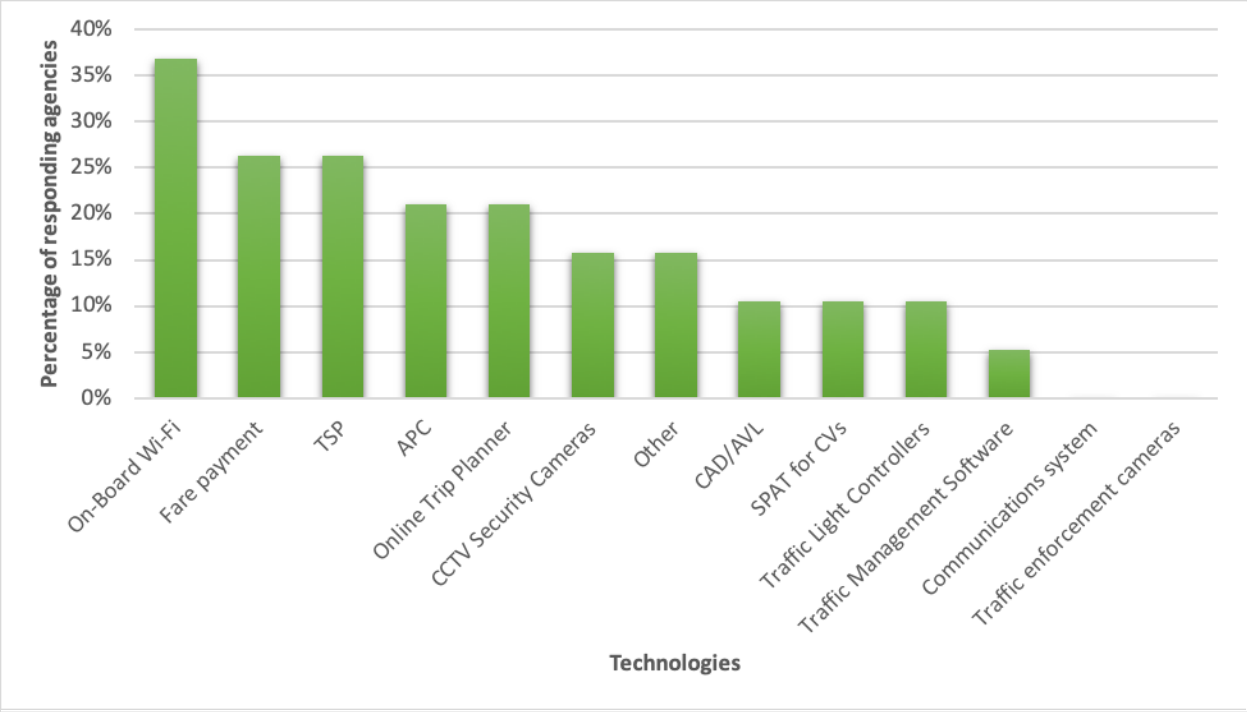

Figure 3.3 Technologies under consideration by transit agencies for deployment (Q7). N = 19

Table 3.2 and Figure 3.4 show the results obtained by merging the answers to Questions 8 and 9. These questions asked participants to provide the perceived probability of deployed (Question 8) and considered (Question 9) technologies being susceptible to attack, using a scale of "Very unlikely", "Somewhat unlikely", "Somewhat likely", and "Very likely". Responses were assigned the following numeric values:

- Very unlikely – 1
- Somewhat unlikely – 2
- Somewhat likely – 3
- Very likely – 4

Table 3.2 Agencies' perceived probability of deployed and considered technologies being susceptible to attack (Q8, Q9).

Technology name	Very unlikely	Somewhat unlikely	Somewhat likely	Very likely	Total responded
Onboard Wi-Fi	1	3	5	7	16
Fare payment	5	5	6	5	21
CCTV Security Cameras	10	6	3	2	21
CAD/AVL	11	4	3	2	20
TSP	1	1	3	2	7
Communications system	11	5	3	1	20
APC	9	3	2	1	15
Online Trip Planner	7	3	3	1	14
Traffic Light Controllers	1	1	1	1	4
Traffic Enforcement Cameras	0	1	1	1	3
SPAT for CVs	1	0	1	0	2
Traffic Management Software	1	0	0	0	1

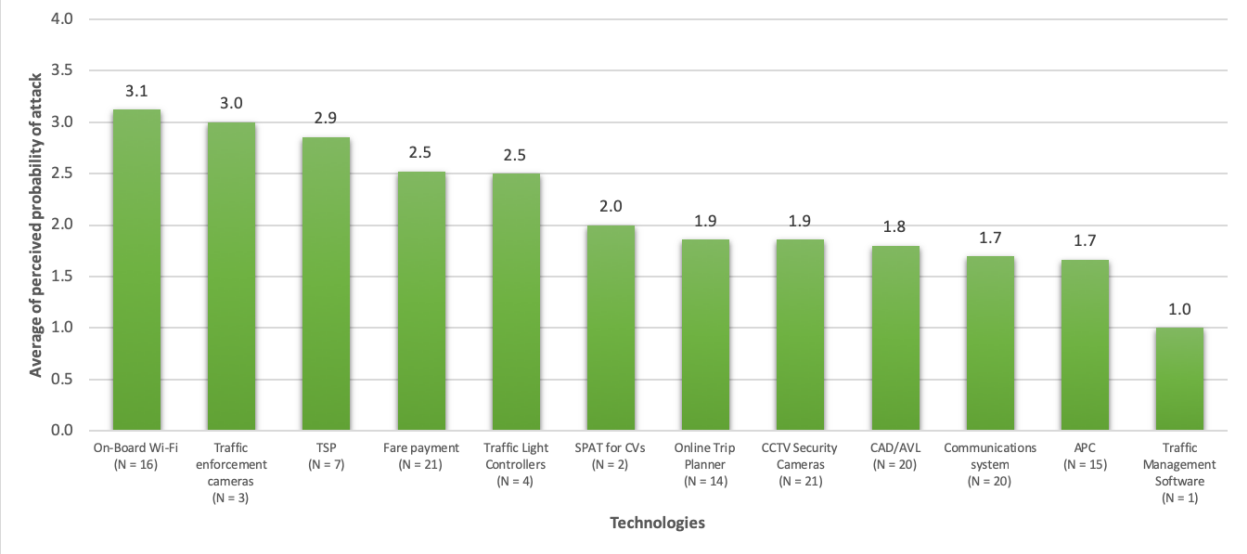

Figure 3.4 Average of agencies' perceived probability of deployed and considered technologies being susceptible to attack (Q8, Q9).

A similar approach was used to aggregate the answers to questions that asked the agencies to evaluate how critical deployed and considered technologies are from operational and financial perspectives. Table 3.3 and Figure 3.5 show the importance level of these technologies from an *operational* perspective. Table 3.4 and Figure 3.6 do the same, but from a *financial* perspective. Responses were assigned the following numeric values:

- Not critical – 1
- Somewhat critical – 2
- Moderately critical – 3
- Very critical – 4
- Extremely critical – 5

Table 3.3 Agencies' perceived operational criticalness of deployed and considered technologies (Q10, Q12).

Technology name	Not critical	Somewhat critical	Moderately critical	Very critical	Extremely critical	Total responded
Communications system	0	0	2	7	11	20
CAD/AVL	0	3	1	6	10	20
CCTV Security Cameras	0	0	3	8	9	20
Fare payment	0	1	6	8	6	21
APC	1	2	4	4	4	15
Online Trip Planner	1	2	2	5	4	14
Onboard Wi-Fi	7	3	5	1	1	17
Traffic Light Controllers	0	0	1	2	1	4
TSP	0	2	3	2	0	7
Traffic Enforcement Cameras	1	1	1	0	0	3
SPAT for CVs	0	0	2	0	0	2
Traffic Management Software	0	0	1	0	0	1

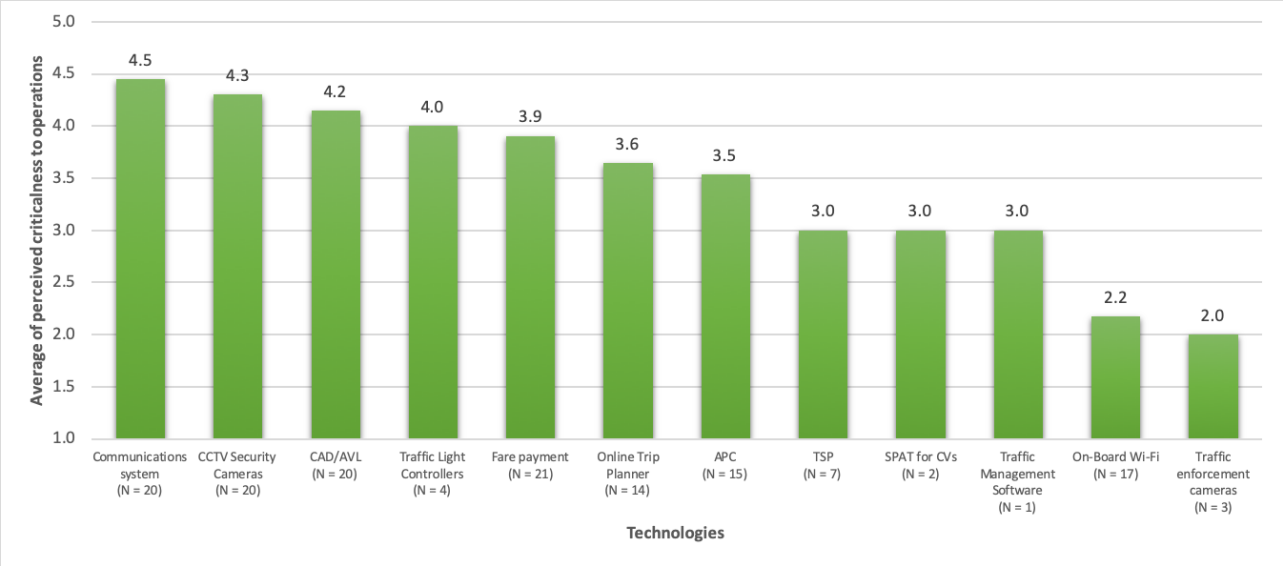

Figure 3.5 Average of agencies' perceived operational criticalness of deployed and considered technologies (Q10, Q12).

Table 3.4 Agencies' perceived financial criticalness of deployed and considered technologies (Q11, Q13).

Technology name	Not critical	Somewhat critical	Moderately critical	Very critical	Extremely critical	Total responded
Fare payment	1	1	2	6	11	21
CCTV Security Cameras	1	3	4	4	9	21
Communications system	1	3	4	4	8	20
CAD/AVL	1	4	6	5	4	20
Online Trip Planner	1	4	4	1	4	14
APC	0	3	6	5	2	16
Onboard Wi-Fi	8	5	3	1	1	18
TSP	0	3	3	1	0	7
Traffic Light Controllers	0	2	2	0	0	4
Traffic Enforcement Cameras	1	1	0	1	0	3
SPAT for CVs	0	0	2	0	0	2
Traffic Management Software	0	0	1	0	0	1

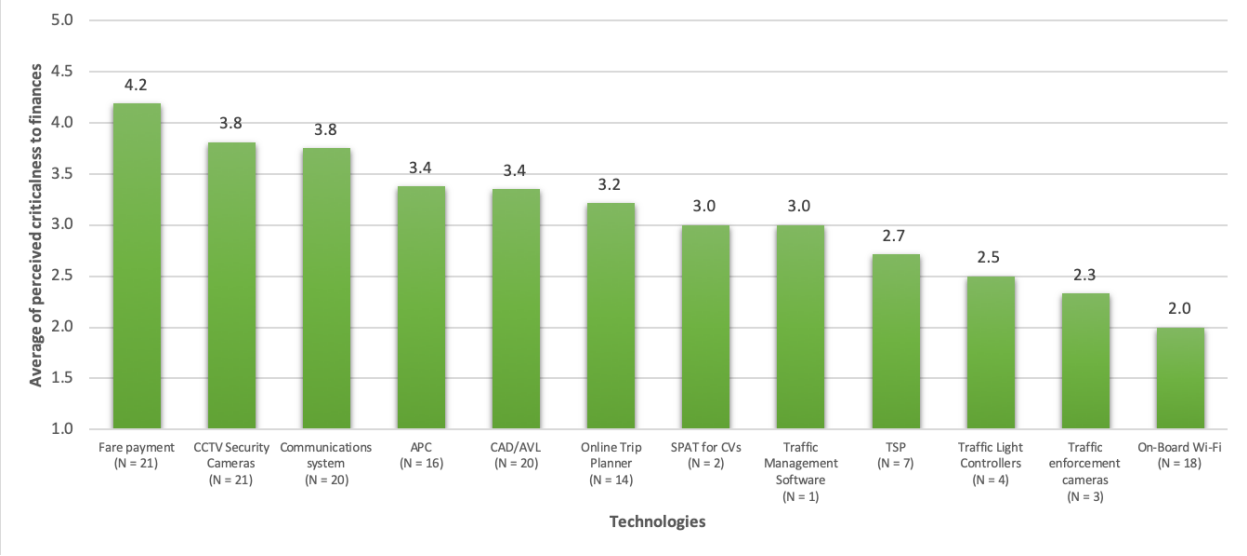

Figure 3.6 Average of agencies' perceived financial criticalness of deployed and considered technologies (Q11, Q13).

Figures 3.7-3.9 provide the results for the same questions as Figures 3.4-3.6, but for the technologies that were entered in the "Other" field. Because these "Other" responses were unique to a single agency, each bar in Figures 3.7-3.9 represents the response of just a single agency (i.e., N=1 for each technology category).

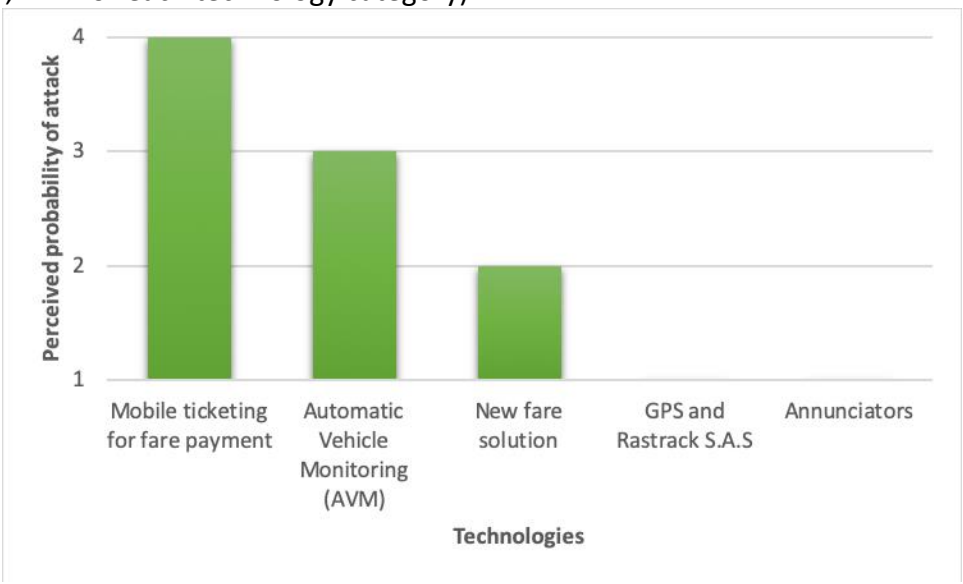

Figure 3.7 Agencies' perceived probability of "other" technologies being susceptible to attack

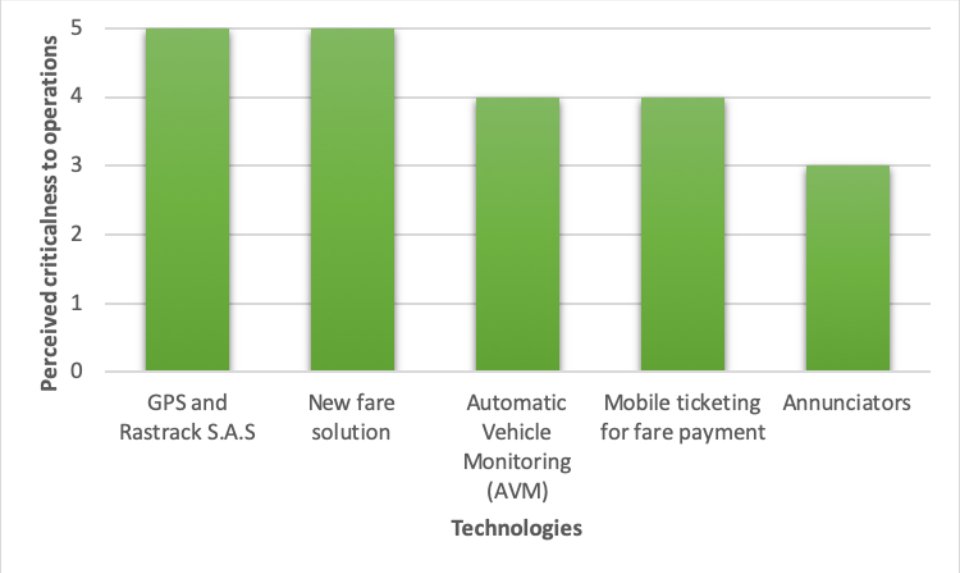

Figure 3.8 Agencies' perceived operational criticalness for "other" technologies.

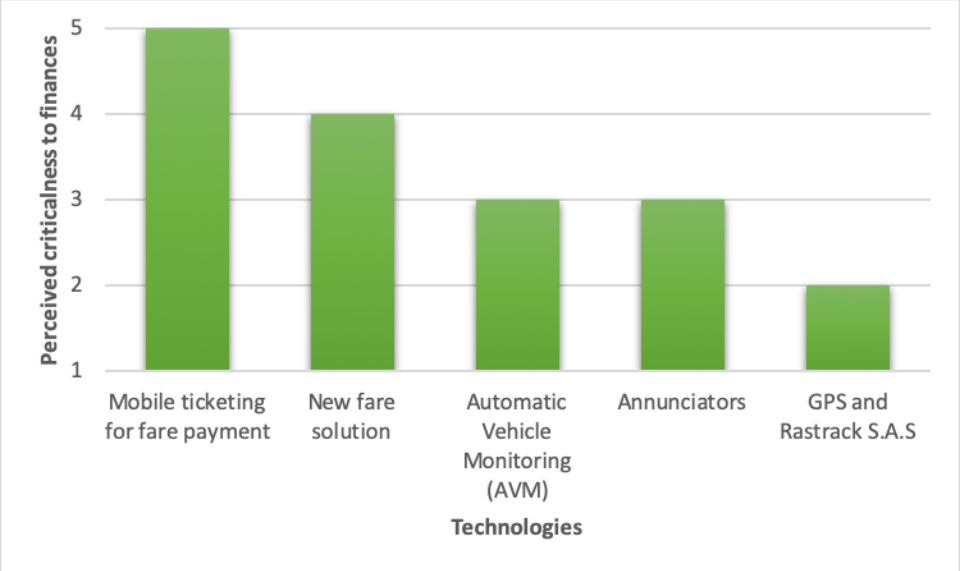

Figure 3.9 Agencies' perceived financial criticalness for "other" technologies.

3.3.2. Planned Deployment of AVs and CVs

Figures 3.10-3.16 present the results to the second area of cybersecurity questions regarding AVs and CVs. Figures 3.10-3.11 show the responses to the questions regarding the deployment of AVs and CVs (Questions 4-5). Of the 25 participating agencies, three (12%) have deployed AVs, and one (4%) has deployed CVs.

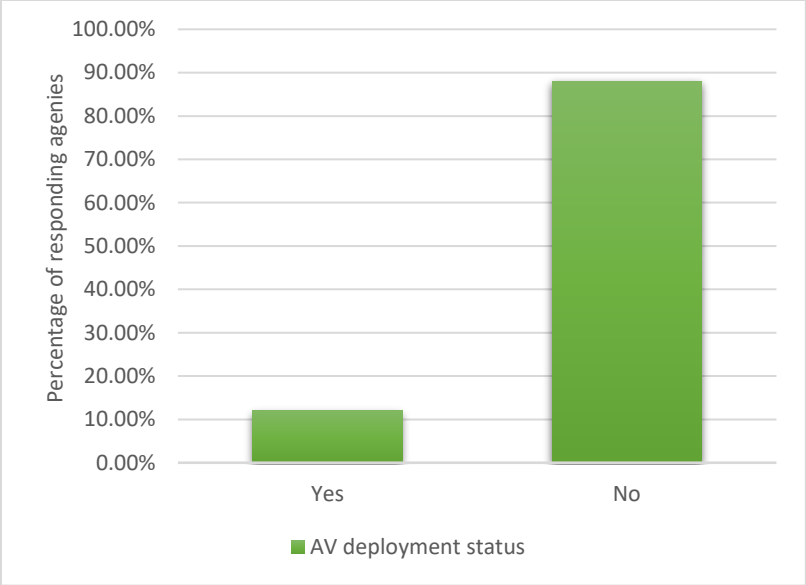

Figure 3.10 Deployment status of autonomous vehicles in transit agencies (Q4). N = 25

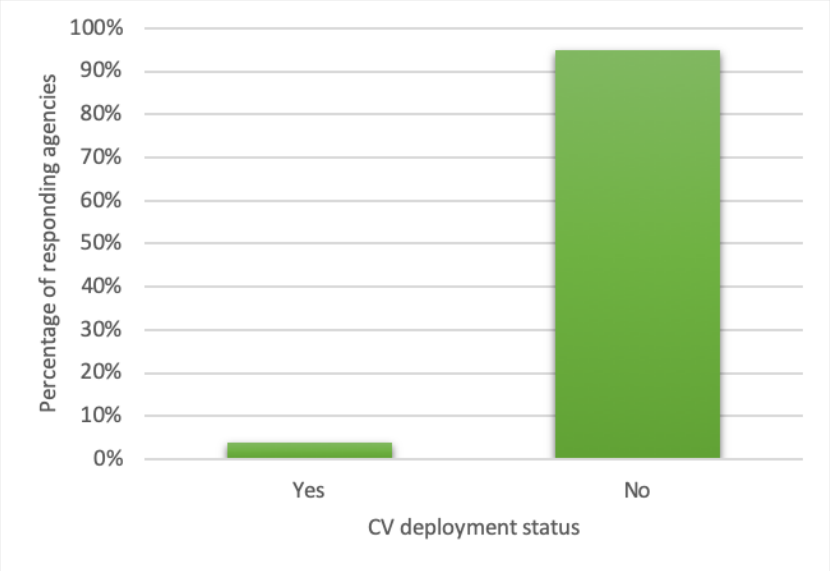

Figure 3.11 Deployment status of connected vehicles in transit agencies (Q5). N = 25

Participants who have not deployed AVs and reached Question 14 were asked whether they are considering deploying AVs. The participants who were considering using AVs were asked to specify the expected timeframe for deployment (Question 15), with the results shown in Figures 3.12 and 3.13.

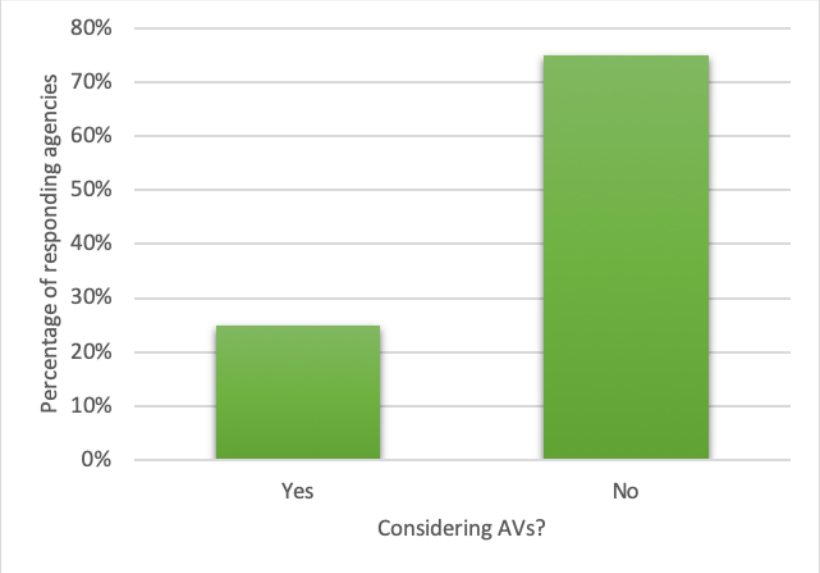

Figure 3.12 Number of agencies that are considering AV deployments (Q14). N = 20

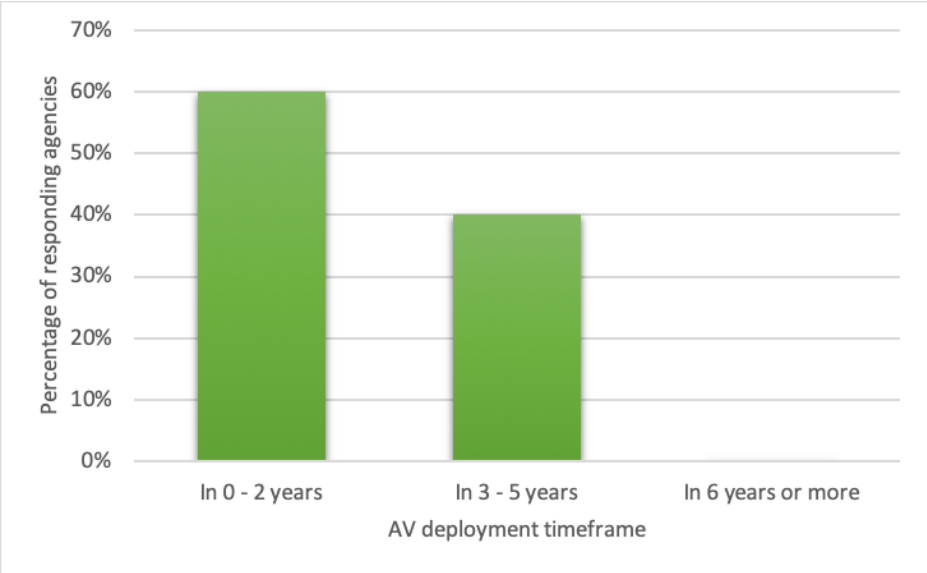

Figure 3.13 Timeframe for considered AV deployment (Q15). N = 5

Questions 16-17 asked for similar information, but for CVs instead of AVs. The results are shown in Figures 3.14-3.15.

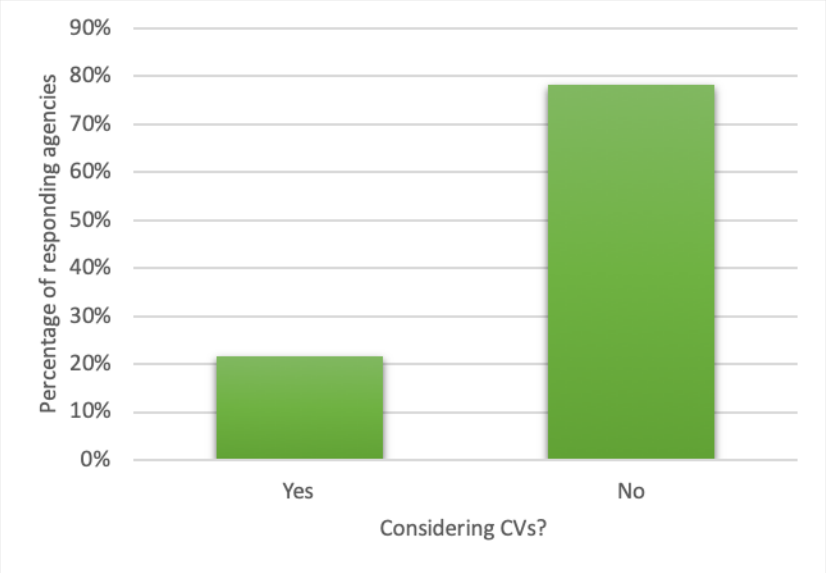

Figure 3.14 Number of agencies that are considering CVs deployments (Q16). N = 23

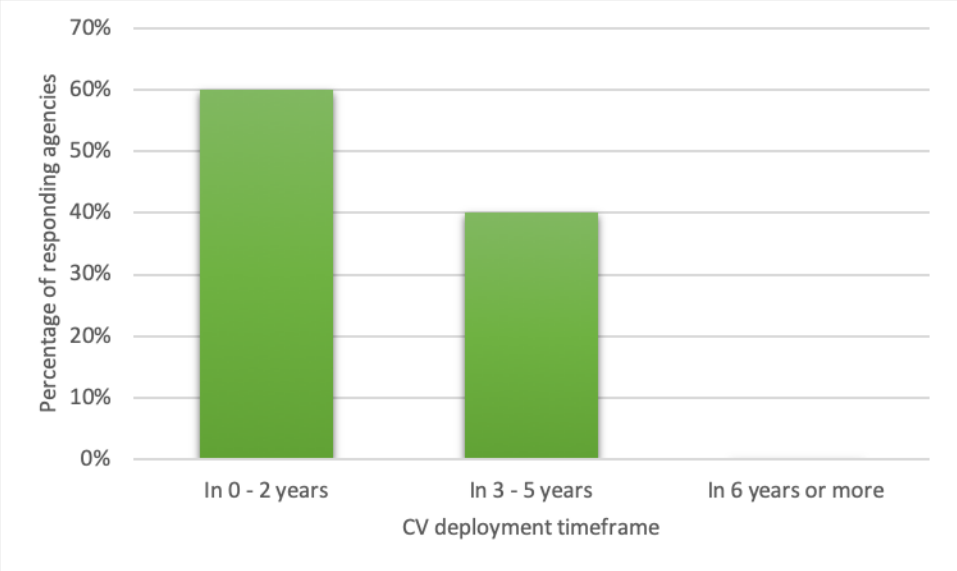

Figure 3.15 Timeframe for considered CV deployment (Q17). N = 5

3.3.3. Data Security

The results for the questions regarding agencies' data management are shown in Figures 3.16-3.21. Figure 3.16 shows the percentage of agencies that collect or store each data type (Question 18).

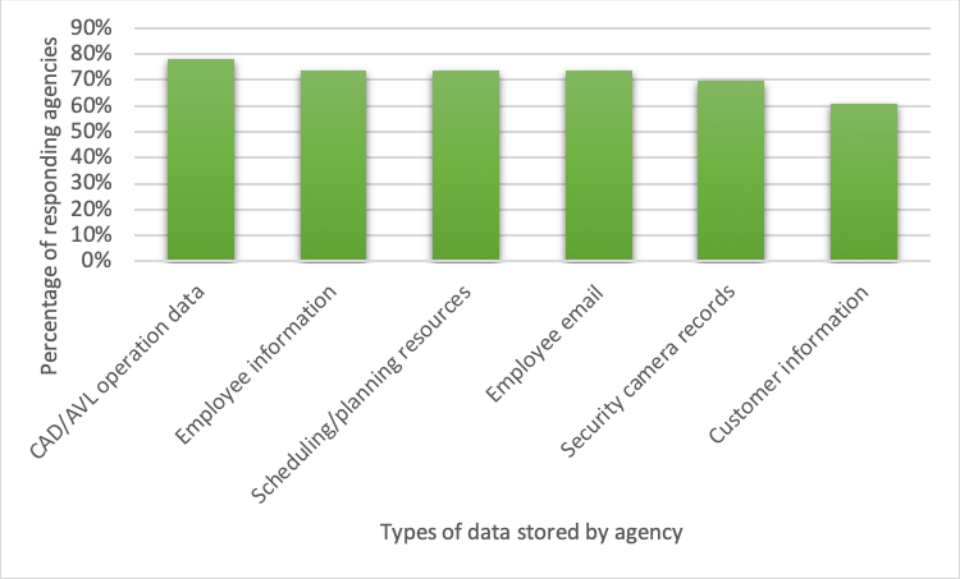

Figure 3.16 Data types collected or stored by transit agencies (Q18). N = 23

Figures 3.17-3.19 show the percentage of each of the selected data properties:

- Kept in local storage, cloud storage, or both (Question 19)
- Shared with any third party or not (Question 20)
- Encrypted or not (Question 21)

The values of the results in Figures 3.17-3.19, for each data type, represent the percentage of agencies who mentioned collecting that data type in Question 18.

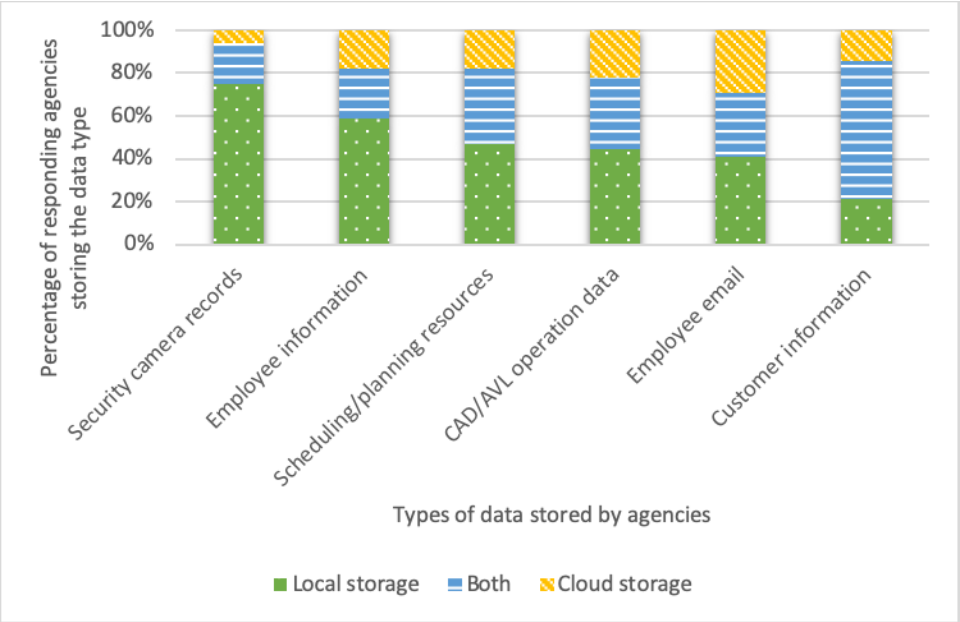

Figure 3.17 Transit agency data storage locations (Q19). N = 23

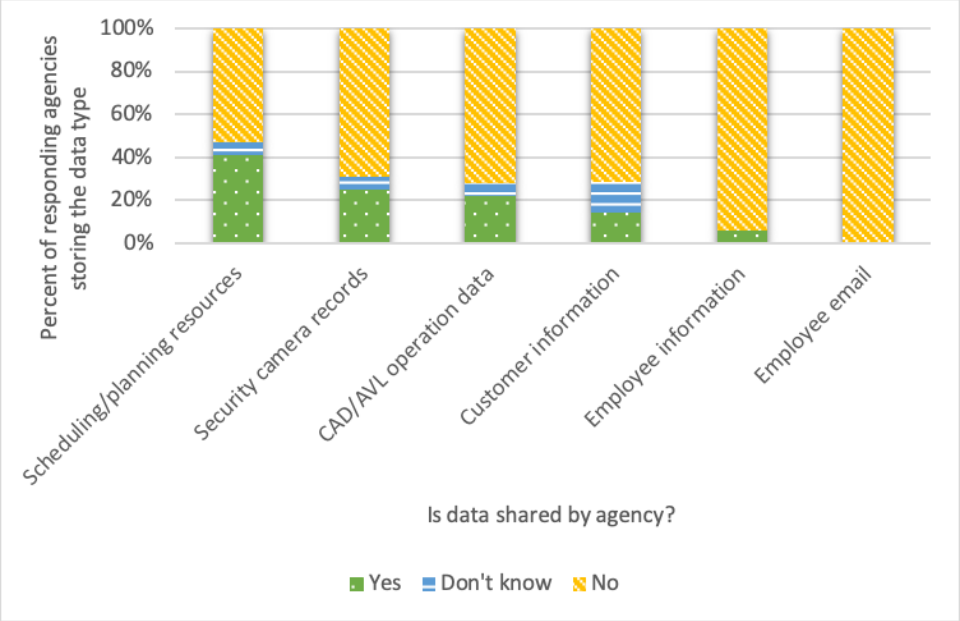

Figure 3.18 Transit agency data-sharing practices (Q20). N = 23

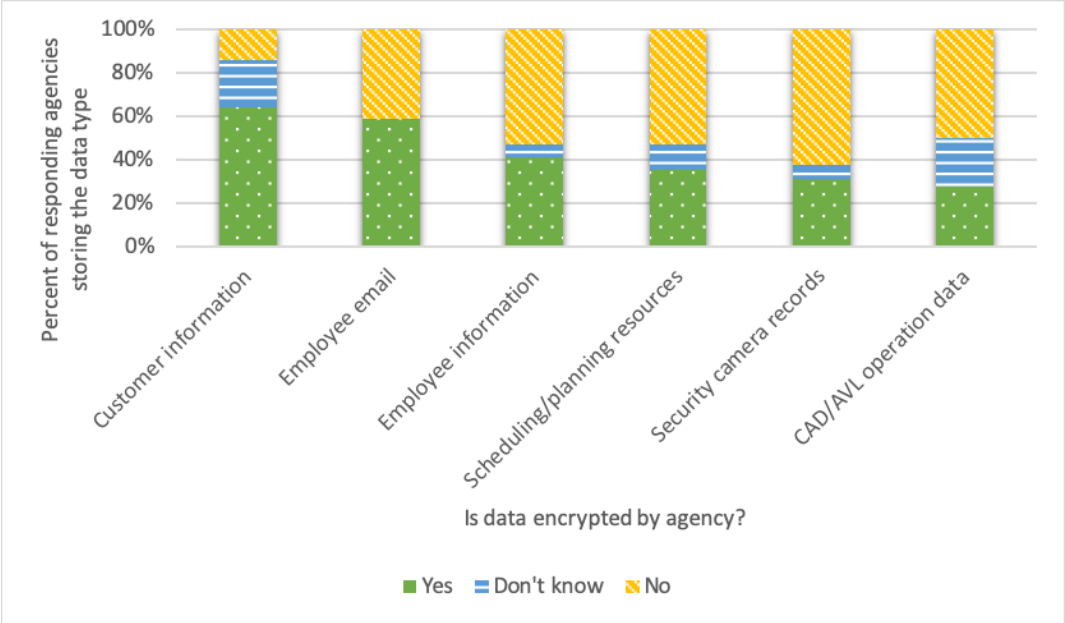

Figure 3.19 Transit agency data encryption practices (Q21). N = 23

Figures 3.20-3.21 show how frequently the agencies make backups for each type of data they collect and for how long they keep those backups. The values of the results in Figures 3.20-

3.21, for each data type, represent the percentage of agencies who mentioned collecting that data type in Question 18.

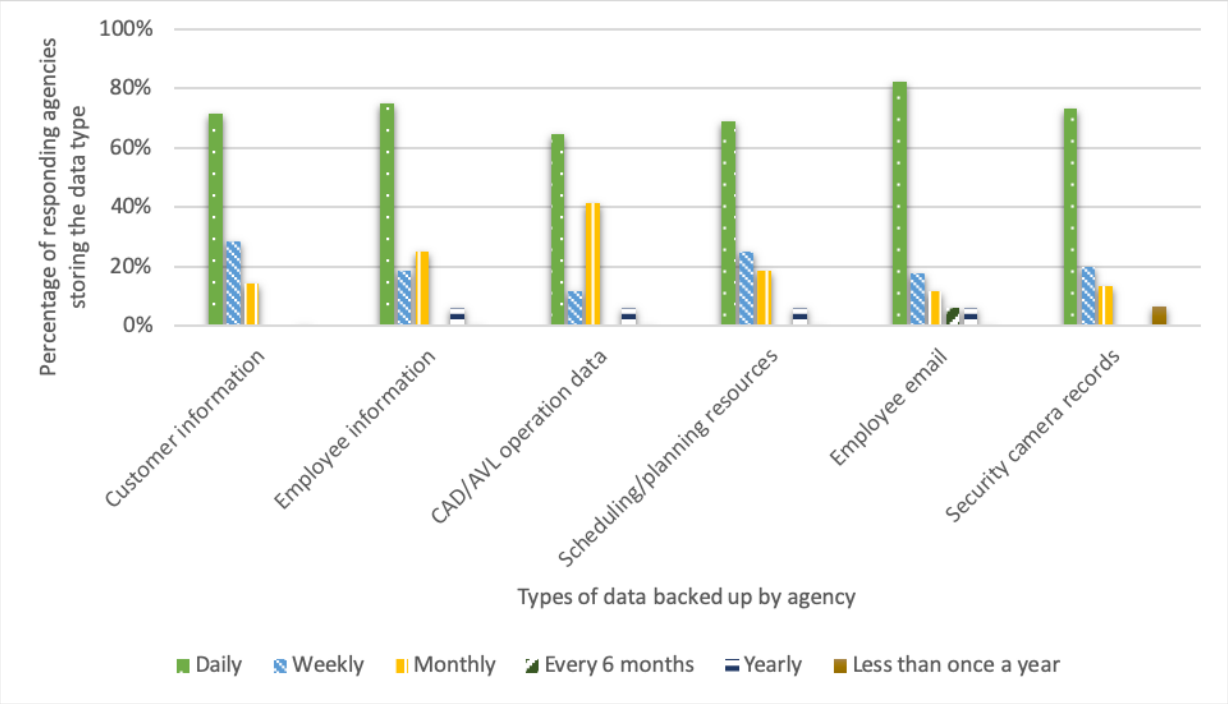

Figure 3.20 Transit agency data backup frequencies (Q22). N = 23

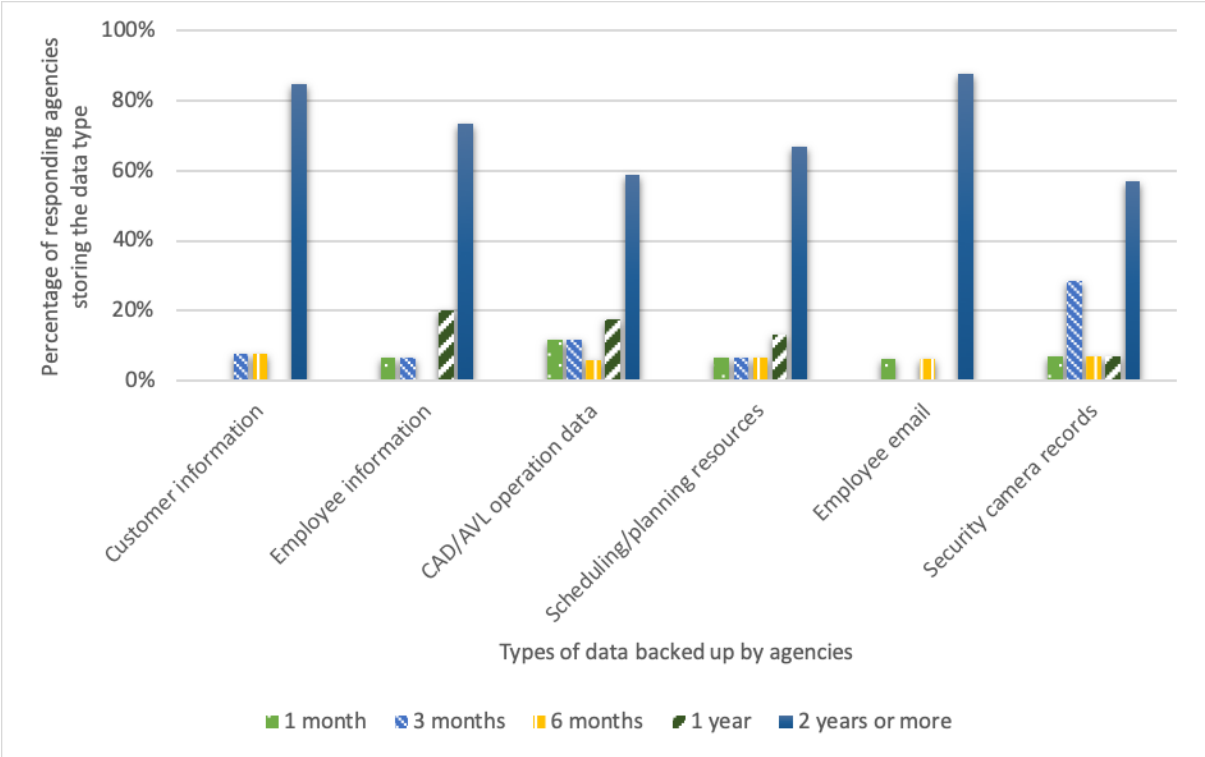

Figure 3.21 Transit agency backup-data retention times (Q23). N = 22

3.3.4. Past Cybersecurity Incidents and Challenges

For Question 24, regarding whether agencies or their vendors have been affected by cybersecurity issues in the past, responses were categorized into “Yes”, “No”, and “Don’t Know”. The results are shown in Figure 3.22.

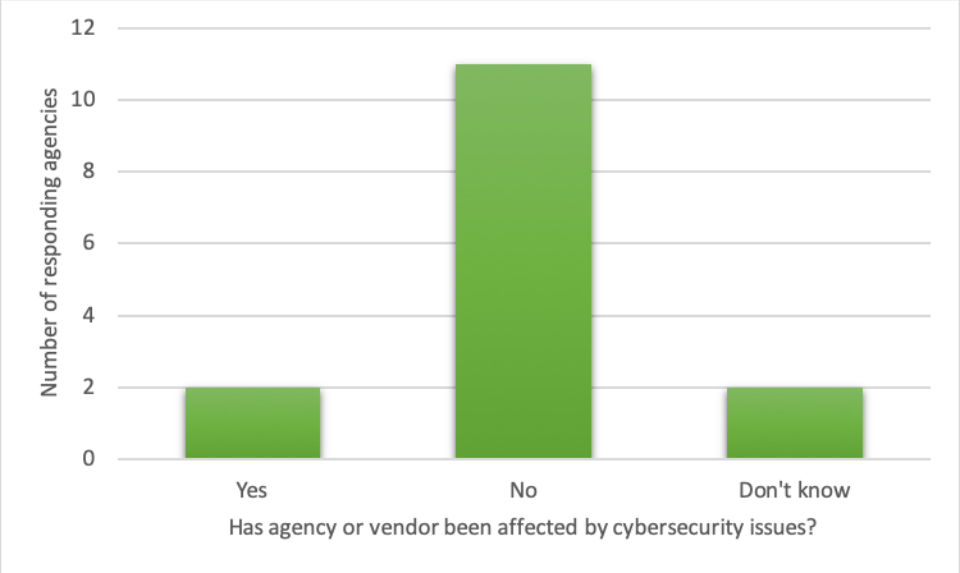

Figure 3.22 How many agencies or their vendors have been affected by cybersecurity issues (Q24). N = 15

Question 25 asked the respondents to specify the challenges for implementing good security at their agencies in an open text response. The answers were combined into four categories: Cost, Employee training, Other, and No challenges (Figure 3.23). The “Other” category includes four responses:

- “The ability to find a vendor that can meet the Buy America requirement.”
- “Building & bus video system that stays up to date.”
- “Simplicity with the end users.”
- “Third party software.”

Figure 3.23 Challenges that prevent implementing good security at transit agencies (Q25). N = 12

3.4. Discussion

3.4.1. Transit Technologies in Use

Not surprisingly, as shown in Table 3.5, the most widely deployed technologies are also the most operationally critical, with the exception of onboard Wi-Fi. The only technology with a lower rated operational criticalness was traffic enforcement cameras.

These results indicate that most agencies use onboard Wi-Fi only as an amenity for passengers. Only two agencies indicated use of Wi-Fi for information transfer related to operations (e.g., loading new schedule and headsign data onto vehicles when they are in the yard, transferring APC data from the vehicle to agency servers), perhaps in addition to providing Wi-Fi as a passenger amenity. Future work should examine the architecture of Wi-Fi systems used for critical operational purposes to determine if these systems are potentially susceptible to attack, especially considering that onboard Wi-Fi was the top-ranking technology being considered by agencies that haven't yet deployed it. Increased scrutiny should be given to operationally-critical Wi-Fi systems that are also used for onboard Internet access by riders.

Table 3.5 Summary of transit technologies in use

Technology name	Percentage of agencies deploying it	Percentage of agencies considering it	Average *operational* criticalness (out of 5)	Average *financial* criticalness (out of 5)	Susceptibility to attack (out of 4)
Communication systems	88%	0%	4.5	3.8	1.7
CCTV Security Cameras	80%	16%	4.3	3.8	1.9
CAD/AVL	76%	11%	4.2	3.4	1.8
Fare payment	64%	26%	3.9	4.2	2.5
APC	52%	21%	3.5	3.4	1.7
Onboard Wi-Fi	52%	37%	2.2	2.0	3.1
Online Trip Planner	44%	21%	3.6	3.2	1.9
Traffic Enforcement Cameras	16%	0%	2.0	2.3	3.0
Traffic Light Controllers	12%	11%	4.0	2.5	2.5
TSP	8%	26%	3.0	2.7	2.9
Traffic Management Software	4%	5%	3.0	3.0	1.0
SPAT for CVs	0%	11%	3.0	3.0	2.0

Also shown in Table 3.5 is that onboard Wi-Fi, traffic enforcement cameras, TSP, and fare payment are perceived to be "somewhat likely to be susceptible to attack or circumvention". However, the number of participants rating these technologies varied significantly. For example, only three of the 25 agencies assessed traffic enforcement cameras, while 21 of the 25 agencies assessed fare payment, a consequence of fare payment's wider deployment.

Approximately half of participating agencies who have deployed CAD/AVL, APC, online trip planner, communication system, or CCTV security cameras perceived these technologies as "very unlikely" to susceptible to attack.

3.4.2. Planned Deployment of AVs and CVs

Three agencies[1] have deployed autonomous vehicles, and one agency has deployed connected vehicles. Table 3.6 lists these agencies.

Table 3.6 Agencies that have already deployed AVs or CVs

Agency name	Technology deployed
Gainesville RTS	AV
Jacksonville Transportation Authority	AV
Miami Bridge Youth & Family Services, Inc.	AV
Lakeland Area Mass Transit	CV

Five agencies are considering deploying AVs (Figure 3.12), and five agencies are considering deploying CVs (Figure 3.14). All of these agencies estimate that the deployment timeline would be no more than six years (Figures 3.13 and 3.15). If all of these deployments do occur within the expected timeline, then within the next six years 36% of the agencies participating in this survey will have AVs deployed, and 24% will have CVs deployed.

3.4.3. Data Security

The survey results indicate that the majority of transit agencies collect many types of sensitive data, and more transit agencies keep their data in local storage than in cloud storage. Security camera records and employee information are overwhelmingly stored locally, while customer information is the type of data most often stored in the cloud (often in addition to being stored locally).

The results also indicate that the majority of transit agencies do not share the data they collect with any third parties. Scheduling/planning resources are shared by more agencies (41%) than any other data type; sharing open schedule data in the General Transit Feed Specification (GTFS) format has been a dominating trend in transit over the past ten years.

Based on the survey responses, the only types of data encrypted by more than half of the responding agencies are customer information (64%) and employee email (59%). Future work could examine agency data encryption practices to discover where and how the data is encrypted. For example, data stored on a computer hard drive (i.e., "data at rest") can be

[1] Further discussion with Calhoun County Senior Citizens Association, Inc. revealed they have not deployed AVs. The survey results have been updated to reflect this discovery. The research team was unable to confirm the existence of AV deployments with Miami Bridge Youth & Family Services, Inc. following the survey.

encrypted or can be stored in plain text. When that data is sent between two computers (i.e., "data in flight"), it could also be encrypted or in plain text, independent of whether it is encrypted on disk. To keep the survey short and encourage a higher completion rate, multiple questions regarding the location of data being encrypted were not asked. As a result, further investigation is recommended to determine where agencies have protected data using encryption and where they have not.

The survey's results on data encryption imply that agencies should investigate and consider improving their encryption procedures, particularly when it relates to the transit riders. Of the responding agency representatives, 21% did not know whether customer information was protected with encryption, and 14% responded that customer information was not protected with encryption. When further breaking down whether customer information was encrypted in rest or in flight in the future, the number of agencies that leave customer information unencrypted somewhere in their system architecture may increase; some agencies may have answered that they encrypted customer information but may only encrypt customer information in-flight but not at rest, or vice versa.

Of the 23 responding agencies, more than 65% back up all types of data every day. All responding agencies make backups for all data types at least every month, with the exception of security camera records.

In addition, more than 65% of participating agencies keep their data backups for two years or more. Customer information and employee email tend to be saved for relatively longer periods of time, while security camera records tend to be saved for relatively shorter periods of time.

3.4.4. Past Cybersecurity Incidents and Challenges

The two open-ended questions (Questions 24-25) were optional, and the response rates for these questions were lower than for the previous questions.

Surprisingly, of the 15 responses to Question 24, 11 (73%) indicated that neither the agencies nor their vendors had been affected by cybersecurity issues. Two agencies (13%) said they did not know whether they or their vendors had been affected by cybersecurity issues. The remaining two agencies said that they had been affected, with the following responses:

- "Hacking of the Company website and Facebook page."
- "Over the course of the last 6-12 months multiple attempts at phishing across our employee base has taken place."

Future work could focus on additional, more specific questions to agencies and their vendors regarding being impacted by cybersecurity issues. Agencies may interpret the wording in the question "affected by cybersecurity issues" differently; for example, some may interpret this wording as asking whether the agency was actively attacked and the system compromised

(as one of the agencies responded that their website and Facebook page had been compromised), while others may or may not include unsuccessful attempts to gain access to a system (e.g., phishing attempts), and still others may interpret the question as asking whether the agency's procedures or budgets had changed due to cybersecurity incidents.

An additional concern is that participants may be reluctant to report cybersecurity incidents via an FDOT-sponsored survey that requires their agency's name. For example, participants may be embarrassed that an incident occurred or fear that the existence of an incident may adversely impact their funding or reputation. In any case, although the responses to Question 24 were, to us, the most surprising of the survey, the results should be considered in this context.

Twelve agencies responded to Question 25 (Figure 3.23) about challenges preventing good security practices, with some providing more than one answer within their open text response. These responses were categorized into four areas: employee training (five responses), cost (four responses), other (four responses), and no challenges (two responses).

Five participants believe that agency employees need to be trained to properly and securely use technologies with which they work. One of those respondents said, "I believe the biggest challenge stands with making sure employees/users are up to date with the knowledge to prevent phishing attempts. As attacks become more sophisticated, we will need to implement better training and technologies to combat this." The response was provided by the agency that stated that they had been impacted by phishing attacks in Question 24. This response indicates that the agency believes that attacks will increase in sophistication, and that employee training programs should improve as new threats emerge.

Four participants said that their agency needs more funding to improve the security of their systems. One participant wrote: "Understanding the threat and impact of the threat. Financial challenges also play a major role in this challenge." The first sentence was categorized as "Employee training" and the second sentence as "Cost".

Two agencies believe that they have no computer security challenges. Their exact responses are as follows:

- "We are County Government so cyber security is handled at that level, no issues"
- "NONE"

The remaining four responses were unique:

1. "The ability to find a vendor that can meet the Buy America requirement."
2. "Building & bus video system that stays up to date."
3. "Simplicity with the end users."
4. "Third party software."

The first response regarding the "Buy America requirements" seems to imply that cybersecurity is negatively impacted by the Federal Transit Administration (FTA)'s policy that "prevents FTA from obligating an amount that may be appropriated to carry out its program for a project unless 'the steel, iron, and manufactured goods used in the project are produced in the United States"[2]. This text suggests that vendors meeting this requirement may be hard to find, so products that enhance cybersecurity cannot be purchased, or that vendors who meet the "Buy America requirement" do not employ standard cybersecurity practices. Future work could further investigate this response to better understand the perceived limitation.

The second response of "building & bus video system that stays up to date" likely refers to the challenges in keeping hardware and software up to date.

The third response of "Simplicity with the end users" refers to the challenges in keeping systems simple for the end users, which limits the ability of agencies to implement more complex and secure features.

The fourth response seems to state that deploying third-party software within an agency's network puts the system at risk.

3.5. Conclusions

The responses from 25 transit agencies in Florida shed light on the technologies agencies have deployed, the technologies being considered, the deployment stage of AVs and CVs, agencies' data management, and past cybersecurity issues that these agencies have encountered.

The first section of the survey focused on better understanding which technologies have been deployed by Florida agencies, and which technologies they are planning to deploy. The most commonly deployed technologies by transit agencies are communication systems (88%), followed by CCTV security cameras (80%), CAD/AVL (76%), fare payment (64%), onboard Wi-Fi (52%), and APC (52%). All of these technologies, except onboard Wi-Fi, are also considered by most agencies to be critical from operational and financial perspectives. Wi-Fi was considered "extremely critical" and "very critical" by two agencies, indicating that, while other agencies likely only provide Wi-Fi as a passenger amenity, these agencies use Wi-Fi as part of their critical operational systems.

Future work should examine the architecture of Wi-Fi systems used for critical operational purposes to determine whether these systems are susceptible to attack. Increased

[2] "Buy America.", FTA, United States Department of Transportation, 16 December 2015, https://www.transit.dot.gov/buyamerica

scrutiny should be given to operationally critical Wi-Fi systems that are also used for onboard Internet access by riders.

The most common technologies that agencies are considering deploying (i.e., more than 20% of agencies are considering them) are onboard Wi-Fi (37%), fare payment (26%), TSP (26%), APC (21%), and an online trip planner (21%). Fare payment systems are considered the most critical of all the technologies from a financial perspective. This is intuitive, as the agency's ability to collect money from riders would be hindered if the fare payment system was not functional. Fare payment systems were also consistently rated at the top of other categories, including the most widely deployed, the most considered for future deployment, and the most likely to be susceptible to attack.

The second area of the survey focused on the current deployment of AVs and CVs in public transit agencies. AVs are currently deployed by four of the responding agencies, and CVs are currently deployed by one of the responding agencies. However, within the next six years, five agencies expect to deploy AVs, and five agencies expect to deploy CVs. The rapid growth of AVs and CVs emphasizes the need to develop robust security practices to mitigate vulnerabilities that may be present in these new technologies.

The third area of the survey captured information about the agencies' management of data. Agencies uniformly collect data on customer information, employee information, CAD/AVL operation, scheduling resources, employee email, and security camera records. The results show that more agencies store data locally, especially security camera records and employee emails. The majority of agencies do not share information about their employees and their emails with any third party. Almost half of the agencies that store their scheduling/planning resources share that data. Around 70% of agencies who store the remaining data types do not share the corresponding data.

All but one of the agencies make backups at least once a month, and most of them do it every day. More than half of the participating agencies keep backups for two years or more. Future work should examine data encryption practices in more depth to determine where and how the data is encrypted (e.g., differentiating encryption of "data at rest" vs "data in flight"). For encryption and other topics, the desire to encourage a high completion rate prevented more in-depth questions. Further investigation is recommended to determine where agencies have protected data using encryption and where they have not. Agencies should also be encouraged to investigate and improve encryption practices being used internally and by their vendors, especially when the data relates to the transit riders.

Future work could also examine data integrity and authentication practices, which were not covered in this survey. Cryptographic hashes and digital signatures could help agencies determine whether data had been altered from its original state. In addition, authenticating the source of internal emails could help reduce the spread of malware from phishing attempts.

The fourth area of the survey covered agencies' experience with cybersecurity issues and their challenges in implementing good security. Surprisingly, only two of the 15 responding agencies reported that they were impacted by cybersecurity issues—one agency's website and Facebook pages were compromised, and one agency reported multiple phishing attempts over the last year. Only one agency was aware of data theft. Future work could focus on additional, more specific questions for agencies and their vendors regarding being impacted by cybersecurity issues. Agencies may have interpreted the wording in the survey question about being "affected by cybersecurity issues" in different, unexpected ways. Agency representatives may also be reluctant to report cybersecurity incidents via a survey that requires their agency's name.

The most commonly reported challenge for implementing good security practices was employee training, followed by funding. One agency stated that improving the level of staff training may help prevent phishing attacks. Two agencies stated that they did not have any computer security challenges; a follow up may enable a better understanding of why they do not perceive cybersecurity to be a challenge.

CHAPTER 4: WORKING GROUPS

4.1. Introduction

One of the primary objectives of the research project is to facilitate ongoing cybersecurity information exchange among Florida transit agencies, their vendors, and cybersecurity researchers. Successfully facilitating discussions between these parties will further encourage cybersecurity awareness in the field. To meet this objective, the research team organized monthly working group meetings for agencies and cybersecurity professionals and held three workshops focused on cybersecurity in public transportation. This section of the report focuses on the working group meetings.

With the ultimate goal of facilitating ongoing cybersecurity information exchange, the working group meetings aim to be proactive in identifying new concerns and mitigations, and share this information with the following stakeholders: Florida transit agencies, the Florida Center for Cybersecurity, and Florida cybersecurity researchers. The working groups also aim to be reactive in considering existing and known vulnerabilities and best practices for preventing their exploit.

This report describes the working groups and major discussion points from each of the meetings. The report begins with a brief introduction to the structure of the working group meetings, followed by a deeper analysis of each of the meetings. Each section will include a description of the material presented, major discussion points, and details about the meeting, such as date, attendance, and agenda.

4.1.1. Working Group Overview

Working group meetings were held approximately once a month during July 2018 to June 2019. All working group meeting were held on Wednesdays 1:30-2:00 PM. The meetings were hosted using Adobe Connect and limited to 30 minutes in length to encourage participation from a large number of agencies. The conference software allowing participants to connect remotely or join a conference call on their phone. For consistency, each of the meetings followed the same structure. Meetings began with introductions and opening remarks, followed by a guest presentation. The meetings were concluded with open discussion and closing remarks from the research team.

Invitations to the working group were sent to the same list of transit agency employees and other transportation experts used during the survey completed as part of this project, which originated from FDOT as well as existing contacts that CUTR staff maintain with organizations across the state. The invitation list grew slightly over time to include contacts referred by working group participants. Personalized email invitations for the first working group meeting were sent to members who had completed the survey. Invitations were originally sent out a week before

each meeting. After the first three meetings, invitations were scheduled farther in advance, almost a month before each meeting. More frequent email invitations were sent out after the fourth working group meeting to increase attendance.

Table 4.1 lists the working group schedule, including the topic, presenter, and number of attendees. A full list of attendees for each meeting can be found in the following sections. Due to limitations of the conference software, the number of attendees does not include anonymous participants who only called into the presentation.

Table 4.1 Working group meeting schedule

Date	Topic	Presenter(s)	Attendees
7/11/2018	Project Overview and Survey Results	USF Research Team	18
8/8/2018	Continuation of Survey Results	USF Research Team	10
9/5/2018	Literature Review	USF Research Team	6
10/3/2018	Continuation of Literature Review	USF Research Team	8
11/14/2018	Cybersecurity for Smart Mobility Initiatives	Scott Keith (City of Tampa), Rick Tiene (Mission Secure)	10
12/12/2018	State of Florida Safety and Security Regulatory Infrastructure	Ashley Porter (FDOT Public Transit Office)	6
1/23/2019	ISAC/ISAO Program	Kevin Salzer (Jacksonville Transportation Authority)	5
2/13/2019	SCMS for Connected Vehicles	Steve Johnson (HNTB)	7
3/20/2019	Mobile Fare Payment App Vulnerability	USF Research Team	9
6/19/19	FDOT Triennial Compliance Review	Gennaro Saliceto	4

4.2 Working Group Meetings

The following sections describes each of the working group meetings in greater detail, including attendees, agenda, presenter, and the outcomes and major discussion points.

4.2.1. Meeting 1: Project Overview and Survey Results

The first meeting was held on July 11, 2018. The presentation for this meeting was given by the USF research team and provided an overview of the project and the survey results from the project. A total of 18 participants, not including anonymous callers, attended the first meeting. The list of participants for the first meeting can be found in Table 4.2.

Table 4.2 Participants for the first working group meeting, held on 07/11/18

Participants (Self-Reported)	
Andy Delk - Sarasota IT	Keiron
Ashley Porter	Kevin Salzer
Chris Wiglesworth	Kyle Masters
David Sharfman	Michelle Arnold
Gabe Matthews-FDOT	Mike
Gennaro Saliceto	PSTA
Jackie Fernandez	Ray Allen
Jafari Bowden	St. Johns Council On Aging
Joe Chagnon	Wendy Awes

4.2.1.1. Presentation Overview

The presentation for the first meeting was split into two parts. The first part of the presentation provided participants with an overview of the project, focusing on the project's main objectives, the objectives for the working group, and describing the structure of future working groups.

The second part of the presentation discussed the results of the project survey. The survey review began by discussing the number of survey participants and the categories of questions in the survey. The majority of the presentation was spent reviewing the data for each technologies' operational and financial criticalness and their perceived susceptibility to attack. USF researchers also presented the most deployed technologies, and ended the presentation by discussing reported autonomous and connected vehicle deployments in Florida.

4.2.1.2. Discussion and Questions

During the presentation, the USF research team asked for participants to provide any insight about the perceived financial and operational criticalness of the various technologies included in the survey. In particular, the USF research team was interested in the high perceived

operational criticalness of Closed-circuit television (CCTV) and why a few agencies responded that onboard Wi-FIWi-Fi was operationally critical while most responded it was not.

Ray Allen from Gainesville Regional Transit System (RTS) explained that, in the case of an accident or theft, the burden of proof lies with the agency, and the high rating for CCTV was likely due to their need for evidence and record keeping. Allen also confirmed the research team's theory that onboard Wi-FI was being used by some agencies to update the various technologies on the bus, adding that Gainesville RTS also uses the onboard Wi-FI to download onboard video.

While discussing the technology deployments, the research team and participants were asked if they had "heard of spoofing on the mobile fare payment systems in use?" None of the participants or the research team had heard of spoofing in systems in use. The research team then described their interest in mobile fare payment applications and offered to provide more information on attacks on mobile fare payment systems in an upcoming meeting. They also agreed to follow up with the participants if they heard of anything similar in the future.

At the end of the working group meeting, Kevin Salzer from Jacksonville Transportation Authority (JTA) mentioned JTA's involvement in an Information Sharing & Analysis Organization (ISAO) and offered to share JTA's experience as a member of the working group during a future meeting. Ray Allen then added that Gainesville RTS was a part of an Information Sharing and Analysis (ISAC) organization, and would also be willing to share their experience. The research team scheduled a time for them to present after the meeting had concluded. The presentation on ISAC/ISAO organizations can be found in Section 2.7.

4.2.2. Meeting 2: Continuation of Survey Results

The second meeting was held on August 8, 2018, and continued discussion of the survey results from the previous working group meeting. The presentation for this meeting was given by the USF research team. A total of 10 participants, not including anonymous callers, attended the meeting. The list of participants for the meeting can be found in Table 4.3.

Table 4.3 Participants for the second working group meeting, held on 08/08/18

Participants (Self-Reported)	
Ashley	Kevin Salzer
David Sharfman	Michelle Arnold
Gabe Matthews - FDOT	Phil Cao
Gilbert Morales, Security Manager, Palm Tran	Ted Woolcock
Jim Dorsten	Vik Bhide

4.2.2.1. Presentation Overview

For the second meeting, the USF research team continued the review of the survey results. The survey results covered in this presentation focused on data storage and security in transit agencies and past cybersecurity incidents and challenges. The data storage questions included data storage location, type of data, data sharing, and data encryption.

The research team then described past cybersecurity incidents described by survey participants. The incidents including the "hacking of the Company website and Facebook page," and multiple phishing attempts. The rest of the presentation was spent discussing the cybersecurity incidents and challenges, including difficulties with keeping building and bus video systems updated.

4.2.2.2. Discussion and Questions

While reviewing challenges to implementing better security, participants discussed updating software and the challenges that may be present to perform updates for technologies such as buses. These challenges primarily consisted of difficulties in managing updates of such a large number of devices on many vehicles. Ray Allen from Gainesville RTS described how they currently use the onboard Wi-FI to upload firmware updates to the buses upon their return to the yard. Updates over onboard Wi-FI will help to mitigate the challenges presented in keeping technologies updated, but may also provide new attack vectors, such as fake and malicious firmware updates.

The reports of phishing attempts from a Florida agency led to a discussion of spear phishing by the USF research team. Spear phishing occurs when an attacker sends a phishing email that has been uniquely crafted to target a single or small group of people. Sophisticated spear phishing attacks are often well written and may contain unique characteristics, such as company signatures, language, or other company mannerisms, to masquerade as an official email. With the meeting coming to a close, the USF research team tabled further discussion of phishing attacks for the next meeting.

4.2.3. Meeting 3: Literature Review

The third meeting was held on September 5, 2018. The USF research team presented their findings from the project's literature review. A total of six participants, not including anonymous callers, attended the meeting. The list of participants for the meeting can be found in Table 4.4.

Table 4.4 Participants for the third working group meeting, held on 09/05/18

Participants (Self-Reported)	
Ashley Porter	Jackie Fernandez Broward County
Gainesville RTS	Michelle Arnold
Gerald Young	Ryan PCPT

4.2.3.1. Presentation Overview

The USF research team presented their findings from the project's literature review for the third meeting. The presentation began with a brief overview of operational technology (OT) and IT, followed by examples of modern cyber attacks. Since most, if not all, agencies use IT systems, such as email or an internal company website, daily, the team started with a brief review IT security. Ransomware and phishing attacks were the focus of this section of the presentation, continuing the working group's discussion on phishing attacks from the last meeting.

After completing the section on IT security, the group examined a variety of transit technologies in greater detail. This meeting focused on online trip planners and real-time passenger information system, allowing time for electronic ticketing, mobile fare payment applications, and traffic signal controllers in the next working group meeting. Given the growth of open source solution for online trip planners, the research team also briefly discussed the benefits of open source solutions.

4.2.3.2. Discussion and Questions

Continuing the discussion from last week, the working group participants discussed phishing attacks in greater detail. One of the participants mentioned that "humans are the weak link in the chain", which led to discussion on employee training and awareness. Participants were encouraged to hold employee security trainings including materials on recognizing and reporting phishing emails. Given the high number of phishing attacks, many free training materials are available online. Another participant suggested employees reach out to their IT team if they were ever unsure of an email.

4.2.4. Meeting 4: Continuation of Literature Review

The fourth meeting was held on October 3, 2018. The USF research team continued their presentation on the findings from the project's literature review. A total of eight participants, not including anonymous callers, attended the meeting. The list of participants for the meeting can be found in Table 4.5.

Table 4.5 Participants for the fourth working group meeting, held on 10/03/18

Participants (Self-Reported)	
Genaro Saliceto	Michelle Arnold
Gerald Young	Richard
Guest	Ryan
Joe	Trevor Martin

4.2.4.1. Presentation Overview

The USF research team continued the presentation of the literature review findings with a discussion of electronic ticketing and mobile fare payment applications. The presentation included both contact and contactless forms of electronic ticketing, such as paper tickets, magnetic swipe cards, and Near Field Communication (NFC) devices. Most attacks consist of breaking the device's cryptographic implementation and copying or changing values. The team discussed one such attack on the fare cards in use by the Massachusetts Bay Transportation Authority subway system from students at the Massachusetts Institute of Technology [42].

The team then discussed mobile fare payment systems, focusing on the benefits offered by these systems. In particular, the team found literature that claimed mobile fare payment may reduce production and cash-handling costs [48], and may reduce boarding times. Passenger Transport [49] reported that First Bus' mobile fare payment system reduced boarding times by up to 75%. The team also mentioned that some mobile fare payment applications are now integrating online trip planning and real-time passenger information into their application.

4.2.4.2. Discussion and Questions

There were no questions after this presentation, possibly due to the more informative nature of the presentation. Instead, the USF research team took the remaining discussion time to discuss the upcoming workshop with the Hillsborough Area Regional Transit Authority (HART). This event, tentatively scheduled for November 9, 2018, would allow students to interact and experiment with the onboard Wi-FI systems available on HART with the goal of identifying potential vulnerabilities. The event topic material was eventually changed due to vendor concerns. More information can be found in the workshop report submitted as part of this project.

4.2.5. Meeting 5: Cybersecurity for Smart Mobility Initiatives

The fifth meeting was held on November 14, 2018. Scott Keith from the City of Tampa and Rick Tiene from Mission Secure presented on cybersecurity for smart mobility initiatives[3]. A total of 10 participants, not including anonymous callers, attended the meeting. The list of participants for the meeting can be found in Table 4.6.

Table 4.6 Participants for the fifth working group meeting, held on 11/14/18

Participants (Self-Reported)	
Ashley Porter	Michelle Arnold
Darrin - Lee County	Ray Allen (Gainesville RTS)
Gabe Matthews	Rick Tiene
Gerald Young	Scott Keith
Kevin	Smith Meyers

4.2.5.1. Presentation Overview

Scott Keith began the presentation with a discussion of potential threats for smart mobility systems. The threats discussed included field-level threats, such as physical security threats, and the threats arising from the decreasing isolation of networks. Traffic cabinet devices may not be hardened against potential threats, allowing an attacker who gains access to easily move across the network. Keith also discussed how data sharing, while offering great benefits, opens access points to the network that could potentially be used by an attacker.

Keith then discussed potential mitigations for these issues. For physical security, Keith suggested unique keys, better tracking of device access, or “smart locks”. Smart locks, in this presentation, refer to electronic locks and keys that may have access remotely disabled or enabled. Keith recommended agencies update firmware across the network, use hardened passwords, and define network access policies. He then mentioned the City of Tampa is also looking into operational-level network security devices, leading into the presentation by Rick Tiene.

Rick Tiene’s presentation was titled “Cyber Risks to Transportation Systems and How to Mitigate Them.” He began the presentation with a discussion of the Purdue Industrial Control System (ICS) Model, which splits OT in ICS into four layers. The presentation focused on layers

[3] The fifth meeting was originally scheduled for October 24, 2018 and featured Kevin Salzer presenting ISAC/ISAO programs. Due to low participation on October 24th, Mr. Salzer’s presentation was rescheduled to January 23, 2019. In an attempt to increase future participation for all working group meetings, reminders were sent out more frequently from this point on, including a reminder sent the Monday before the meeting and another sent the day of the meeting.

zero, one, and two. Layer zero consists of process input/output devices, such as pumps, sensors, or traffic lights. Layer one consists of safety devices or basic control devices such as Programmable Logic Controllers (PLCs). Layer two consists of Human Machine Interfaces (HMIs) that provide operators with control or monitoring capabilities over the lower layers.

The presentation focused on the lack of protection for the communication between layers zero, one, and two. Rick Tiene discussed how an attacker who is able to gain access to any of the three layers can communicate and possibly manipulate the other layers due to the lack of authentication, encryption, and monitoring. In addition, due to a lack of forensics data, the cause of the attack cannot be discovered, and a lack of automated restoration capabilities lead to expensive, manual restoration processes.

Tiene then discussed the need for a technology that sits between layers zero and one and between layers one and two that seamlessly encrypts communications and authenticates access to the devices. These devices should also monitor attempted accesses and alert the operator in the case of malicious behavior.

4.2.5.2. Discussion and Questions

During Keith's talk on physical security threats, the working group discussed smart locks in greater detail. One member discussed the current trend in hotels where guests are able to use their cell phone to access their room. A similar system could enable transit agencies to grant access to contractors, employees, or other personal without the need for the guest to have a specific device or special hardware. This would allow cities or agencies to have more fine-grained control over their systems and allow for automated monitoring.

After Tiene's presentation, a participant asked Tiene to describe a potential attack scenario. Tiene described how an attacker that has gained access to layer one, two, or intercepted communications between those layers could perform a Man-in-the-Middle (MitM) attack. In a MitM attack, an attacker intercepts the communications between two parties and manipulates the messages being passed. In this scenario, an attacker could send false commands to the layer one controller or pass false data to the layer two HMI. This could cause the system to be in a different, potentially unsafe, state without alerting the operators.

In Tiene's scenario, he proposed a cell signal from a rural traffic controller could be intercepted by an attacker. The attacker then pretends to be the management system, giving a command to the device that sets the traffic light to flashing. The attacker then pretends to be the controller, and sends falsified data to the actual management system suggesting the system is working correctly.

4.2.6. Meeting 6: State of Florida Safety and Security Regulatory Infrastructure

The sixth meeting was held on December 12, 2018. Ashley Porter from the FDOT Public Transit Office presented on the state of Florida's safety and security regulatory infrastructure. A total of six participants, not including anonymous callers, attended the meeting. The list of participants for the meeting can be found in Table 4.7.

Table 4.7 Participants for the sixth working group meeting, held on 12/12/18

Participants (Self-Reported)	
Ashley Porter	Gerald Young
Gabe Matthews	Kevin Salzer
Gainesville RTS	Phil

4.2.6.1. Presentation Overview

Ashley Porter began the presentation with a discussion of existing statutes and rules in the state of Florida. The review focused on the security requirements of Rule 14-90 from the Florida Administrative Code, but also briefly described Section 341.061 of the Florida State Legislature which allows FDOT to suspend service when immediate danger to the public exists. Rule 14-90 requires agencies to provide a Security Program Plan (SPP) that define organization roles, responsibilities, and other processes such as employee training and security data acquisition.

Porter then discussed Safety Management Systems (SMS), which aim to "manage risk and assure effectiveness of safety risk mitigation". The SMS was broken into four pillars: safety management policy, safety risk management, safety assurance, and safety promotion. Employee training, awareness, and reporting was a key idea to the successful implementation of the SMS.

4.2.6.2. Discussion and Questions

During the presentation, participants asked if plans generally have cybersecurity included in them. Porter said they do not currently include cybersecurity, but it is entering discussion in conferences and other official gatherings. The discussion then turned to potential policy changes that could be made to Rule 14-90 to add cybersecurity guidelines. The USF research team agreed to draft some sample guidelines, and scheduled a meeting to discuss the matter further with Porter. More information on the sample policy is available later in this report.

4.2.7. Meeting 7: ISAC/ISAO Program

The seventh meeting was held on January 23, 2019. Kevin Salzer from Jacksonville Transportation Authority and Ray Allen from Gainesville Regional Transit System were scheduled to present on their experience with ISAC/ISAO programs. Ray Allen was ultimately unable to attend so Kevin Salzer presented for the entire working group meeting. A total of five participants, not including anonymous callers, attended the meeting. The list of participants for the meeting can be found in Table 4.8.

Table 4.8 Participants for the seventh working group meeting, held on 01/23/19

Participants (Self-Reported)	
Gabe Matthews-FDOT	PSTA
Kevin Salzer	Steve Johnson, HNTB
Lee Arciniegas	

4.2.7.1. Presentation Overview

To begin the presentation, Salzer discussed the benefits and challenges for organizations seeking to share cybersecurity information. By sharing cybersecurity information, such as potential threats or vulnerabilities, organizations are given time to prepare for and possibly prevent exploitation. However, organizations may be unwilling to share this information due to a fear of penalties, limited funds or human resources, and a fear of identifiable data being compromised during the sharing process. Salzer then shared recent legislature that protects ISAO participants against penalties, citing executive order 13691 and the cybersecurity act of 2015.

Salzer then reviewed JTA's experience with the Community and Transportation ISAO. JTA is currently a part of the National Cyber Neighborhood Watch Program, which enables them to better protect their Intelligent Transport Systems (ITS), Internet of Things (IoT) devices, connected and autonomous vehicles, and their IT systems. The organizations in the program, which include vendors, cities, and other partners, work together to meet regulatory requirements and reduce cyber risk.

4.2.7.2. Discussion and Questions

After the presentation, one of the participants asked about the cost of joining the ISAO. Salzer told the group that there was no fee for joining the ISAO, but that there may be fees for certain services, such as installing firewall software. The firewall software in question allows organizations to regularly update their firewall rules based on data collected by the ISAO. Vulnerability knowledge is also shared manually by the ISAO in addition to the automated firewall updates. JTA currently participates in the firewall attack sharing program, which is called Secure Together.

Another participant asked about the timeliness of the information sharing. Salzer referred to a statistic shared in the presentation which states "participants know of an attack before experiencing the attack because of information sharing on Secure Together" three days in advance. He also mentioned again that 62% of attacks on Secure Together participants are also experienced by another participant.

4.2.8. Meeting 8: SCMS for Connected Vehicles

The eighth meeting was held on February 13, 2019. Steve Johnson from HNTB presented on Security Certificate Management Systems (SCMS) for connected vehicles. A total of seven participants, not including anonymous callers, attended the meeting. The list of participants for the meeting can be found in Table 4.9.

Table 4.9 Participants for the eighth working group meeting, held on 02/13/19

Participants (Self-Reported)	
Danielle Geiger	Gerald Young
Gabe Matthews	Kevin Salzer
Gainesville RTS	Steve Johnson
Gennaro Saliceto	

4.2.8.1. Presentation Overview

Johnson began the presentation with a discussion of the Connected Vehicle (CV) Pilot in Tampa. Tampa [108], New York City [107], and the state of Wyoming [106], received funding from the US Department of Transportation to implement a wide range of connected vehicle technologies tailored to each region's unique needs [105]. Johnson introduced the technologies that the Tampa CV Pilot is bringing to downtown Tampa, including pedestrian safety systems, wrong-way entry prevention, and streetcar safety systems.

Johnson then introduced SCMS, including a brief discussion of their architecture and their purpose. To help explain the concept, he used SCMS for Internet browsers as an example. Security certificates provide users with the ability to verify the identity of the other party during communication. At a high level, an SCMS passes trust through the use of Certificate Authorities (CAs). The CAs sign valid certificates which can then be validated by the user to validate the identity of communicating party. SCMS for connected vehicle technologies allow devices such as traffic cabinets, passenger vehicles, or other transportation technologies to verify the data received from other parties. Johnson emphasized that these technologies include transit technologies such as transit signal priority, electronic fare payment, and driver assistance.

4.2.8.2. Discussion and Questions

After the presentation, a member of the work group asked what the volunteer process for the CV pilot looks like. Johnson explained that the volunteers have equipment installed in their vehicle which allows them to communicate with the installed technologies. The equipment is typically two or three antennas added to the volunteer's car and an onboard CV processor unit that is installed in the trunk of the vehicle. The radio antennas in the car have a max range of 300 feet, which can be tuned down to 100 feet.

Johnson then explained what the volunteer process looks like for pedestrian participants. Pedestrian participants have an application installed on their device, which allows them to communicate with the CV technologies installed at crosswalks and various other points. However, current smartphones do not have an accurate enough Global Positioning System (GPS) to trust messages from pedestrians in the walkways, so they are currently not using that technology.

4.2.9. Meeting 9: Mobile Fare Payment App Vulnerability

The ninth meeting was held on March 20, 2019. The USF research team presented a vulnerability that was discovered in a Florida mobile fare payment application as part of this project. A total of nine participants, not including anonymous callers, attended the meeting. The list of participants for the meeting can be found in Table 4.10.

Table 4.10 Participants for the ninth working group meeting, held on 03/20/19

Participants (Self-Reported)	
Dexter Corbin	PCao
Gainesville RTS	Shannon H.
Joe	Steve Johnson, HNTB
Joe Chagnon	Terry @ Space Coast Area Transit
Julie Cagliostro	

4.2.9.1. Presentation Overview

The presentation began with a review of mobile fare payment applications and common implementations for ticket verification. The presentation focused on visual validation and QR codes, but also discussed Near-Field Communication (NFC) and Bluetooth Low Energy (BLE) implementations. The team then presented possible vulnerabilities in mobile fare payment applications, such as replay attacks that recreate the ticket screen used during visual validation.

After completing the overview, the team introduced the new vulnerability they discovered in a mobile fare payment application for a Florida transit agency. The vulnerability

was reported on October 30, 2018, and was patched by December 8, 2018. The vulnerability allowed an attacker to gain private information about other users, including name, phone number, license plate, and parking location. The vendor that developed the application also supported several other applications through the same service, allowing an attacker to use the same vulnerability to gain private data from those applications as well. More information about the vulnerability can be found in the upcoming final report.

To conclude the presentation, the team discussed the implications for transit agencies. The team presented several questions that agencies should consider when discussing with their vendor:

- Does the vendor have a plan?
- Will you be charged?
- Do they inform users of breaches?
- Do they inform agencies of breaches?
- Do they conduct independent security audits?

4.2.9.2. Discussion and Questions

During the presentation, a participant asked if any current transit systems expressed concerns of attackers compromising their mobile fare payment systems. The USF research team had not heard any concerns expressed by transit agencies. The participant then asked about the Token Transit [50] mobile application. Since the participant knew Token Transit was deployed at many Florida agencies, they asked if there had been any security breaches. The USF research team confirmed that Token Transit was not the application they discovered the vulnerability in. The team also added that they had discussed mobile application security with the Token Transit team and they had not mentioned any security breaches.

After the presentation, the research team asked for the participants' opinion on potential policy changes and any suggestions they may have. Terry from Space Coast Area Transit said "I definitely think having a policy that ensures users & agencies are informed, also conducting independent security audits are a part of any policy drafted." Other members also expressed positive sentiments for policy guidelines, including policy that allowed transit agencies to share vulnerability information data with other state agencies.

4.2.10. Meeting 10: FDOT Triennial Compliance Review

The tenth and final meeting was held on June 19, 2019. Gennaro Saliceto from the Center for Urban Transportation Research at the University of South Florida. A total of four participants, not including anonymous callers, attended the meeting. The list of participants for the meeting can be found in Table 4.11. This meeting was scheduled more than a month apart from the previous meetings to encourage working group participants to attend the workshop held on April 26, 2019.

Table 4.11 Participants for the tenth working group meeting, held on 06/19/19

Participants (Self-Reported)	
Dean Kirkland-McMillian	Gennaro Saliceto
Gainesville RTS	Steve Johnson

4.2.10.1. Presentation Overview

For the tenth meeting, Saliceto began the presentation with an overview of the compliance review process. The process consists of three phases: the pre-review, the on-site review, and the post-review. During the pre-review, the agency is informed of the audit date and are required to submit safety and security documentation. Agencies that assist in meeting the transportation needs of the elderly or those with disabilities may have additional or different set of plans to submit. During the on-site review, the reviewer rides on a bus and observes the facility, listing potential safety hazards or other concerns. Finally, during the post-review, a draft report is issued to the Department of Transportation for further review. Common findings include expired driver's licenses, non-approved documentation, or lack of training records.

After describing the process, Saliceto described how cybersecurity is currently not part of the existing review process. However, it is believed that future audits may soon be added that relate to cybersecurity. Given the physical consequences of many transportation technologies, cybersecurity is becoming increasingly related to safety issues. For example, new technologies such as autonomous and connected vehicles, dispatch or onboard communications, and onboard video, may all have safety-threatening consequences if exploited by an attacker.

4.2.10.2. Discussion and Questions

After the presentation concluded, the research team suggested having cybersecurity experts on review. Saliceto agreed and mentioned that there are currently security, but not cybersecurity, experts being sent for reviews. Agencies could implement their own cybersecurity policies if desired, but Saliceto reported that in his experience cybersecurity hasn't been addressed by any agencies. Being proactive rather than reactive may reduce the cost of an incident if one were to occur. This is a common ideology in current safety policies, with employee trainings and other preventative measures being put into action. Cybersecurity could be integrated into these existing processes (e.g., training, policy development, reporting) that currently exist for safety and security.

The group also discussed how agencies could discuss confidentially discuss vulnerabilities (e.g., before they are publicly disclosed). Saliceto mentioned that the Florida Transit and Safety Operations Network (FTSON) provide a peer-to-peer service, allowing experts from different agencies to communicate and post questions about any issues. These issues could include cybersecurity, and this may be a potential avenue for vulnerability information sharing.

After discussing the SPP with Saliceto, the research team suggested it may be beneficial for agencies to create a document listing the capabilities of their technologies and how they perform these tasks. This list should also include attack models and how their system architectures and defense mechanisms mitigate these attacks. Such a list would encourage agencies to analyze their systems and think through potential vulnerabilities, as well as how the agency would react when a vulnerability is discovered.

CHAPTER 5: TAXONOMY

5.1. Introduction

This section introduces a taxonomy classifying the different transit technologies based on five dimensions:

- The extent to which the technology is deployed in Florida
- The mode of transportation for which the technology is used
- The technology's functionality
- The organization(s) or individual(s) responsible for the technology, where "responsibility" may include owning, controlling, or maintaining the technology
- Liabilities, including the likelihood and severity of successful cyber-attacks and privacy violations

This taxonomy is useful to focus analysis of the most important—most widely deployed, critical, or highest-liability—technologies, and to ensure that the analysis has a broad coverage of transportation technologies. The remainder of this section provides a brief background of the field and presents related work.

5.1.1. Background

Transportation technologies have rapidly developed from individual nodes to large, interconnected networks of devices, similar to those seen in modern IT systems. With this rapid development comes security concerns that have typically been constrained to classical computer systems. The transportation sector is a particularly attractive target for adversaries seeking to have a wide area of impact. As the technology continues to grow, it is crucial that critical technologies are analyzed for new security concerns.

This taxonomy is informed by the literature review in Chapter 1 and the survey described in Chapter 2. The literature review examines known vulnerabilities and defenses in existing transit technologies, focusing on technologies currently deployed or under consideration for deployment in the state of Florida. The survey captures information from transit agencies in Florida including the current and planned deployments of transit technologies, the perceived financial and operational criticality of these technologies, and the likelihood of vulnerability for each technology.

5.1.2. Related Work

This section introduces a related taxonomy that classifies vulnerabilities for the Internet of Things (IoT). Many transportation technologies can be classified as IoT devices, including

connected vehicles, automatic vehicle location, and traffic signal priority, and the vulnerabilities seen in other IoT devices may be seen in transportation technology.

5.1.2.1. Internet of Things (IoT): Taxonomy of Security Attacks

Internet of Things (IoT): Taxonomy of Security Attacks [132] provides a taxonomy for the vulnerabilities commonly seen in IoT devices. The taxonomy identifies the attributes seen in IoT vulnerabilities and the different values they may have. An example of these attributes is access level, which the paper defines as the type of access needed to perform an attack. Passive attacks eavesdrop on or monitor communications without authorization. Active attacks attempt to break or otherwise directly circumvent protection mechanisms, often with the intent of escalating privileges or masquerading as an authorized user. The paper then describes each of these different values, and describes potential vulnerabilities that fit in each category.

Transportation is one of the example domains considered in the paper, and a potential scenario of IoT technology being used for transportation is described. The scenario presented describes using mobile applications for self-check-in at an airport. In addition to this scenario, several other listed vulnerabilities are present in transportation technologies. These vulnerabilities include Sybil attacks, which can be performed on location based services [133], and man-in-the-middle attacks, which can be used to eavesdrop on riders using onboard Wi-Fi.

5.2. Taxonomy

5.2.1. Overview

The taxonomy is based on five dimensions: the extent of deployment in the state of Florida, the functionality, the liabilities present in each technology, the transportation mode or application type, and the responsible parties for the technology.

The structure of the taxonomy is shown in Figure 5.1. Each technology is categorized by functionality, and the liabilities, modes, and responsible parties for each technology are listed under the technology. The functionality is colored according to the percentage of agencies that have deployed the technologies in that category based on responses to the survey conducted as part of this project.

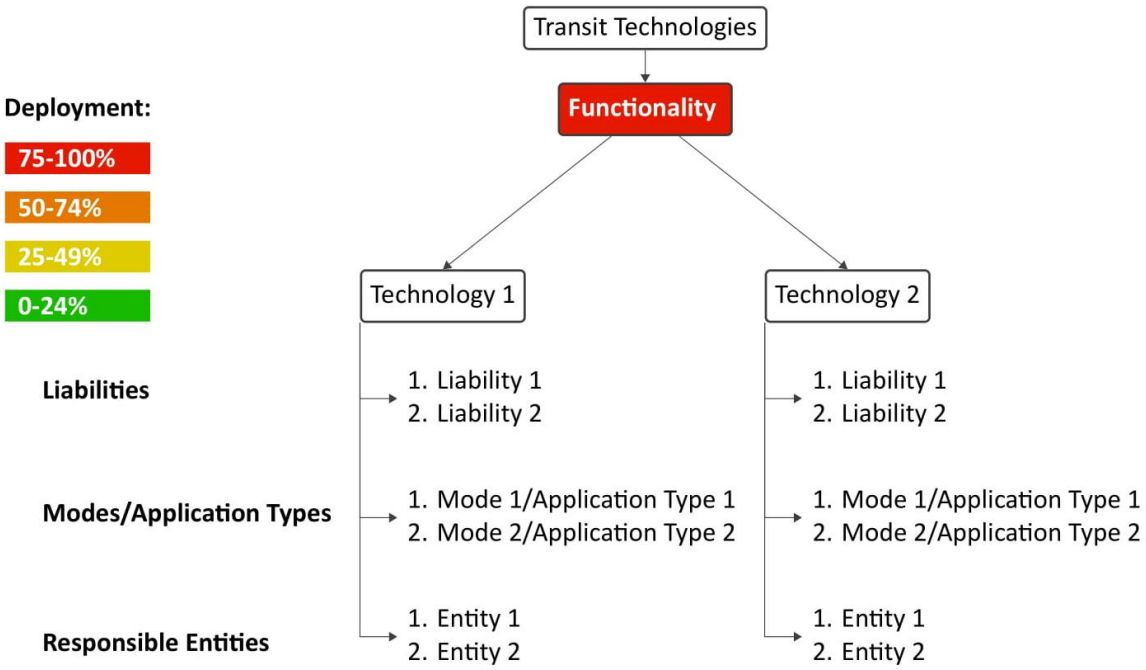

Figure 5.24 Structure of the taxonomy

The reader should note that most of the respondents were Florida transit agencies, and as a result some technology deployment percentages may be skewed as a result. For example, because transit agencies are not directly responsible for maintaining traffic signals many respondents indicated that they had not deployed related traffic signal technology. However, this technology may have been deployed by other public agencies (e.g., city or county government).

Certain functionalities may be more operationally or financially critical than other functionalities. By grouping the technologies based on functionality, technologies that provide critical functionality can be identified. In addition, technologies with a shared function are more likely to have similar liabilities, modes of transportation, and responsible parties.

The taxonomy focuses on liabilities that may arise due to vulnerabilities being exploited in transit technologies. By focusing on these liabilities, the most critical technologies for security analysis can be identified. For the sake of brevity, repair or replacement fees have not been included in the taxonomy itself as these costs would be incurred in any given scenario for all affected technologies after an attacker compromises a system.

The mode of transportation is included in the taxonomy to help identify the presence of the various technologies in different modes of transportation. However, for a few technologies such as email, mode of transportation does not apply. For these technologies, the application type is described instead. The application type for a particular technology will be explained in the section for that technology.

When analyzing a technology, communicating with the parties responsible for the ownership, management, and control of the technology will be necessary. If any vulnerabilities

or issues are identified, the responsible party will need to be contacted. Future analysis may require that all of the responsible parties must be contacted, or only a subset of them. For example, a transit agency could be contacted for a configuration issue, and the vendor may be contacted for a vulnerability present in the software.

The final taxonomy can be seen in Figure 5.2 and Figure 5.3. Due to the size of the taxonomy, Figure 5.2 shows the first four functionalities, and Figure 5.3 shows the final three functionalities. The taxonomy is ordered based on percentage of deployment, with least deployed technologies on the left and most deployed on the right.

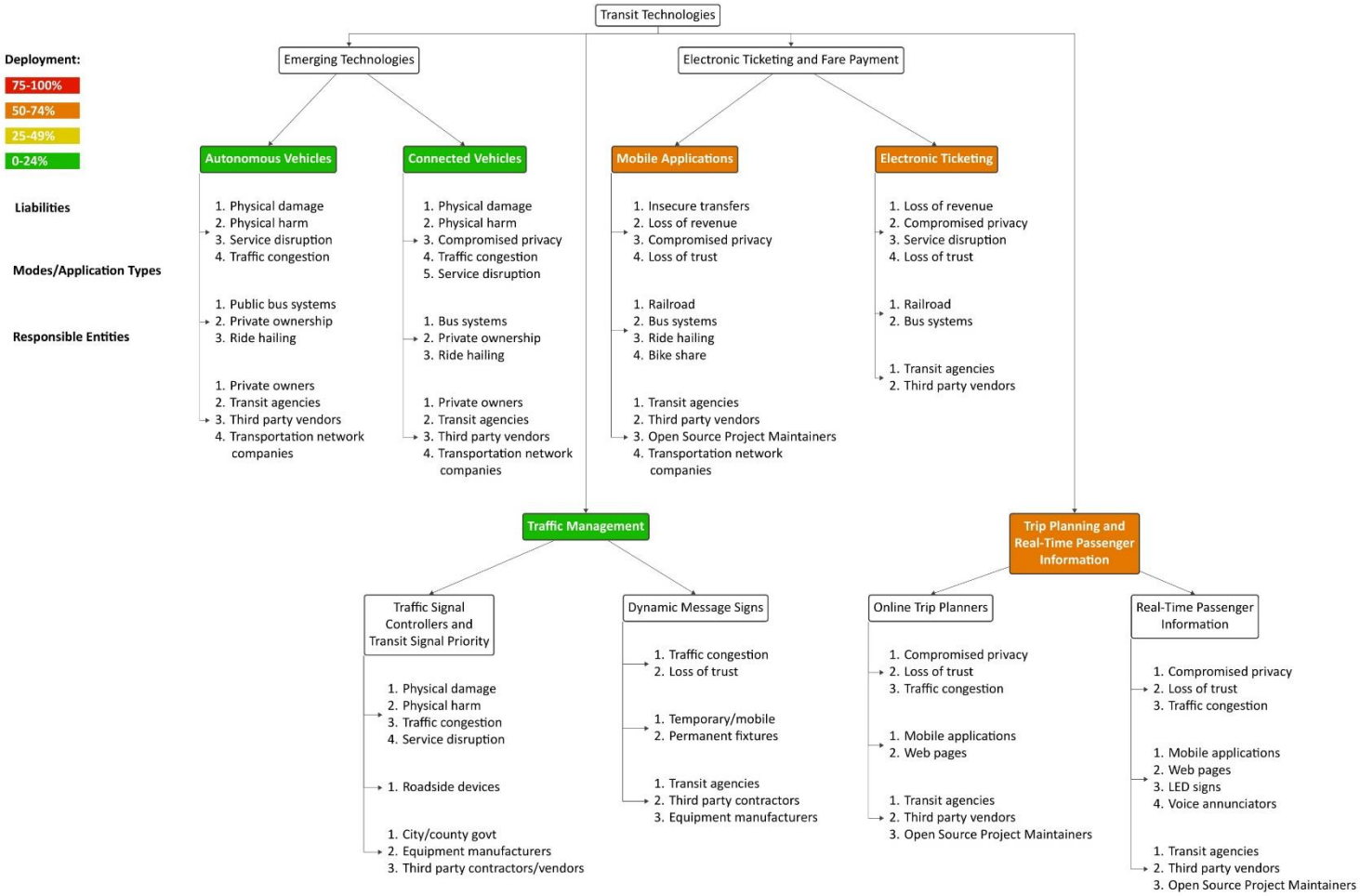

Figure 5.25 Taxonomy of Transit Technologies part 1

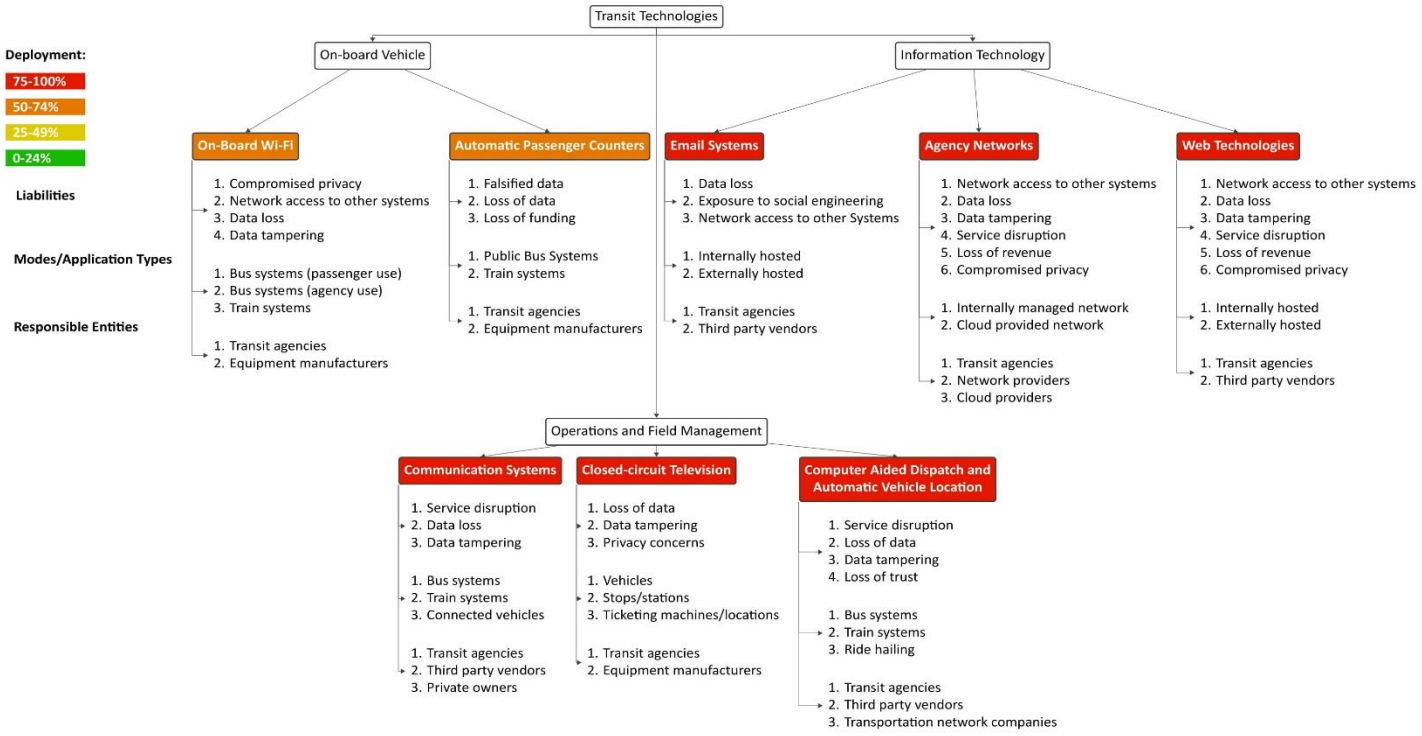

Figure 5.26 Taxonomy of Transit Technologies part 2

5.2.2. Transit Technology Common Vulnerabilities Taxonomy

Many of the vulnerabilities that appeared in the literature review are seen across multiple technologies, and so an additional taxonomy has been created to highlight these vulnerabilities. The vulnerabilities listed include attacks that are theoretically possible, as well as those that have been exploited in the past. Figure 5.4 shows the vulnerabilities which are present in three or more technologies in public transportation. The most common vulnerability in the taxonomy is Denial of Service (DoS), since many technologies now really on communicating with other devices.

DoS attacks can be made against a wide range of technologies that rely on communicating with other devices. DoS attacks attempt to make access to the system unavailable for authorized users by occupying resources. Jamming attacks are a type of DoS attack that can be performed against wireless mediums. Jamming attacks interfere with radio signals, typically by flooding the network frequencies with unauthorized noise.

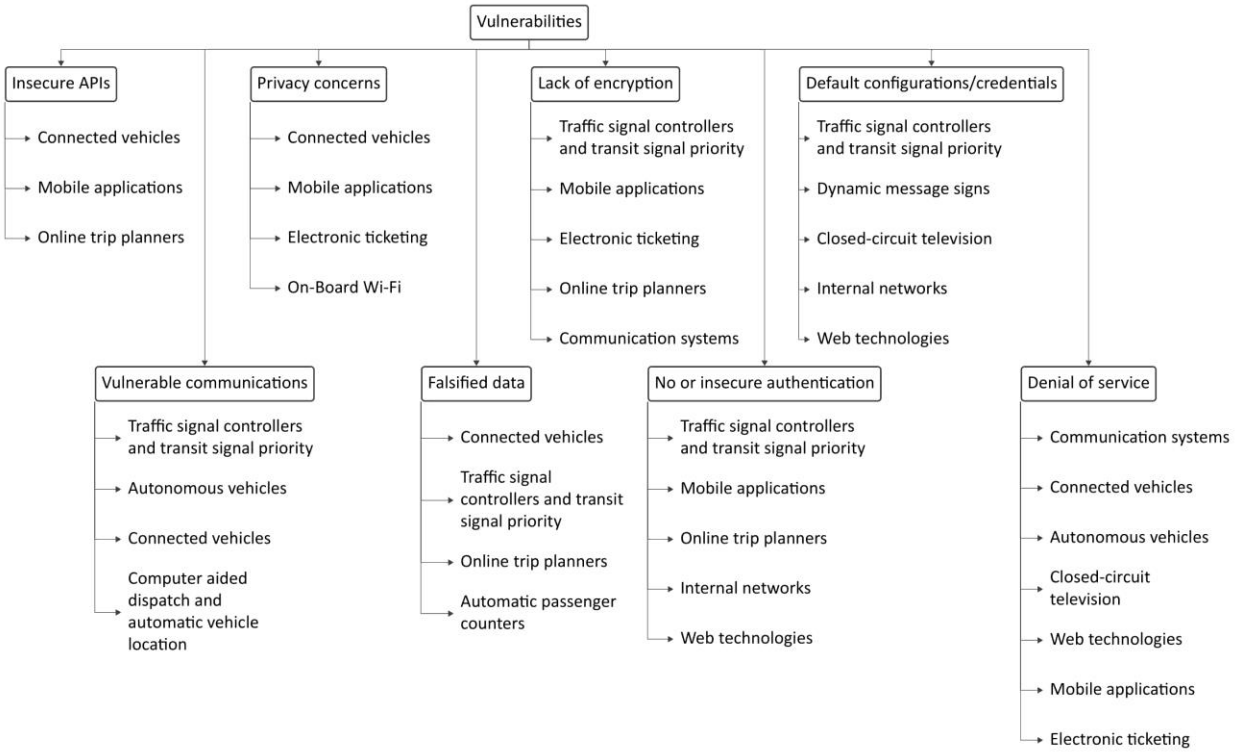

Figure 5.27 Transit Technology Common Vulnerabilities Taxonomy

Default configurations/credentials are present in traffic management technologies, CCTV, and information technologies. Default configurations may introduce insecure settings, and the default credentials for a particular device are typically easily accessible online, allowing an attacker to guess the right credentials and gain full access to the device.

Similarly, lack of proper authentication can allow an attacker to gain access to the system as well. Lack of proper authentication could refer to a communication protocol that lacks any authentication process, or that there are logical flaws in the authentication process that could be exploited to access a device without the proper authentication. Ghena et al. [7] showed that traffic control systems could be remotely attacked, and the communication protocol used had no authentication scheme.

Communication that lacks encryption may give an adversary the opportunity to steal sensitive data from a user. Electronic ticketing and fare payment technologies, online trip planners, and communication systems may have this vulnerability.

Falsified data, and privacy concerns are the second most frequent vulnerabilities in the taxonomy with four appearances each.

Falsified data attacks are possible against devices that collect information from the environment or users. In transit technologies, such as traffic light controller, CVs, and online trip planners, an attacker may be able to directly or indirectly cause traffic congestion. Automatic

passenger counters (APC) can also be subject to data falsification, but no literature was found examining APC security.

User privacy is also a concern in public transit. Compromised privacy can lead to sensitive user information being stolen (e.g., payment, location, and trip information). Privacy concerns are present for onboard Wi-Fi, fare payment technologies, and CVs.

Vulnerable communications, and insecure APIs are the third most frequent vulnerabilities in the taxonomy with three appearances each.

Vulnerable communication systems can be attacked in order to gain remote control over a system. Checkoway et al. [8] were able to gain remote control over a vehicle through vulnerabilities in the communication systems. It is possible that similar vulnerabilities may be present in autonomous and connected vehicles.

Application programming interface (API) provides an interface for data to be shared between devices. In mobile applications, the API is often set up as a web server that provides data when queried. Insecure APIs that fail to correctly authenticate a user may allow an attacker to collect sensitive data or perform actions they are not permitted to do.

The vulnerabilities described above can cause significant problems for the system owners. For example, if an attacker gains access to a traffic signal controller, the attacker can remotely control the intersection. While the Malfunction Management Unit (MMU), a hardware safeguard against erroneous programming that defaults to a flashing cycle if an unsafe state is detected, would prevent a green-on-green scenario, the attacker could set the intersection to another malicious logic state, which could result in traffic congestion or potential harm.

From the survey conducted as part of this project, communication systems were perceived as the most operationally critical technology for transit agencies. A denial of service attack against these systems may significantly disrupt transportation services. Denial of service or jamming attacks against the communication systems of an autonomous vehicle may cause the vehicle to be forced to a halt or take unsafe actions, which may cause physical damage to the vehicle or harm the occupants or the environment.

5.2.3. Emerging Technologies

Emerging technologies include connected vehicles (CVs) and autonomous vehicles (AVs). These are technologies that are currently being researched or developed, and have not yet been widely deployed. Figure 5.5 shows the section of the taxonomy classifying these technologies.

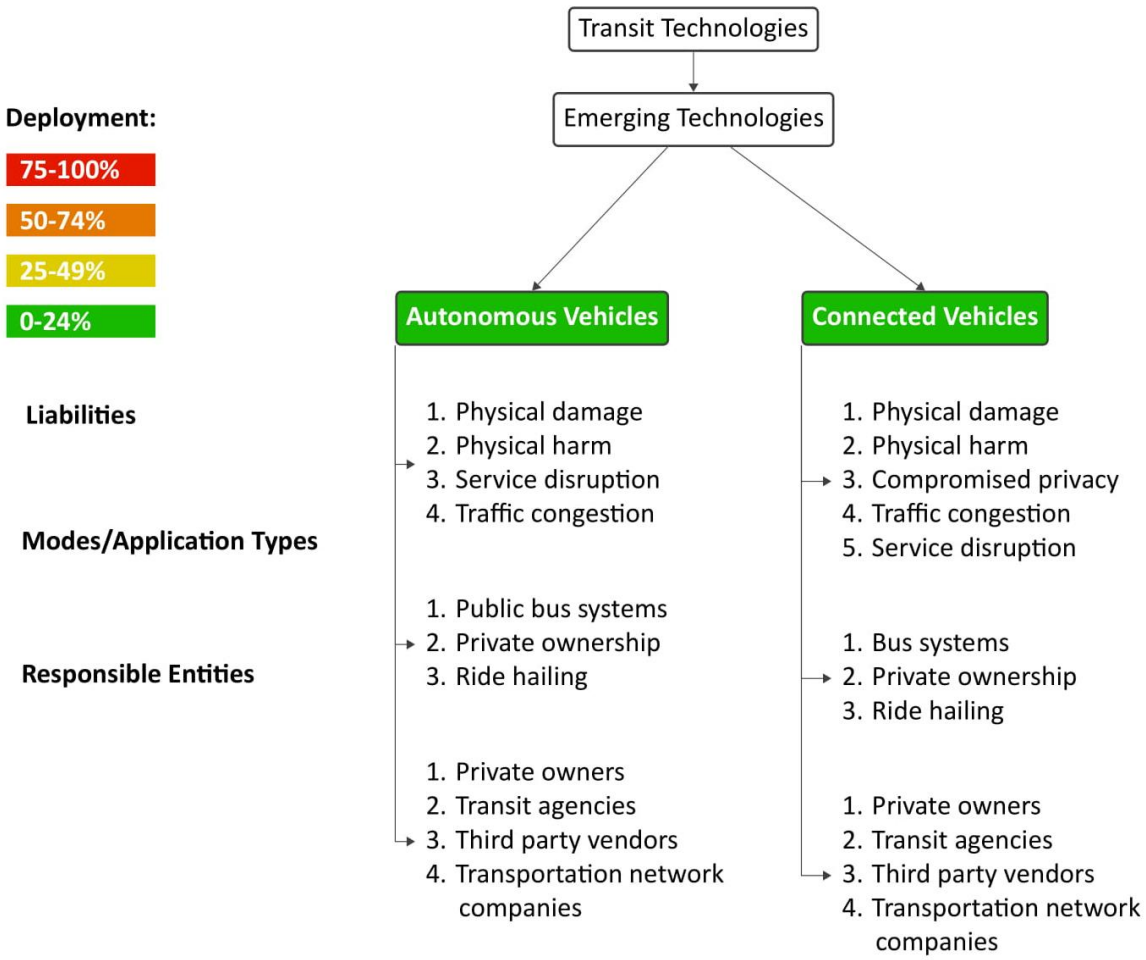

Figure 5.28 Emerging Technologies

5.2.3.1. Autonomous Vehicles

Autonomous vehicles (AVs) are private or public vehicles that provide automated control over at least one safety-critical control function, such as steering, without user input [118]. AVs can be owned by private users, and may also be used by transit agencies and private companies for public transportation. An autonomous shuttle service in Las Vegas has recently begun offering free rides as part of a pilot program [134].

Autonomous vehicles rely on a wide variety of sensors, including LiDAR and computer vision, to create a 3D map of the environment. An attacker may be able to cause an autonomous vehicle to make unsafe actions or unnecessarily halt by providing incorrect data to the vision systems. Jamming or otherwise preventing the sensors from detecting the environment may force the vehicle to a halt, disrupting service. Google researchers [88] [89] developed stickers with particular patterns can deceive artificial-intelligence algorithms used in computer vision. The adversarial images can be attached to traffic signs or other objects and may cause autonomous vehicles to behave unpredictably.

Autonomous vehicles can also be used by an attacker to create traffic congestion. By feeding false data to the AV, or by taking control of the vehicle, AVs could take actions that reduce the travel times of other nearby vehicles. The taking control of multiple AVs, an attacker can dramatically decrease the rate of travel of surrounding vehicles. A recent study [135] found that an attacker that controls only one percent of the vehicles on a road can increase the average trip time by 50%.

As agencies begin to adopt autonomous vehicle technology, they will need to collaborate with third party vendors to ensure proper configuration. In addition, agencies should carefully consider which scenarios they may be considered liable for by reviewing state and federal law, since the legal ramifications for malfunctions or accidents in autonomous vehicles are still evolving. Florida, in an attempt to attract companies developing AV technology, have been creating new opportunities for AV testing by lifting previous restrictions [136]. Federal agencies have also been pushing to ease restrictions on deployment of AVs nationally [137].

5.2.3.2. Connected Vehicles

Connected vehicle (CV) technology consists of a broad range of technologies that enable private or public vehicles to communicate with other vehicles, the road infrastructure, and the Internet. CVs improve the driving experience by providing advanced knowledge of the environment to the driver and vehicle. Applications include Intelligent Driver-Assistance Systems (IDAS) [103], Vehicle-to-Infrastructure (V2I) safety, and Vehicle-to-Vehicle (V2V) safety [104].

CVs have similar liabilities to those mentioned for AVs such as physical damage and harm, traffic congestion, and service disruption. Additionally, attackers may be able to recover private information about the vehicle or owner, such as travel time [117].

While personal vehicles are outside of the control of state agencies, agencies should still be aware of the increased attack surface that connected vehicles introduce. As agency vehicles begin to become increasingly connected, agencies and vendors will need to ensure that these vehicles observe recommended security practices, such as employing encryption, and are configured correctly. Additionally, local government will likely ultimately own the "infrastructure" access point for V2I applications, and therefore this exposes a potential attack surface on the government's network.

5.2.4. Traffic Management

Traffic management technologies consists of technologies designed to improve or control the flow of traffic. Figure 5.6 shows the taxonomy for traffic management technologies. Traffic signal controllers and Transit Signal Priority (TSP), and Dynamic Messages Signs (DMS) fell into this category.

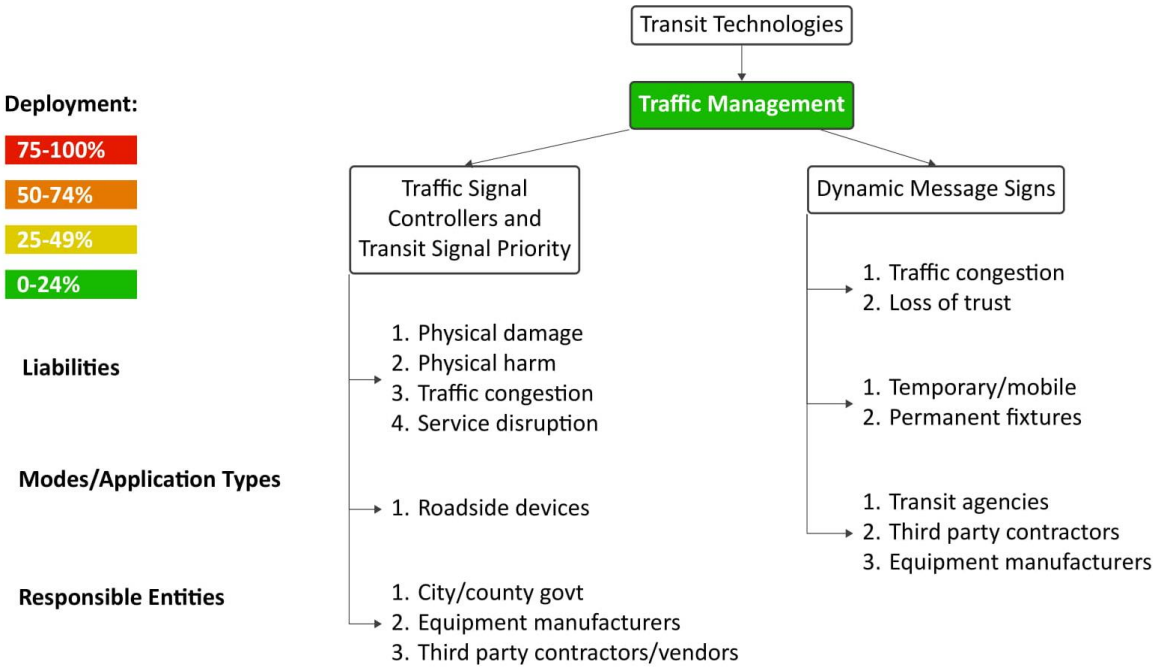

Figure 5.29 Traffic Management

5.2.4.1. Traffic Signal Controllers and Transit Signal Priority

Traffic signal controllers are responsible for managing traffic signals at intersections, and are located near the intersection. Traffic Signal Preemption and Traffic Signal Priority (TSP) decreases the time transit vehicles (e.g., buses) spend waiting at traffic lights by facilitating movement through the intersection [56]. TSP may reduce transit delay and travel time, and improve reliability.

Traffic signal controllers and TSP technologies are not widely deployed among the transit agencies according to the survey results. Out of 25 agencies, they are deployed in three and two agencies, respectively. Five out of 19 agencies responded that they are planning to deploy TSP. However, as mentioned earlier the survey respondents were primarily transit agencies, and these results may not reflect the true distribution of these technologies which in many cases would be primarily maintained by the city or county government.

The traffic signal controller is responsible for light cycle logic. These devices can support remote access through a wireless network. An attacker that gains access to the system may be able to set malicious logic or disrupt TSP service, which may cause traffic congestion. While the Malfunction Management Unit (MMU), a hardware safeguard against erroneous programming that defaults to a flashing cycle if an unsafe state is detected, should prevent a green-on-green scenario, malicious lighting programming may increase the likelihood of an accident.

In particular, red/red flashing signals have not been shown to have a significantly higher rate of accidents, but the yellow/red flashing state, often used when large roads intersect with

smaller roads, have shown an increase in right angle collisions [138]. Road accidents may cost 0.3% to 2.8% of the gross national product, not to mention the potential loss of life as well [139].

5.2.4.2. Dynamic Message Signs

A Dynamic Message Sign (DMS) serves as the primary means of communication between agencies and en route travelers. DMSs are used by transit agencies to display estimated arrival times and delays at transit stations [72]. Due to the ease of physically accessing DMSs, DMS tampering has become a popular prank, with online guides detailing the process [77].

DMSs are often deployed by third party contractors. Managing access to these systems can be complicated, and often these systems are left unlocked to allow ease of access.

Online guides [77] have been published on the Internet giving detailed instructions on how a layperson can change the message of DMS, and such attacks continue to occur as of October 2018 [78]. These attacks may result in traffic congestions by confusing motorists with misleading messages. In addition, travelers may lose their trust in future DMS messages they see and to the agencies who are responsible for entering the messages.

5.2.5. Electronic Ticketing and Mobile Payment

Electronic ticketing and mobile payment technologies provide riders with more convenient forms of fare payment. Fare payment technologies were rated one of the most financially critical technologies by transit agencies in the survey conducted as part of this project. Figure 5.7 focuses on the electronic ticketing and mobile payment technologies in the taxonomy, electronic ticketing, and mobile fare payment applications.

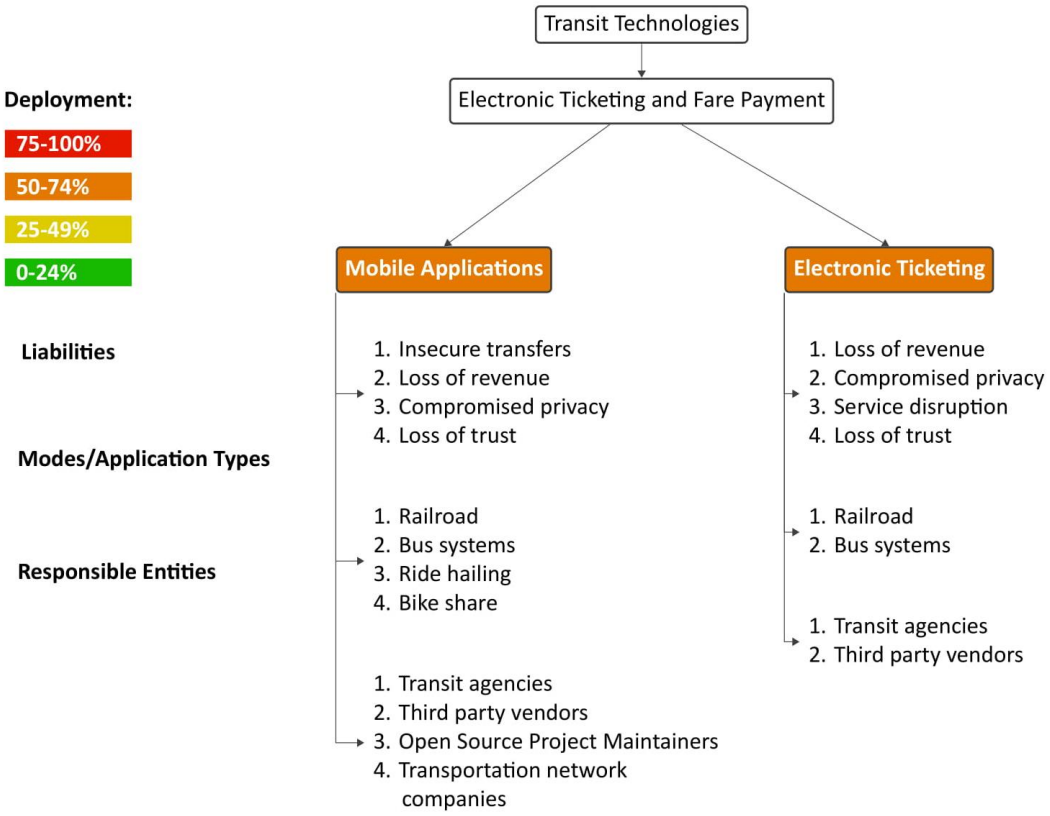

Figure 5.30 Electronic Ticketing and Fare Payment

5.2.5.1. Mobile Fare Payment Applications

Mobile fare payment is a form of contactless electronic ticketing that enables riders to purchase a ticket and validate the purchase using their mobile device. Mobile fare payment is typically added as an additional, more convenient fare payment option, rather than replacing existing options entirely [3, p. 36].

Many mobile fare payment applications are developed by third party vendors, who may also manage the application. These vendors may provide similar mobile fare payment applications for multiple agencies. When a rider boards, the tickets are often visually validated by the vehicle operator, but QR codes or other techniques may also be used to programmatically validate passes.

Visual validation schemes may provide opportunity for attackers to duplicate and share the visual tickets with others. This would allow riders to access transit agency services without paying the fare, which may result in a loss of revenue for the agency.

Attacker may also be able to retrieve information on other users by exploiting vulnerabilities in the application, or gather information from insecure financial transactions. Private user information could also be stolen through Trojan applications that mislead users by masquerading as other applications [55]. If a user provides their credentials to the fraudulent

application, the attacker may be able to access private user information, such as credit card information and travel history from the legitimate app or database. If stored incorrectly, the retrieved credit card information could also be used for fraudulent money transfers.

Mobile fare payment apps are also widely used in transportation network companies (TNCs) (e.g., Uber, Lyft). Ride hailing has become very popular in recent years, bringing an increase in the number of people using mobile fare payment apps and the number of transactions through these applications. As these applications continue to gain popularity, the greater the likelihood that transit payment apps are targeted for exploitation.

5.2.5.2. Electronic Ticketing

Electronic ticketing, or e-ticketing, is a broad term for ticketing systems that rely on any form of electronic device to provide proof of ticket purchase. Four generations of ticketing systems exist, often coexisting in the same city or agency, with the most recent three categorized as electronic ticketing: paper tickets or tokens, magnetic ticketing systems, contactless tickets, and mobile ticketing systems [37].

A survey from 2016 [3, p. 28] reports that 54% of the Florida agencies surveyed make use of magnetic stripe tickets or farecards, and 15% use smart cards. Electronic ticketing systems "offer a large range of possibilities to make public transport easier to use, to manage and to control" [37, p. 8].

Many older forms of electronic tickets have information stored on the ticket itself, such as value of the available balance and may not be encrypted. An attacker could tamper with the device to modify the stored values. However, most cards today employ encryption and validate the information against a database when the ticket is read. If someone tampers with the ticket or disrupts the connection between the ticket scanner and agency server, agencies may lose revenue and service may be disrupted.

Smart cards that are implemented with a contactless system may be scanned from a short distance. This may put the private user information stored on the card at risk of being stolen. Kerschbaum et al. [46] describe how an attacker can retrieve a rider's travel records from the EZ-Link smart cards by scanning the card from a short distance. The distance depends on the technology used, but most attack scenarios assume an attacker walking within arms reach of the user holding the device.

5.2.6. Trip Planning and Real-Time Passenger Information

Trip planning and real-time passenger information allow riders to access find directions and access information about transit vehicles from a wide variety of devices. These technologies are often used in conjunction with Automatic Vehicle Location to provide riders with information on the real-time location of transit vehicles. Figure 5.8 shows the section of the taxonomy for online trip planners.

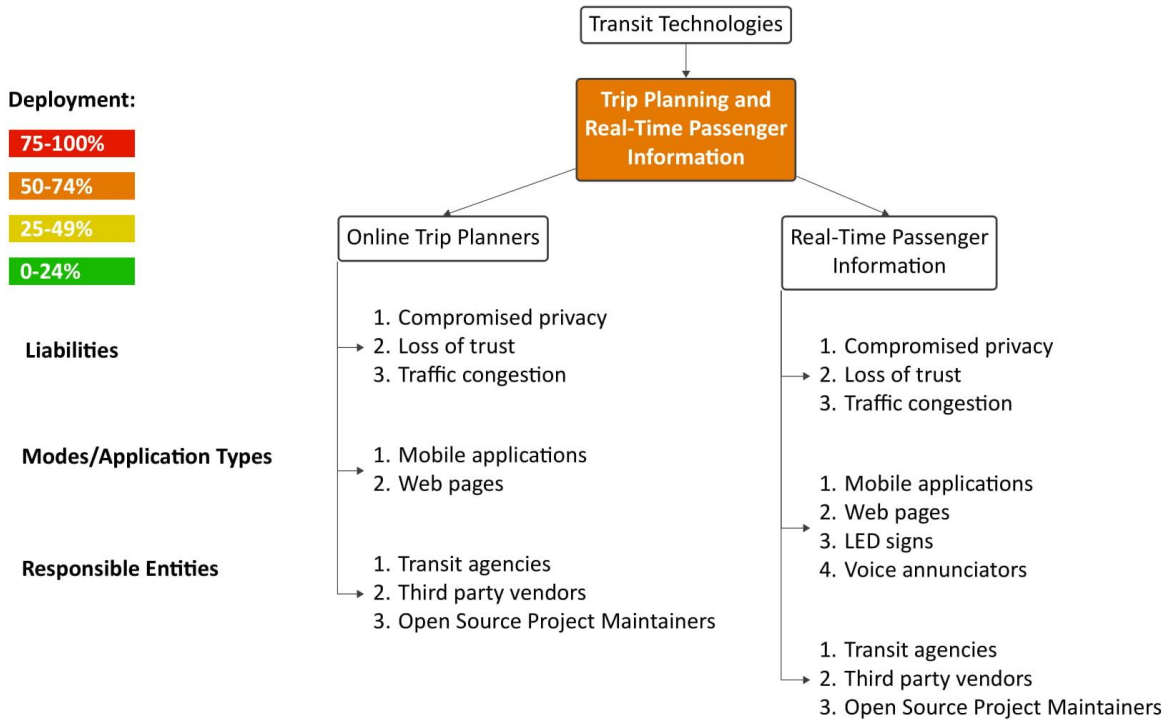

Figure 5.31 Trip Planning and Real-Time Passenger Information

5.2.6.1. Online Trip Planners

Online trip planners assist riders by creating step-by-step directions to a given location using a source and destination provided by the user. This information may include real-time information about the vehicles or route, such as position or arrival times, which enables users to make more informed decisions. Since several online trip planners will provide multimodal directions, the taxonomy lists the various different formats that online trip planners may take instead of providing the mode of transportation.

If an online trip planner stores information about rider history, an insecure planner may be used by an attacker to gather personal information such as location and travel patterns. Loss of trust and traffic congestion are other scenarios that may arise due to data tampering. Riders who are led astray by a defaced planner may stop using the application, and riders may be redirected to busy routes, increasing the level of congestion at those locations.

Since many online trip planners are used to decide on a particular route or method of travel using real-time information, an attacker may be able to influence riders to change their travel patterns by changing the data or otherwise presenting false information to the user. For example, users who may typically ride the bus may be convinced to take an alternate form of transport, such as ride hailing or private vehicle. If many users make this decision, traffic conditions may become congested.

Open source applications are becoming increasingly popular in this area with applications such as OpenTripPlanner and OneBusAway [25]. Just as third party vendors are responsible for patching vulnerabilities in closed source software, the community is tasked with repairing any vulnerabilities that appear in open source applications. For actively maintained projects, vulnerabilities that are discovered may be repaired quickly by the community, but abandoned projects may never be patched. Just as agencies must be aware of the support lifetime for software from vendors, they should also monitor the support for any open source projects they implement.

5.2.6.2. Real-Time Passenger Information Systems

Passenger information systems are automated systems used to provide passengers with information through visual, audio, or other media. Real-time passenger information systems are passenger information systems that update the information provided to users in real-time. With the growth of IoT devices, LED displays and Automatic Voice Annunciation (AVA) systems can now be updated remotely in real time. In addition, to better accommodate users, updates can now received directly from a user's personal device via web or mobile applications. This wide range of technologies leads to real-time passenger information systems sharing the liabilities, modes, and responsible parties of dynamic message signs and mobile applications.

For physical information systems, such as LED displays inside vehicles, physical access is a concern as they are similar to DMS systems. While it may be harder for attackers to tamper with these devices because of the increased presence of agency or city employees, attackers have been able to gain access to populated areas [41]. Tampered devices may lead to a loss of trust in customers who see or hear of this "electronic graffiti".

With the increased level of connectivity, attackers may also be able to collect private data, such as location, from customers as described in online trip planning.

5.2.7. Onboard Vehicle Technologies

Onboard vehicle technologies refer to devices that extend the capabilities of transit vehicles. The taxonomy examines onboard Wi-Fi, which allows riders to access the Internet from the vehicle, and automatic passenger counters, which counts the number of riders as they enter or exit the vehicle. Figure 5.9 shows the section of the taxonomy on onboard vehicle technologies.

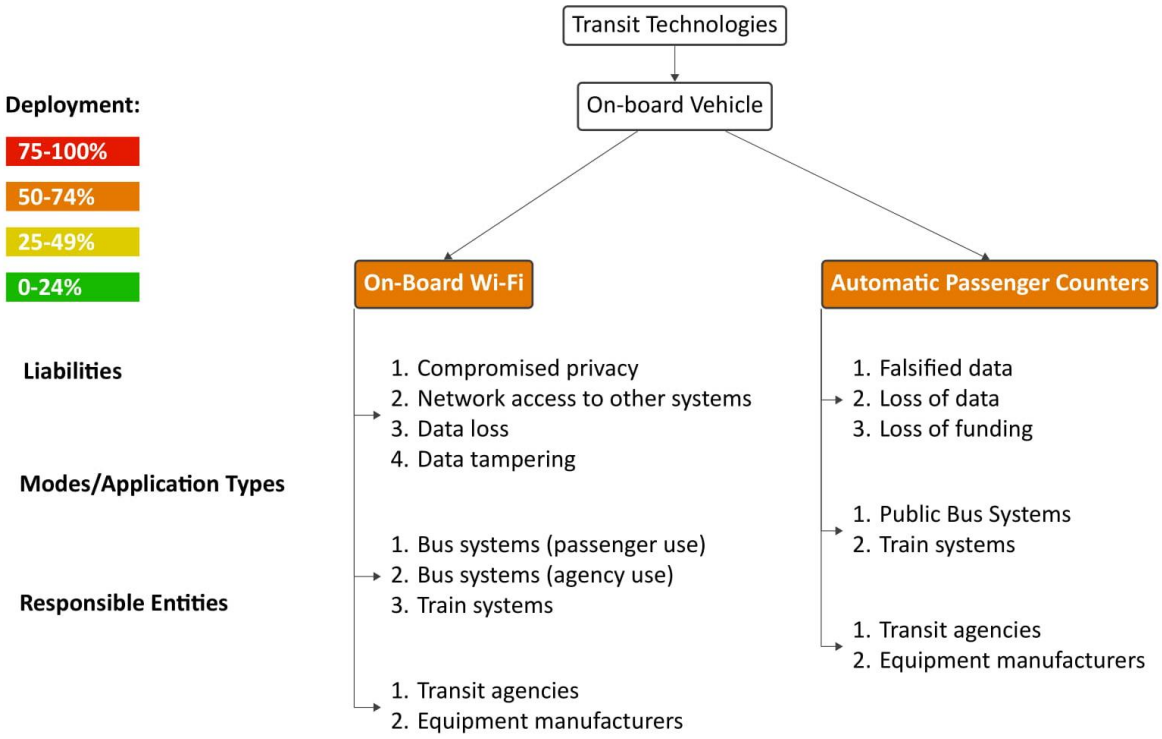

Figure 5.32 Onboard Vehicle Technologies

5.2.7.1. Onboard Wi-Fi

Onboard Wi-Fi offers transit passengers the ability to wirelessly connect to the Internet using a mobile device, such as a smartphone or laptop. This addition makes transit options more attractive to riders. As in traditional Wi-Fi networks, a wide range of potential attacks exist to eavesdrop on connections.

While privacy is the primary concern here, onboard Wi-Fi may also provide an attacker with a way to attack other systems or tamper with data. Onboard Wi-Fi may be used to provide a more convenient interface to transfer data, such as automatic passenger data, or to update bus systems when the bus returns to the agency. If these updates are not properly validated, an attacker may be able to cause malware to be installed. Additionally, if the onboard Wi-Fi network isn't correctly isolated from critical bus systems such as onboard network used for vehicle control or automatic vehicle location connection to a server, an attacker could potentially access those critical systems from the onboard Wi-Fi connection. Agencies will be responsible for keeping these systems correctly configured and up to date, while vendors will be responsible for patching new vulnerabilities and distributing updates to agencies.

5.2.7.2. Automatic Passenger Counters

Automated Passenger Counters (APCs) record the number of passengers that board and disembark from a vehicle. A survey conducted in 2008 [99] found that APCs are primarily used to collect ridership data for a given route (including tracking ridership changes), but many

agencies also use this data to evaluate performance at individual stops as well as adjusting schedules based on ridership [99, p. 1].

No papers could be found that discussed APC security in detail. However, potential liabilities include loss of data, incorrect data, or loss of funding if ridership data is a critical requirement for new funding. An attacker could theoretically perform a jamming attack on the APC or provide the device with false data. Federal funding is allocated to transit agencies based in part on ridership data [101], and agencies must validate their use of APC data for National Transit Database ridership reporting every three years. Thus, corrupted APC data could potentially force the agency to use an alternate means of reporting ridership until the APC data could be proved to be reliable again when the next validation year arrives [102].

5.2.8. Operations and Field Management

Operations and field management refers to technologies that enable an agency to manage their equipment that is deployed in the field, such as vehicles and ticketing machines. Figure 5.10 shows the taxonomy for operations and field management technologies, including communication systems, closed-circuit television, computer aided dispatch, and automatic vehicle location.

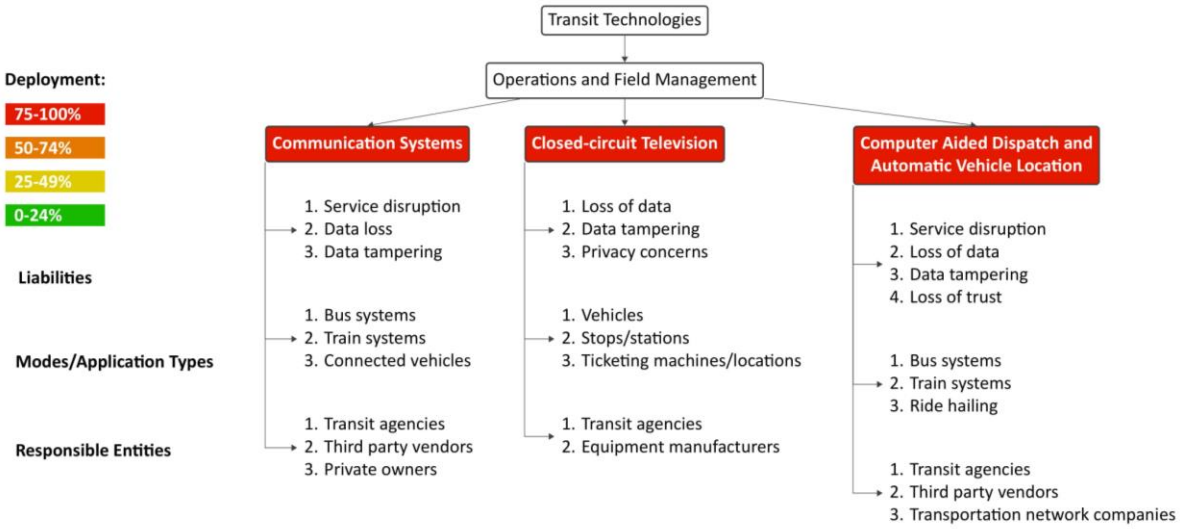

Figure 5.33 Operations and Field Management

5.2.8.1. Communication Systems

Communication systems, such as Wi-Fi, Ethernet, cellular networks, and radio, provide agencies with a means of quickly exchanging information with distant technologies. Every technology in the taxonomy has some means of communication, and many of them require such communications to fully function. For example, fare payment equipment on the vehicle must communicate with a server to validate a ticket purchase, and connected vehicles gather information about the environment from roadside beacons.

As connected vehicles continue to become more popular, private owners gain more direct access to new communication systems. Agency infrastructure that communicates with connected vehicles may become a potential attack surface, which is described in more detail in the section on connected vehicles.

Since so many technologies require on being able to communicate, service disruption may be quite costly. Agencies are primarily responsible for ensuring the correct configuration and deployment of these systems, while the equipment vendors will be responsible for patching identified vulnerabilities. Since some vulnerabilities are exposed to the public before vendors have a chance to distribute an update, agencies may need to take temporary precautions. Online resources like forums for the particular technology are a way to stay up to date on current trends.

5.2.8.2. Closed-Circuit Television

Closed-circuit television (CCTV) allow agencies to monitor their equipment and assist in incident response, as well as review evidence after-the-fact when investigating issues related to passengers or vehicle operators. Since CCTV may be found in any form of transportation, mode refers to the different locations that CCTV may be found. Transit agencies or their vendors can install CCTV cameras on agency vehicles, street intersections, vehicle stops, and stations, next to ticket vending machines and other infrastructures. The survey results show that CCTV cameras are widely deployed among Florida transit agencies (in 16 out of 25 respondents). They are also considered to be one of the most operationally and financially critical technologies.

Attackers that gain unauthorized access to the camera recordings may be able to tamper with the data, or compromise the privacy of individuals who may have been recorded. Costin [85] discusses vulnerabilities in online video surveillance systems such as default credentials, which were used by 40% of online cameras, allowing attackers to gain access to these systems. Disrupting the service of CCTV systems (e.g., physically damaging the camera or a jamming attack during data transmission) may also cause data loss.

Agencies are responsible for ensuring that CCTV records are properly backed up and encrypted to avoid unauthorized access and loss of data. Agencies are also responsible for maintaining and configuring the camera systems. The equipment manufacturers are responsible for providing updates to vulnerabilities found in CCTV systems.

5.2.8.3. Computer-Aided Dispatch and Automatic Vehicle Location

Automatic Vehicle Location (AVL) systems allow transit agencies to track the location of a vehicle in real time, and Computer Aided Dispatch (CAD) systems work closely with AVL technologies to provide transit agencies the ability to manage their fleets in real time, including tracking transit routes, trip orders and vehicle assignments.

Vehicle location data is often provided to riders through mobile applications that offer trip planning and real-time arrival information. Disrupting these services may reduce ridership,

and lead to a loss of trust in the accuracy in these systems. If the CAD service is taken down, continued operation will take significantly more effort. In Baltimore, when the police CAD system was taken down, the city was forced to record incidents by pen and paper, and lost about 22 hours of recorded calls [140, 141]. However, response times were not noticeably impacted.

5.2.9. Information Technology

Information technology refers to the technologies used in storing, retrieving, or sending information, such as email. Since these technologies are deployed at agencies, and are not bound to specific forms of transportation, mode in this section refers to the different types of organizations these technologies may take. Figure 5.11 shows the taxonomy for information technology.

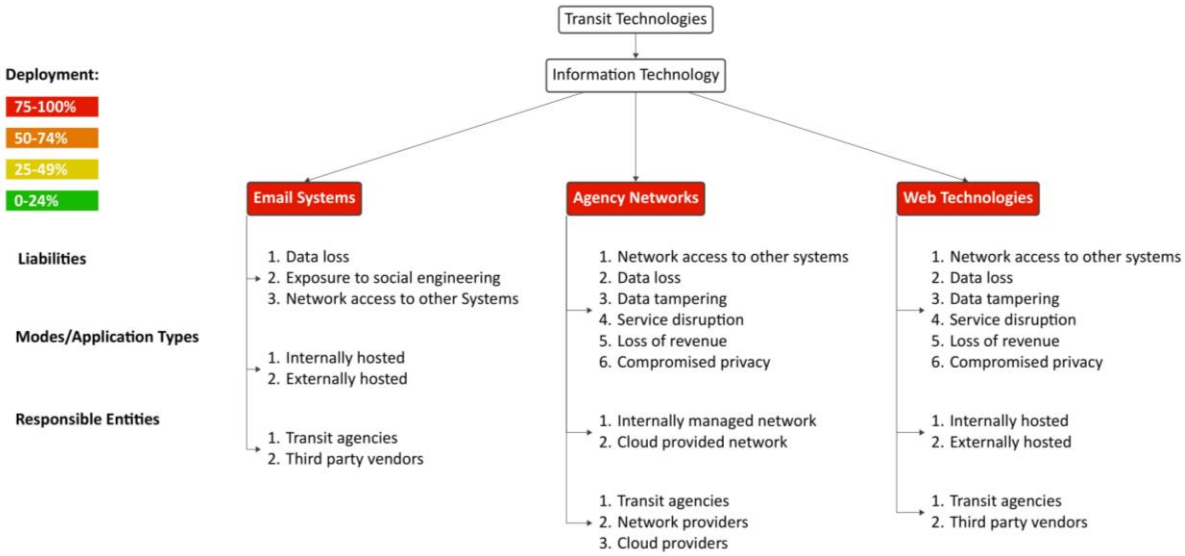

Figure 5.34 Information Technology

5.2.9.1. Email Systems

Email is a common vector for cyber attacks due to the convenience and scalability of attacks on these systems (e.g., phishing attacks). Phishing is often conducted by sending emails with urgent requests for information or tempting offers that aim to convince the victim to provide information at a web link provided in the email. From the 2017 survey [14] results released by the Florida Center for Cybersecurity [15], phishing attacks were considered the greatest security risk by stakeholders in government, academia, and business. Successful phishing attack may result in leaked sensitive data of both an individual employee and the whole company, infecting the company system with viruses, including ransomware. Ransomware is a form of malware that prevents the normal operation of a computer system and typically demands payment in virtual currencies (e.g., Bitcoin) to restore functionality [18].

From the survey that was conducted as a part of the project, one of the participants mentioned that their agency was receiving emails with phishing attempts:

"Over the course of the last 6-12 months multiple attempts at phishing across our employee base has taken place."

Agencies are responsible for ensuring their employees are properly trained to recognize and avoid dangerous emails and phishing attacks. Larger state agencies such as the Florida Department of Transportation (FDOT) may help by ensuring that high quality training materials are distributed to transit agencies. Many training materials are readily available online and could be gathered and distributed by FDOT or transit agency personnel.

Bring your own device (BYOD) refers to the policy of allowing or encouraging employees to use personal devices in the workplace or at home to access company resources, such as email. If these personal devices were compromised by an attacker, the attacker may be able to exfiltrate information that the personal device has access to. For cyber incidents in the transportation industry, the average cost is $121 for each record [1, p. 2].

5.2.9.2. Agency Networks

Agency networks may be implemented internally, cloud provided, or a combination of the two. These networks are supporting an increasing number of more complex devices in order to improve the efficiency and convenience of agency operations. The majority of the services provided by the agencies for their customers and employees (e.g., fare payment and online trip planning for mobile apps, employee emails, communications, etc.) communicate through the agency's network.

Due to the number of technologies that communicate through the network, attacks that disrupt the network may be quite costly, resulting in disruption of agency services and possible loss of revenue. An attacker with access to the network may also be able to gather sensitive user data stored by the agency, and may attack other services from inside the network.

Agency machines may also be compromised with the intention of using them as part of a botnet. The term botnet refers to a collection of computers or devices (often called "bots" or "zombies"), typically connected to the Internet, that an attacker has compromised and controls, often through the use of malware. Botnets can be used to stage attacks on other systems, such as a distributed denial of service (DDoS) attack. A DDoS attack is performed by using many different devices to simultaneously consume resources and prevent authorized users from accessing the system (e.g., by rapidly connecting and leaving the connection "hanging"). A new trend is to use these computers for cryptojacking, where a machine is used to perform cryptomining without the authorization of the user. In either scenario, the agency would expect to see delays in service as the malware consumes CPU cycles. In the worst case scenario, the agency servers may need to be temporarily brought down to prevent the spread of malware or other attacks [142].

Insider threats are consist for nearly 75% of security breach incidents [143]. Insider threats refer to employees or other authorized users that intentionally or accidently create security holes, access information without proper authorization, or damage equipment and software. Insiders often already have access to sensitive infrastructure, and this may make them more dangerous than outsiders. Agency employees should be properly trained to recognize insider threats, and should regularly check log files for potential signs of misuse.

In the case of a ransomware attack, the agency may either pay the ransom or restore the data from their backups. If the backups were not made, then it may be better to pay ransom and take steps to be prepared for these kinds of situations in the future. If an agency does decide it is financially wise to pay the ransom, they should be aware that the attackers may not release the data, and may not remove their presence from the network. This strategy was shared by Yarrow Point Mayor Richard Cahill [144] after Yarrow Point was the victim of a ransomware attack on the town computer systems. In this scenario, the attackers wanted nearly $10,000 in ransom. For cyber incidents in the transportation industry, the average cost is $121 for each record [1, p. 2]. According to the conducted survey results, Florida transit agencies backup their systems at least once per month.

5.2.9.3. Web Technologies

Web technologies include web servers, software, and other technologies used to create a web site or application. These technologies are well-known, and extensive vulnerability research has been conducted on web technologies. They may be popular targets for attackers because of the many automated tools exist to exploit these systems, their familiarity to a potential attacker, and the ease of access over the Internet. External web servers managed by a cloud provider may still be used to attack an internal network if the server communicates with the internal network.

These sites may contain customer data, and agencies should properly encrypt and backup any data they collect. In addition, web servers often communicate with other devices on the network, such as querying vehicle information to provide to riders. Attackers may use a vulnerable server, which could potentially be hosting non-critical content, as a pivot to attack other critical systems in the agency's network. In other words, good security practices such as frequent software updates should be applied to all servers in the agency network, even if the server is perceived as being less critical. Disrupting web services may lead to a loss of revenue if technologies such as mobile fare payment depend on them. In the survey conducted for this project, one agency responded "Hacking of the Company website and Facebook page" when asked about past cybersecurity incidents.

The agency that owns the website will ultimately be responsible for ensuring the proper configuration and backup systems for the site. Cloud providers may offer hosting and certain security services, but the correct operation and security of the site may still be the agency's responsibility. Whenever technology is hosted on a cloud provider, the agency should have a

clear understanding what software components the agency is responsible for updating and which will be maintained by the cloud provider.

5.3. Summary

A taxonomy classifying transportation technologies has been developed, which partitions technologies based on five dimensions: extent of deployment in Florida, mode of transportation, functionality, responsible organizations, and liabilities. Communication systems and 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 CAD/AVL and mobile fare payment are also widely deployed, and have many critical liabilities. Mobile fare payment apps are being deployed by transit agencies nationally at an increasing rate. Given the intersection of revenue collection for the agency and transit rider payment information on privately-owned devices, mobile fare payment apps are a critical technology to examine in detail. Onboard Wi-Fi is under consideration by more than 35% of survey respondents that have not deployed it, making it an important technology to analyze further as well.

CHAPTER 6: WORKSHOPS

6.1. Introduction

As described in earlier parts, one of the primary objectives of the research project is to facilitate ongoing cybersecurity information exchange among Florida transit agencies, their vendors, and cybersecurity researchers. Successfully facilitating discussions between these parties would further encourage cybersecurity awareness in the field. To meet this objective, the research team organized monthly working group meetings for agencies and cybersecurity professionals and held three workshops focused on cybersecurity in public transportation.

This section describes the workshops and major findings from each of the workshops. The section begins with a brief introduction to the different workshops, followed by a deeper analysis of each of the workshops. Each section will include a description of the material presented, major discussion points, and details about the workshop, such as date, attendance, and agenda.

6.1.1. Workshop Overview

The research team organized two different types of workshops. Two of the three workshops focused on student involvement with hands-on sessions and exposure to transit technology. These workshops gave students an opportunity to investigate vulnerabilities and mitigations in transit systems. The third workshop focused on bringing together cybersecurity researchers and transit agency expertise to provide cybersecurity researchers an opportunity to review technical architectures and implementations of transit technologies, and to provide feedback on potential attacks and mitigations based on their specific areas of expertise. Both types of workshops included participation from the Florida Center for Cybersecurity, cybersecurity graduate students, and transit agencies.

The first event was a hands-on session examining mobile fare payment applications in public transportation systems. The session began with an introduction to transportation technologies, mobile fare payment, the Android operating system, and reverse engineering applications made for Android devices. After the introductory presentation, students were given the opportunity to set up their own test environment on their personal devices and examine publicly available mobile fare payment applications. The workshop was held November 9th, 2018.

The second event was also a hands-on student session. The workshop focused on vulnerability discovery and analysis for traffic cabinet technologies with an emphasis on the traffic signal controller. The research team began the workshop event with an introduction to the technologies contained within the traffic cabinet followed by a presentation on vulnerabilities found in the traffic cabinet by Mission Secure, Inc. After the event, students were

given the opportunity to interact with the traffic cabinet donated by the City of Tampa. The workshop was held January 25th, 2019.

The final event brought together faculty from various Florida universities to present their research to other faculty researchers, graduate students, and transit agencies. Participants introduced their research and how the research relates to cybersecurity in public transportation, allowing questions at the end of their presentation. Each participant also acted as a scribe, recording session notes for an assigned presentation. The workshop was held May 7th, 2019.

6.2. Mobile Fare Payment Workshop

The first workshop organized by the research team focused on giving students a hands-on opportunity to analyze vulnerabilities in mobile fare payment applications and was hosted November 9th, 2018[4]. Attendance was estimated at 17 participants, including 16 students from the Whitehatters Computer Security Cub (WCSC) and a representative from SOFWERX.

6.2.1. Overview

The workshop began with a brief introduction of the research project and the purpose of the workshop. The research team then gave a presentation on mobile fare payment applications and the common implementations discussed in the literature review, including visual validation and QR codes. With the introductions completed, the team then presented common vulnerabilities that may be present in mobile fare payment applications, including a review of the vulnerability and liability taxonomies developed as part of this project and a short description of the vulnerability discovered by the team in a mobile fare payment application deployed in Florida. The vulnerability was not covered in detail, as it had yet to be patched by the vendor.

Students were introduced to the Android [146] operating system and several tools needed to perform a vulnerability assessment for an application. The workshop covered Android system internals, the Android PacKage (APK) file format, and the Dalvik Virtual Machine, including a demonstration of the Android Debug Bridge (ADB). The students were then introduced to smali, a disassembler for examining the code contained in an APK, and APKTool [147], a reverse engineering tool for APK files through a live demonstration.

[4] The research team originally intended to coordinate a collaborative security analysis event with the Hillsborough Area Regional Transit Authority (HART). The original event would still include mobile fare payment applications, but would have given students the opportunity to investigate the technologies on one of HART's buses by bringing one of the buses to the university. However, shortly before the event, HART had to delay the event due to concerns about the necessary time for their vendors to address any potential issues. As of this writing, HART is still interested in hosting a similar event with the research team, but have been unable to secure a response from all of their vendors. So far Cisco is the only vendor that has provided a definite policy for addressing issues (90 days to address issues) [145].

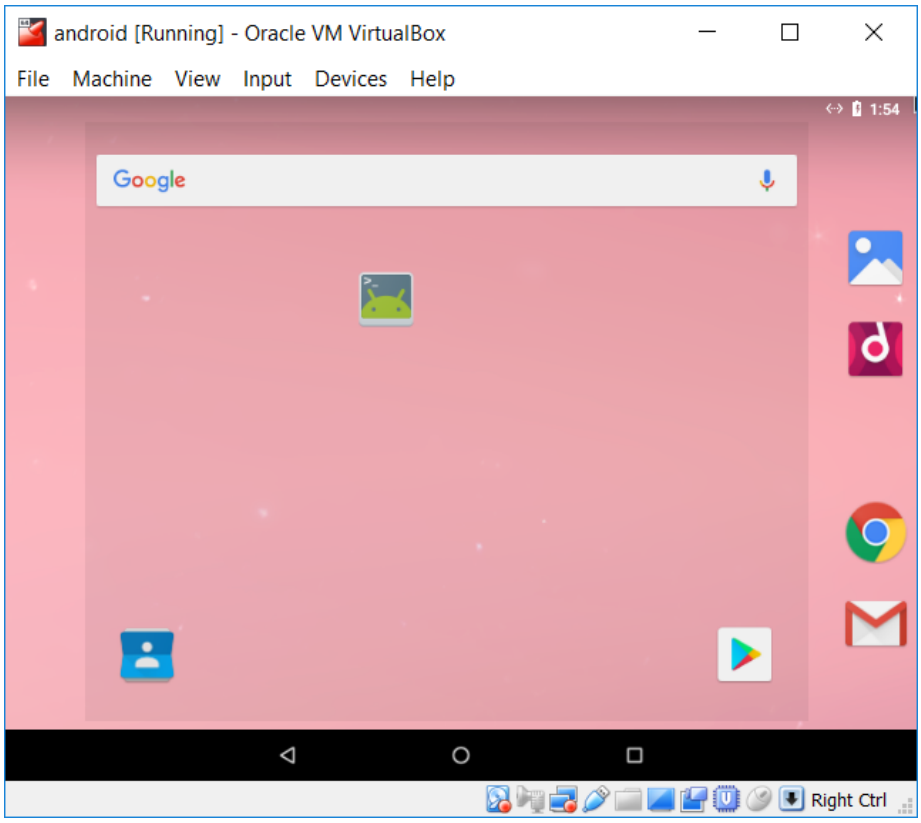

Figure 6.1 Android virtual machine for evaluating mobile fare payment apps

The demonstration included altering the name validation on an application installed on an Android device. While altering the name validation was not dangerous, it introduced the skills necessary for more complex analysis and the potential vulnerabilities an attacker may exploit, including creating trojan horse applications, bypassing visual validation schemes by re-using existing code, or gaining access to data hidden in the application.

The workshop concluded with a hands-on session where students were encouraged to practice the skills taught in the workshop. A link to download the necessary tools and a example virtual machine set up by the research team were provided to the students. Virtualbox [148] was used to run the virtual machine because it is a familiar tool for WCSC members. Figure 6.1 shows the virtual machine running in Virtualbox. The research team provided support for the students as they set up their own testing environments, answering any installation questions.

6.2.2. Outcomes and Discussion Points

During the presentation, the students and the research team discussed several areas of potential interest, including QR codes in airlines, the technical limitations of visual validation and QR codes, and new potential vulnerabilities.

After discussing QR codes in mobile fare payment applications, students asked the research team about QR codes used in tickets for airlines. Students discussed the potential for

similar attacks used on mobile fare payment applications to be applied to QR codes in airlines. In addition, the students and the research team discussed why visual validation is not a useful scheme for airlines. These reasons included more expensive fare and greater risk. This may be a potential area for future research.

6.3. Traffic Cabinet Security Workshop

The second workshop gave students an introduction to traffic cabinet technologies and an opportunity to analyze the traffic cabinet donated by the City of Tampa. The workshop was held on January 25th, 2019. Attendance was estimated at 33 students, including students from the USF Whitehatters Computer Security Club and students from the USF Department of Computer Science and Engineering. Five other participants attended remotely, including representatives from the City of Tampa, the Tampa Hillsborough Expressway Authority Connected Vehicle Pilot, and Mission Secure (a vendor working on traffic controller security solutions).

6.3.1. Overview

The workshop began with introductions from the Mission Secure team and the USF research team, including a brief introduction of the project. The USF research team gave a presentation on the technologies contained within the traffic cabinet donated by the City of Tampa, including the traffic cabinet controller and malfunction management unit. The traffic cabinet was moved into the presentation room, allowing students to see the technologies in person as they were discussed. Figure 6.2 shows the room layout while a research team member gives a presentation on the traffic cabinet technologies.

Figure 6.2 Maxat, from the research team, presenting traffic cabinet technologies to WCSC

After the students were introduced to the technologies contained within the cabinet, Weston Hecker from the Mission Secure team presented a potential attack scenario. This potential attack scenario follows a stolen GPS device that is sent overseas to be analyzed by foreign attackers. With the device, the attackers are able to locate a vulnerability in the device that can be remotely exploited. Mission Secure then describes the potential harm that such an attack may cause, including how the vulnerability may have an effect on other systems and how it may cause physical damage or traffic congestion.

Austin Suhler from the Mission Secure team then gave a live demonstration of how a traffic cabinet may be remotely exploited. Using a remote network connection setup by the research team, Austin discussed the web interface that was running on the traffic cabinet controller and showed students how he could use this web interface without any credentials. In addition, this web interface provided an attacker with all of the capabilities an operator with physical access to the control panel would have. Austin then demonstrated how timing values could be altered to create a invalid state, causing the intersection to enter flashing a state.

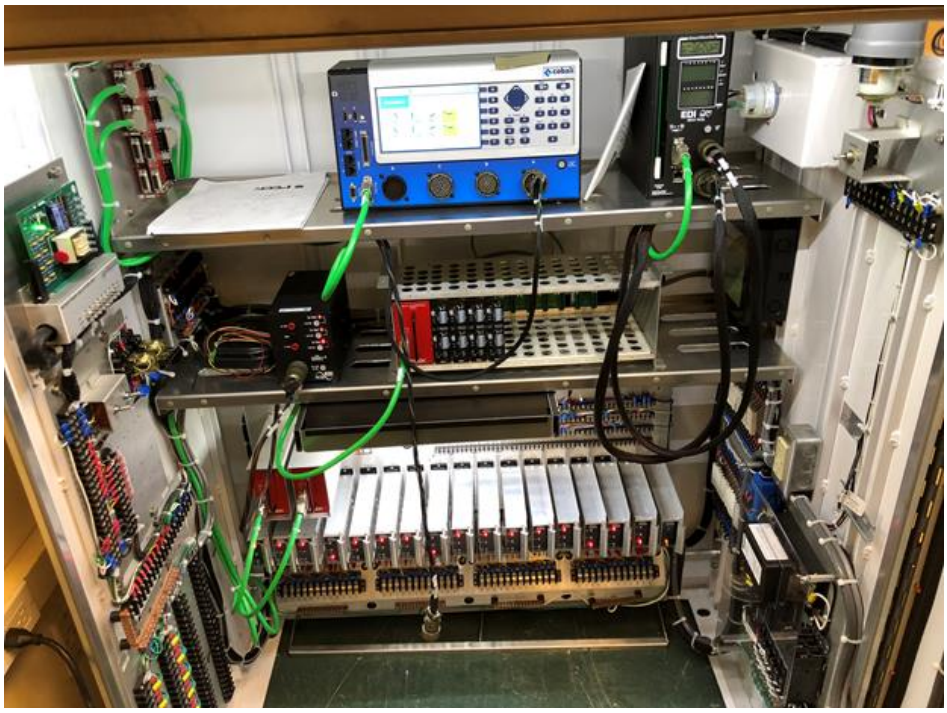

Figure 6.3 CUTR traffic cabinet donated by the City of Tampa

With the demo completed, questions were taken from the audience and the remote portion of the workshop was concluded. The research team opened the traffic cabinet to allow students to gain hands-on experience with the technologies within the traffic cabinet. Students were encouraged to interact with the console and the research team explained the functionality of each screen as students explored the features available. A few students were able to force the traffic cabinet into the flash mode by setting incorrect state values. Figure 6.3 shows the traffic cabinet students were able to experiment with.

6.3.2. Outcomes and Discussion Points

After the research team concluded their presentation, the team took questions from the participants. The first discussion point focused on the number of devices that were contained in the cabinet. The student suggested that each device was a potential point of failure, and an attack could be mounted against any of them. The research team agreed, but also briefly discussed the differences between the communication capabilities of the devices. Many of the devices in the cabinet would be much more difficult to communicate with and attack than the controller. This may be a potential subject for future work. The participants also asked about other scenarios that may cause the cabinet to enter the flash mode. The research team gave a few examples, such as low voltage from the load balancers, and discussed the error messages that appear on the malfunction management unit that can be used to diagnose issues.

Once Mission Secure's presentation was finished, students asked about one of the images contained in the presentation that featured a crashed vehicle. The student wanted to know if that crash was actually caused by an incident related to a security vulnerability in a traffic cabinet

controller. That was not the case, but the Mission Secure team described the potential for this to become a reality. In particular, they described that they had discovered vulnerabilities in traffic devices that could potentially lead to congestion and crashes.

6.4. Cybersecurity in Public Transportation Workshop

The final workshop brought together researchers from Florida universities to discuss their research related to cybersecurity in public transportation. The workshop was held on April 26th, 2019. Thirteen faculty members from universities in Florida were chosen to attend in coordination with the project manager based on their expertise and , research history, with a goal of representing multiple institutions at the workshop. Each faculty member attendee was provided $1,000 for their participation in the workshop as outlined in the project scope. The list of participants can be found in the agenda in Appendix C.3. Approximately 5-10 graduate students from various universities were present during any given session, and representatives from Gainesville Regional Transit System also attended the workshop in person. Dr. Nasir Ghani, CyberFlorida Research Liaison and professor for the USF Electrical Engineering department, was also present for the morning sessions. A remote attendance option was also provided via Adobe Connect, with an announcement sent ahead of time (the week before and day before the event) to the working group mailing list[5].

Each presenter was responsible for providing the following services:

1. Create a 20 minute Powerpoint presentation on their research area of expertise and any applicability to public transportation, and present this information at the beginning of the workshop
2. Create a written summary of a workshop session assigned to them by the PIs
3. Present the summary of the assigned session at the end of the workshop
4. Revise the summary of the assigned session based on feedback from other workshop attendees and submit this summary to the PIs

6.4.1. Overview

The workshop began with introductions from each of the members in attendance and a brief introductory presentation by the USF research team. The introductory presentation described the expectations of the presenters in greater detail, including a review of example

[5] No guests attended remotely. Seven participants completed the RSVP form, but did not attend. While two in-person participants used the conference software to access the presentation files, none of the working group attendees called in for the meeting. Fridays, while the best time for university faculty, may be a inconvenient time for agency employees.

session notes written by the research team. The remote capabilities offered through the meeting software were also introduced, including the ability to download the presentation files.

Presenters were given twenty minutes to present their research area of expertise and any applicability to cybersecurity in public transportation. Presenters were asked to leave 2-5 minutes for questions from the other participants and guests. During the presentation, one of the other participants acted as a session scribe, recording the main topic, important details, and any questions or discussion during the presentation. Participants were assigned a session to act as scribe by the research team. The scribe for each session is listed on the agenda in Appendix C.3.

Agency employees and other guests were invited to attend the workshop online. Invitations to the workshop were sent out to participants in the monthly working group meetings that were held as part of this project. Remote guests were invited to ask questions through the online meeting software or through the conference call, and the presentation files were made available through the online software.

With the introductions completed, the research team began the session with a presentation on the previous deliverables for the Enhancing Cybersecurity in Public Transportation project, focusing on the other workshops described in this document. The participants then began their presentations in the order listed on the agenda in Appendix C.3. Participants were given five and two minute warnings to encourage presenters to leave time for questions and discussion.

After the five morning presentations were completed, the group broke for lunch at 12 PM and resumed the workshop at 1 PM. Once the remaining eight participants had given their presentations, the research team led a short review of the session notes. The session notes were read by each of the scribes in the order presented, and participants were given time to voice any concerns or feedback. Once the feedback was received, the research team approved the notes for the session, and began the review process again for the next presentation. With all of the session notes approved and collected, the research team gave their concluding remarks and expressed their gratitude to all participants and guests.

The full set of session notes can be found in Appendix D in the order listed in the workshop agenda. Minor grammatical and spelling changes were made to the session notes by the research team, including adding a consistent title and subtitle that lists the presenter and scribe. Beyond these minor edits, the content has not been altered.

6.4.2. Outcomes and Discussion Points

Questions and discussion points for each of the presentations can be found in the session notes in Appendix D for that presentation.

At the end of the workshop, many of the participants began discussing potential collaboration and funding opportunities. Several participants expressed interest in a similar workshop in the future.

CHAPTER 7: TECHNOLOGY ANALYSIS AND RECOMMENDATIONS

7.1 Technology Analyses

Section 7.1 describes the technologies analyzed during the project and resulting recommendations.

7.1.1 Analysis of Mobile Fare Payment Applications

Mobile fare payment is a form of contactless electronic ticketing that enables passengers to purchase a ticket and validate the purchase using their mobile device. Mobile fare payment is typically added as an additional, more convenient fare payment option, rather than replacing existing options entirely [3]. Tickets, once purchased, are commonly verified using visual validation, Quick Response (QR) codes, or Near-Field Communication (NFC). Figure 7.1 presents a diagram of potential liabilities of mobile fare payment applications from the project taxonomy. More information on the benefits of mobile fare payment applications, implementation details, and potential vulnerabilities can be found in Chapter 2: Literature Review and Chapter 5: Taxonomy.

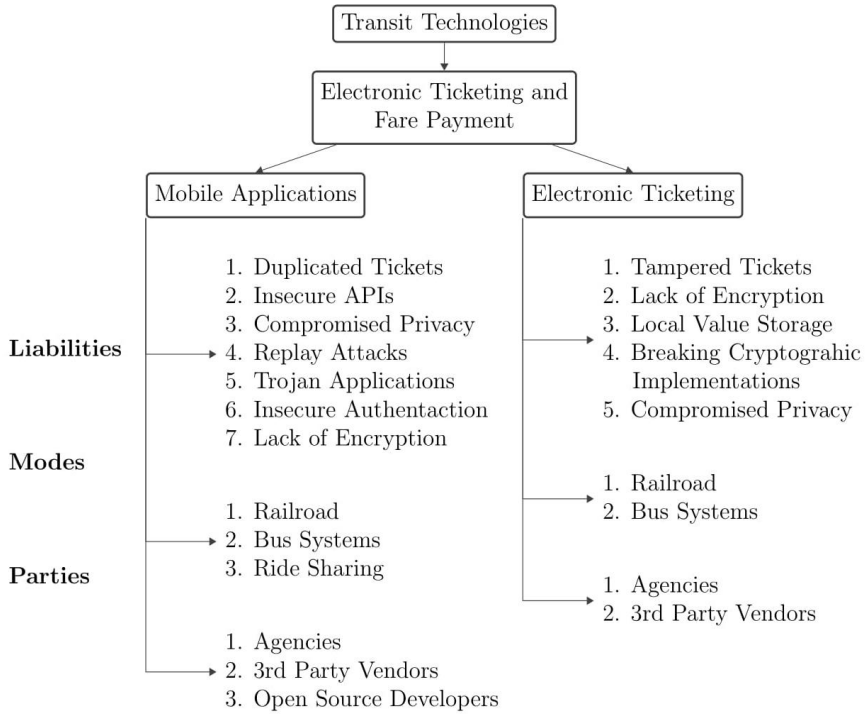

Figure 7.1 Mobile application liabilities from taxonomy

7.1.1.1. Case Study: MyJTA Mobile Application

In Jacksonville, Florida, the Jacksonville Transportation Authority (JTA) has contracted Passport [149] to develop and deploy the MyJTA [150] mobile fare payment application for their transit users. MyJTA also provides trip planning services, allowing passengers to identify the bus route they should take to reach their destination. Passport also provides parking applications for a variety of organizations across the country, such as Passport Parking, and other transportation applications. As part of the project, the research team analyzed a number of Florida mobile fare payment applications for vulnerabilities, and discovered a vulnerability in the MyJTA application. Specifically, the research team discovered a vulnerable server Application Programming Interface (API) endpoint for Passport applications that failed to authenticate the user. This vulnerability allows a malicious user to collect personally identifiable information from Passport servers.

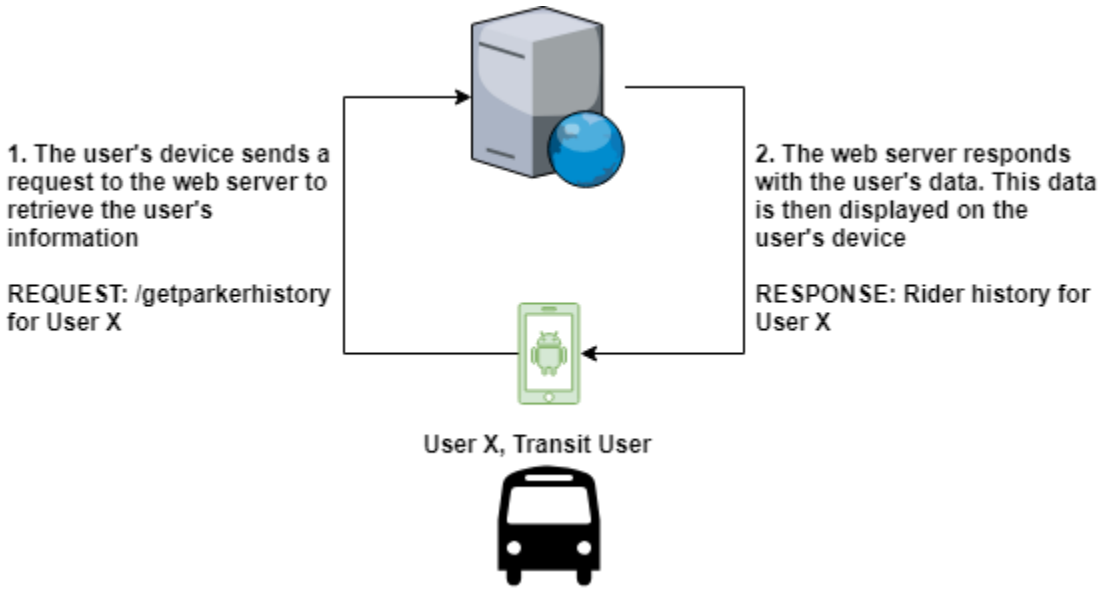

Figure 7.2 A transit user accessing the rider history API

The MyJTA application provides a rider history page for users to review their purchases and past rides. To access the user's data for this page, the application sends a request to an API endpoint made available on a Passport server. An API is a set of well-defined functions that a service or program can access to communicate or perform an action, such as requesting data from a database. In this scenario, the API is a web server that accepts requests containing information about the user, including an authorization code, and responds with the requested data. Figure 7.2 illustrates a user's device accessing the API.

Unlike the other API endpoints, the rider history endpoint did not correctly verify the authorization code for the user. Normally, the API checks that the authorization code is valid and confirms it belongs to the requested user. However, the rider history endpoint only checked that the code was valid and did not confirm the user. This allows a malicious user to send a request for another user using their valid authorization code. The API, after verifying the authorization code was valid, would respond with data for another user. This data includes personally

identifiable information such as name, phone number, and the last four digits of the credit card numbers used for purchases. Figure 7.3 shows the compromised personal data of the account created by the USF research team.

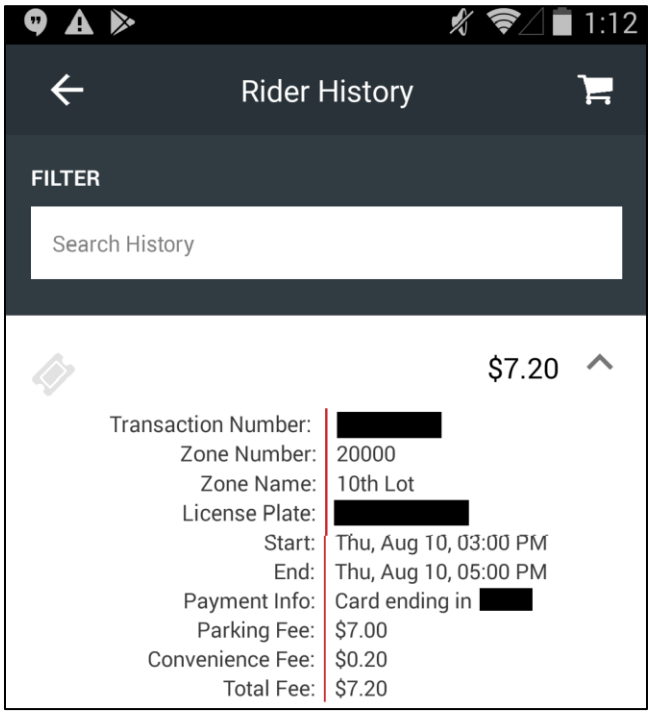

Figure 7.3 Compromised USF account displayed in the MyJTA application

The API also provided data for other Passport applications, including the Passport Parking application [149]. The same rider history API endpoint is used to provide parking history data for this application and suffers the same vulnerability. A malicious user can request data for a parking user using a valid authorization code and receive the parking user's data. This data includes the parking user's license plate number and the parking location and time. Figure 7.4 illustrates the API being user by transit, parking, and malicious users.

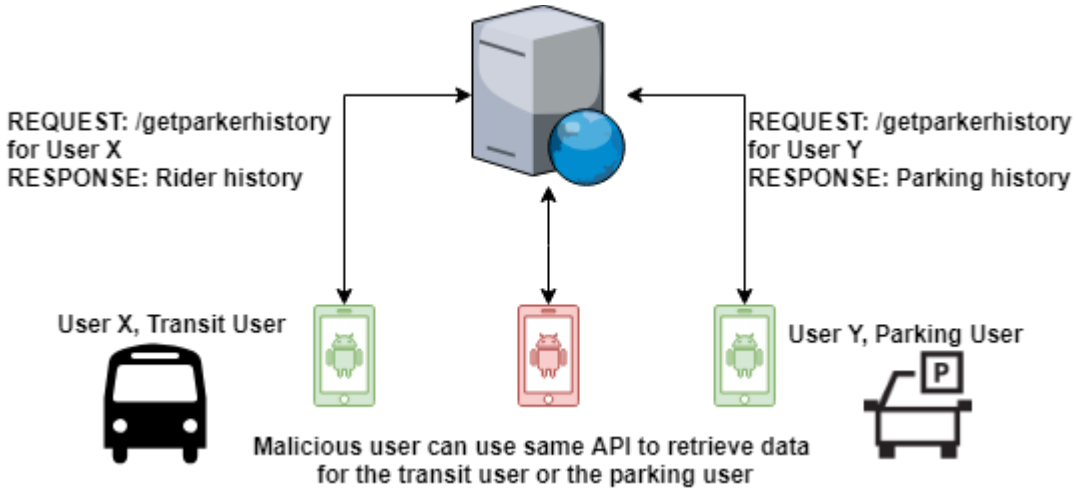

Figure 7.4 The parker history API used by a transit, parking, and malicious user

The vulnerability was discovered early October, 2018, and was reported to MyJTA on October 30, 2018. The vulnerability was patched by December 8, 2018, based on tests by the research team.

In the vulnerability report, the research team provided a recommended fix for the vulnerability. The recommended fix suggested comparing the implementation of the authorization check for the vulnerable endpoint with the correct end points and providing the correct unauthorized reply to invalid requests. Given that the authorization code was correctly validated in other API calls made by the application, the team believed that addressing this vulnerability required a very small amount of development effort. In addition, the patch was not believed to require a client update as the client application exhibited the correct behavior.

The vulnerability report included the following disclosure statement: "This research project follows a 60-day disclosure deadline. After 60 days elapse or a patch has been made broadly available, the vulnerability will be disclosed to the public." After reviewing vulnerability disclosure policies from various organizations including Google [151] and Cisco [145], the research team agreed on a 90 day disclosure deadline. However, due to the perceived ease of the vulnerability patch and correct client behavior, the team shortened the period to 60 days. Based on the tests of the vulnerability during the disclosure period, the vulnerability was fixed in under 38 days. The research team will use a 90 day disclosure policy going forward, but retains the right to extend or shorten this deadline in extenuating circumstances.

The vulnerability report was sent to a staff member from JTA participating in the cybersecurity working group. While this participant was not in the correct role to handle such reports, neither JTA nor Passport had vulnerability disclosure policies publicly available. This complicated the disclosure process, and while the vulnerability was eventually fixed, the research team is unaware of the exact process used to communicate and patch the vulnerability. However, JTA is not alone. The research team could not find vulnerability disclosure policies for any transit agencies in Florida. Section 7.2.1 describes the need for publicly available vulnerability disclosure processes in greater detail. Because the Passport application was "white-labeled", or a shared system with deployments at other transit agencies and cities, up to 40 organizations and their customers may have been affected by this vulnerability. It is unknown to the research team if JTA or Passport notified any of the other potentially affected organizations or end-users.

7.1.1.2. Recommendations

Agencies seeking to deploy mobile fare payment and other mobile applications should be sure to discuss how vulnerabilities are handled with their vendors. Agencies should ask about the timeline for patching discovered vulnerabilities and the vendor's responsibilities if a breach were to occur (e.g., if the agency or riders will be notified if a vulnerability in the vendor's system is discovered). More information on suggested vulnerability disclosure processes can be found in section 7.2.1.

For agencies seeking to deploy in-house solutions, their developers should be sure to follow industry best practices. In particular, care should be taken when handling user input and

authenticating users. Organizations such as the Open Web Application Security Project (OWASP) [34] provide training and informational resources for developers looking to develop new applications in a secure manner. Agencies should also conduct internal security reviews for their in-house applications.

7.1.2. Analysis of Traffic Cabinet

Traffic signal controllers are responsible for managing traffic signals at intersections. Traffic signal controller security has been the subject of many research endeavors in recent years, possibly due to the criticality of these systems. Traffic signal controllers store pre-programmed timing controls that define the order and length of the traffic signals. Many modern traffic signal controllers also allow for actuated control based on data received from a variety of sensors, potentially allowing for more efficient traffic flow. Figure 7.5 presents a diagram of potential liabilities of traffic signal controllers from the project taxonomy. More information on the benefits of traffic signal controllers, implementation details, and potential vulnerabilities can be found in the project literature review and taxonomy.

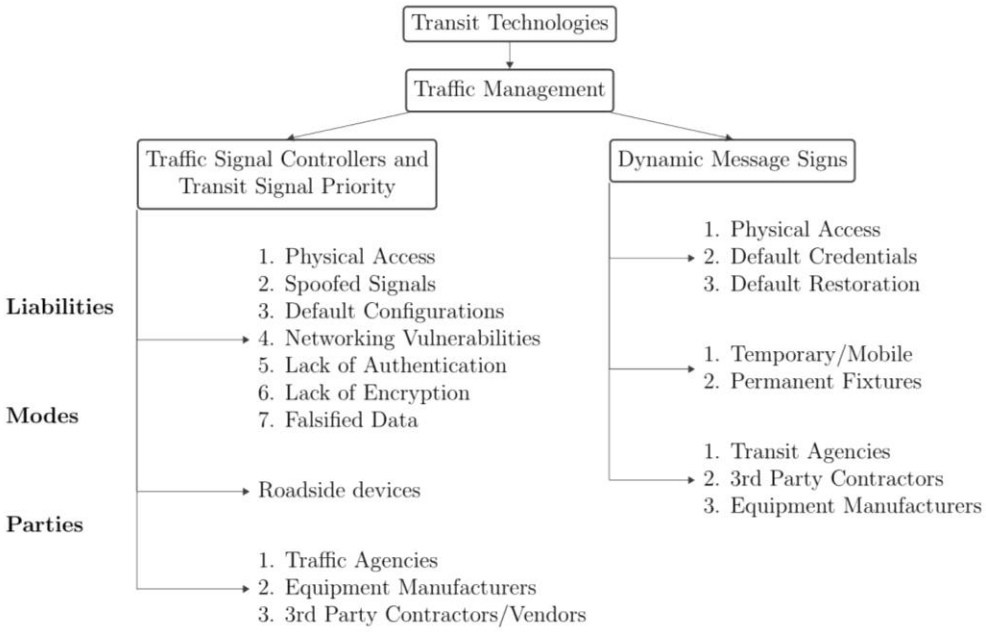

Figure 7.5 Traffic management liabilities, transportation modes, and responsible parties from the project taxonomy

7.1.2.1. Case Study: CUTR Traffic Cabinet

During the project, the City of Tampa donated a traffic controller cabinet to CUTR for research purposes. The USF research team helped coordinate the installation of the cabinet, and this project was the first to perform research on the donated traffic cabinet. The traffic cabinet included a Econolite Cobalt Controller [58], an Eberle Design, Inc. Malfunction Management Unit (MMU) [152], and a RuggedCom RS900 switch [153]. The traffic cabinet was analyzed for vulnerabilities by the USF research team and used during one of the hands-on workshops

described in Chapter 6. Figure 7.6 shows the inside of the traffic cabinet, including the controller, MMU, switch, and a laptop for testing the equipment.

Figure 7.6 Inside of the traffic cabinet, including the controller, MMU, and switch

To analyze the traffic cabinet technologies for vulnerabilities, the research team used the network layout shown in Figure 7.7. The controller, MMU, and a laptop with the Ubuntu 18 operating system were connected by Ethernet to the RuggedCom switch. The laptop was able to access the Internet using Wi-Fi but did not forward packets into or out of the traffic cabinet network. The controller and laptop were also connected by a USB to serial connector, allowing the laptop to make use of the controller's serial interface. The laptop ran applications from the device vendors and monitored the communications sent to the devices from the applications.

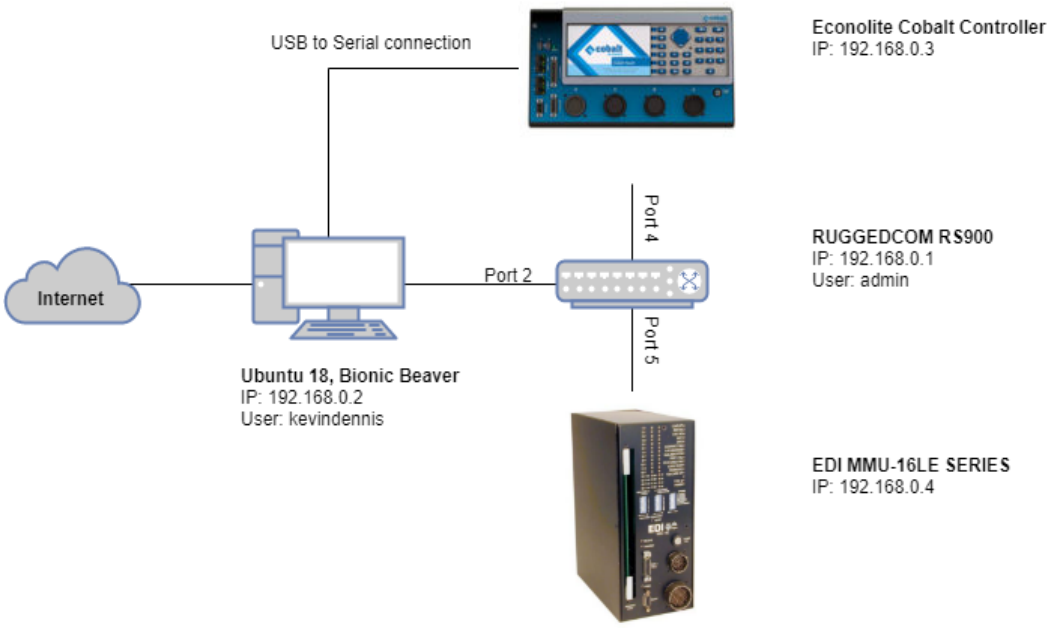

Figure 7.7 Network diagram for the CUTR traffic cabinet

The research team used nmap, a port scanning tool, to identify several services running on the controller including File Transfer Protocol (FTP), Secure Shell (SSH), and a web server. The web server hosted a control interface for the controller, which required no authentication to access. While experimenting with the device, the research team discovered the default SSH login credentials through documentation publicly available online. The credentials allowed for administrative access to the device. The research team was able to identify the controller software stored on the device and manipulate the running processes. An attacker with access to this interface could install malicious software on the device, including malware to mine cryptocurrency, prevent the device from running the controller process, or manipulate the traffic light signal timings.

An attacker could use the SSH service and web server to remotely attack the traffic cabinet if the controller is publicly visible on the Internet or an attacker gains access to the private network through another method (e.g., another compromised controller if the controllers are on a common network). Once they have access an attacker could manipulate the controller to create an unsafe state.

The USF research team were able to recreate an attack scenario from Ghena et al. [66]. In the recreated attack, the cabinet timings correspond to a simple four-way intersection. The North-South route was the busier road, with a 100 second green light time. The East-West route was less busy and only requires 40 seconds of green light time. The team changed the North-South signal timing to one second of green and four seconds of yellow. The East-West signal timing, on the other hand, was altered to be much longer, with a four minute green light. This simulated attack causes severe traffic congestion by preventing the North and South bound

traffic from making progress. Drivers may grow irritated with the lack of progress and make unsafe decisions.

7.1.2.2. Traffic Cabinet Assessment with Mission Secure

During the summer of 2018, the research team was introduced to Mission Secure (MSi), a vendor that produces hardware for securing traffic signal controllers, by City of Tampa staff. The City of Tampa was in the process of testing MSi products at Westshore Advanced Traffic Management System (ATMS) locations and facilitated the deployment of MSi hardware to the donated traffic cabinet at CUTR for evaluation by the research team.

CUTR was provided an MSi 1 device, an MSi console, and an MSi Intrusion Detection System (IDS). The MSi 1 acts as a firewall by blocking communication with the controller based on configurable rules and is connected between the controller and switch. The MSi console configures and provides an overview for the other MSi devices, and the MSi IDS monitors the network for suspicious behavior defined by configurable rules. Figure 7.8 shows the new layout of the traffic cabinet network once the MSi equipment was installed. The MSi IDS is connected into the switch twice, with the second line providing port mirroring from the switch. Port mirroring is a setting available in many switches that allows a device to monitor the communications between other devices on the switch by forwarding packets to the mirrored port.

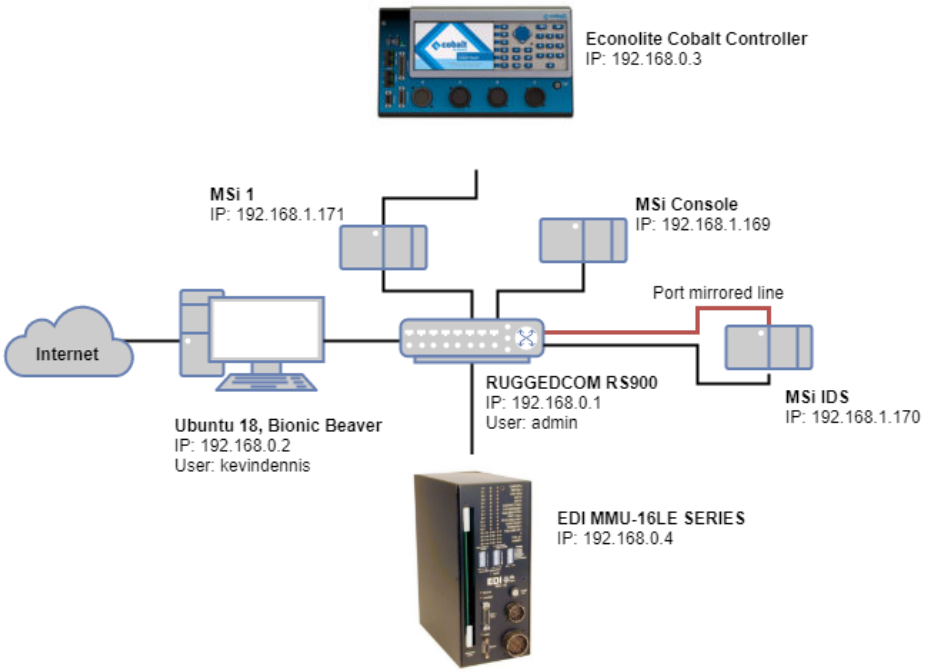

Figure 7.8 Network diagram for the CUTR traffic cabinet after installing MSi equipment

To test the provided equipment, the research team scanned the traffic cabinet network with and without the MSi equipment and enabled rules to monitor and block traffic. The

equipment was found to offer the same benefits as a firewall or IDS in an IT environment. With the correct rules established, such as blocking ports and whitelisting IP addresses, access to the traffic controller could be prevented. However, the system could still be vulnerable to those issues seen in traditional IT firewalls and IDS, such as misconfigured rules or attacking from a whitelisted IP.

7.1.2.3. Regulatory Guidelines and Recommendations

During the fifth working group meeting of this project, Scott Keith, a Traffic Signal Maintenance Supervisor from the City of Tampa, recommended implementing "smart locks" to prevent unauthorized physical access to the cabinet. The term smart lock refers to an electronic lock that may have access enabled or disabled remotely. The smart lock may allow the TMC to track access to the cabinet and remotely grant access to their vendors or technicians on a scheduled basis. Other methods for improving physical security of the cabinet include the use of unique keys, alarms, and security cameras that observe the cabinet.

Agencies should be sure to routinely apply critical security updates from their vendors. Failing to apply critical updates may leave cabinets or other OT vulnerable to exploit. In addition, agencies should log which updates they have applied and any security modifications made to the technologies. Agencies should be aware of their vendor's update policy, and vendors should provide regular notification for new updates. This notification should include a list of changes including patched security vulnerabilities.

Using default credentials is another critical issue commonly found in OT, such as traffic controllers. These credentials are often publicly available in the manufacturer's documentation or documentation from other vendors. Agencies should be sure to use unique passwords, and vendors should offer the ability to change default passwords if their equipment currently does not provide that capability.

Technologies deployed in the field that must communicate over a network should be protected by firewalls and IDS just as normal IT systems typically are. This equipment may prevent some attempts at unauthorized access to the technology. Unused services should be disabled, and their ports should be blocked by the firewall. The firewall is recommended to have the following functionalities:

- Block/restrict access to/from protected devices;
- Provide mechanical fail open or closed capabilities depending on cabinet needs;
- Monitor settings of protected devices;
- Add multi-factor authentication to access controllers;
- Add encryption and VPN connections to/from protected devices;
- Remotely restore control devices to a "known good" state;
- Support a robust set of field device protocols; and

- Provide data collection and security event detections for real-time alerting and event forensics.

IDS is recommended to have the following functionalities:

- Passively monitor field network traffic via span port or serial tap with no impact to operations;
- Provide and securely store deep packet inspection into protocols specific to the field devices;
- Store filed device network data including IP addresses, commands, configuration and state information and provide analytics for collected operations data;
- Provides and securely store real-time security event detection; and
- Provide whitelisting rules for operational traffic monitored.

In addition to firewall and IDS, the agencies may employ a separate device for centralized management and monitoring of the firewall and IDS. The device for this task is recommended to have the following functionalities:

- Unified visibility across network monitoring and end point protections from levels zero to two and above;
- Investigate incidents and troubleshoot control system issues;
- Provide operator guided or automated corrective actions;
- Alert operators, engineers and security personnel of incidents;
- Collect and store OT network and end point data for trans and post attack forensics;
- Integrate easily with various Security Information and Event Management (SIEM) and Security Operations Center (SOC) solutions; and
- Centrally manage configurations and security settings.

7.2. Recommendations and Suggested Policies

Many existing security best practices and policies are effective in the area of transportation security. This section provides recommendations for agencies seeking to improve cybersecurity in their organization. These recommendations are included based on the research team's evaluation of the current state of cybersecurity in public transportation in Florida.

The first step for an agency seeking to improve cybersecurity for their organization is to review their cybersecurity processes and training. Management should provide resources for employees to learn to be wary of potential threats, such as phishing emails. In addition, employees should be provided a process for reporting suspected vulnerabilities. While it may be more difficult to discover vulnerabilities in deployed operational technologies, employees in technical positions should be encouraged to report any suspected vulnerabilities. Transportation professionals needing to perform security sensitive tasks without a security background may find

it beneficial to review report 930 from the National Cooperative Highway Research Program (NCHRP) [154], which details many security best practices for both physical and cyber systems.

When available, agencies should employ authentication and encryption with their operational technologies. Requiring authentication and encrypting communications may prevent attacks from less sophisticated attackers. Default passwords for technologies are commonly available online, and attackers may cause significant damage simply by gaining access. This is especially true for isolated technologies, such as traffic cabinets or road side signs, where an attacker may easily access the device. For example, keys to traffic cabinets can be purchased online. An example policy may require technicians to use unique passwords for deployed technologies and disable any unnecessary applications/protocols such as Telnet that aren't used in operations.

In the event of an attack, an agency that deploys proper logging technologies may be able to determine the source of the attack and prevent future attacks from the same vulnerability. Responding to and recovering from a breach is often costly. If the source of the attack is not discovered, the costs may increase further due to repeated attacks.

7.2.1. Rule 14-90 Policy Review

For the sixth working group meeting held on December 12, 2018, Ashley Porter from the FDOT Public Transit Office presented on the state of Florida safety and security regulatory infrastructure. During the meeting, the participants discussed potential Security Program Plan (SPP) additions for Rule 14-90 and the desire to add cybersecurity guidelines to those additions. The research team agreed to review the current requirements and provide FDOT with suggested wording for the cybersecurity guidelines. This section reviews the suggested policy change from the research team, including the team's revision goals and recommendations for agencies.

The addition to the SPP requirements from the research team is included below. The addition would require agencies to include the following system activities in Section 3 of their SPP:

- *(l) A public cybersecurity vulnerability disclosure policy that includes:*
    a. *a single, public point of contact at the bus transit system for disclosure of vulnerability reports.*
    b. *expeditious notification of any and all potentially affected or in-danger parties, including users of the system.*
    c. *practical and timely steps to mitigate and recover from known vulnerabilities.*
    d. *a location for prominent public display of the policy (e.g., on the agency's website).*
    e. *compliance with the Florida Information Protection Act of 2014* [155].
- *(m) Contractual templates used by the bus transit system to engage contractors and vendors that require these entities to comply with the bus transit system public*

cybersecurity vulnerability disclosure policy described in Section (3)(l). Contractors and vendors shall report all known vulnerabilities to the bus transit system in a timely manner and shall describe in the contract practical and timely steps to mitigate and recover from known vulnerabilities without additional charge to the bus transit system (e.g., as part of a maintenance agreement).

The research team hopes to accomplish two key goals with the addition of these SPP requirements. The primary goal is to improve the vulnerability disclosure process for Florida transit agencies, and the secondary goal is to improve the discussion of cybersecurity between agencies and their vendors.

7.2.1.1. Vulnerability Disclosure Policies

When attempting to report the mobile fare payment vulnerability described in Section 7.1.1, the research team were unable to find an appropriate contact for the agency or the vendor. After reporting the vulnerability, the research team reviewed several Florida transit agency websites and were unable to find publicly available contacts for any transit agency in the state of Florida. As transit agencies continue to employ new technologies such as mobile fare payment, the number of discovered vulnerabilities is expected to increase. By providing clear vulnerability disclosure policy, vulnerabilities may be patched more quickly and communication between agencies, researchers, and vendors can be improved.

A common challenge for successful vulnerability disclosure is the lack of experience for both the vendors and security researchers in regards to accepting or providing vulnerability reports [156, pp. 7–8]. Smaller organizations, such as transit agencies, may be unprepared to accept vulnerability reports and, due to the sensitive nature of vulnerabilities, inexperienced researchers may be overly aggressive when discussing a timeline with an agency. Providing a clear vulnerability policy will provide a smoother experience for both the agency employees and security researchers.

Providing a prominent location for the vulnerability policy, such as the agency website, will allow vulnerability researchers and vendors to easily access the policy, especially if the page can be found using a search engine. This prominent location should have a single point of contact listed, and should ideally specify what information should be included in the report.

The point of contact could be an online form instead of an email or other form of communication. This will allow agencies more control over the information that is submitted along with the report. Agencies have deployed similar online forms for safety reporting [157]. These online forms can be programmed to provide other advantages, such as forwarding alerts to all relevant personnel [157].

The Florida Information Protection Act of 2014 [155] requires a covered entity to provide notification within 30 days after a breach affecting 500 or more individuals in Florida is

discovered. By providing expeditious notification of all affected parties in their vulnerability disclosure program, an agency may be more prepared to meet this requirement. Rapid notification of relevant vendors and other agencies may also reduce exploitation of the vulnerability.

CHAPTER 8: Conclusions

8.1 Conclusions

Over the course of the project, 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, and organized three workshops.

During the literature review, existing vulnerabilities were discovered for CVs, AVs, electronic ticketing systems, traffic signal controllers, traffic signal priority, DMS. No known vulnerabilities were found in the literature for AVL/CAD systems, online trip planners, mobile fare payment, onboard Wi-Fi, CCTV, and APCs, 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 most 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 have deployed autonomous vehicles and five agencies considering deployment in the next five years. Agencies and researchers should continue to analyze this emerging technology for security vulnerabilities as they continue to increase in deployment.

Ten working group meetings were held throughout the project with the goal of facilitating ongoing cybersecurity information exchange among Florida transit agencies, their vendors, and cybersecurity researchers. The working groups 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 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 CAD/AVL and mobile fare payment are also widely deployed, and have many critical liabilities. Mobile fare payment apps are being deployed by transit agencies nationally at an increasing rate. Given the intersection of revenue collection for the agency and transit rider payment information on privately-owned devices, mobile fare payment apps are a critical technology to examine in detail. Onboard Wi-Fi

is under consideration by more than 35% of survey respondents that have not deployed it, making it an important technology to analyze further as well.

Finally, 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 device and were given the opportunity to interact with the technologies inside of the CUTR traffic 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 and reported a vulnerability in a Florida mobile fare payment application that exposed private user information such as emails, partial credit card numbers, license plate numbers, and parking locations to malicious users. While reporting the vulnerability, the research team were unable to find vulnerability disclosure policies for the agency or vendor. After reviewing other agency websites, the research team were unable to find policies for any agency in the state of Florida. Further study of mobile applications in transportation may identify unique threats.

This report also included security recommendations for transit agencies and reviewed existing policy. The research team drafted policy language for vulnerability disclosure policies for the security program plan additions for Rule 14-90 under consideration by the Florida Department of Transportation, which is presented in Chapter 7.2.1. Agencies should also comply with the Florida Information Protection Act of 2014, which outlines requires of government agencies and their vendors in case of a data breach. The guidelines in this project should be expanded further, including the creation of template documents agencies can directly include in their security program plan and template contract language for working with vendors. Future work should 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. Future work may also examine the development of a vulnerability information sharing program amongst Florida transit agencies, including examining the potential use of the Florida Transit Safety and Operations Network as an avenue for vulnerability disclosure between transit agencies. The balance of sharing information publicly vs. privately among agencies should be examined.

Examining the average service age of technologies deployed by transit agencies and the effects on cybersecurity may be another possible source of future work. In industrial control systems, technologies see long lifespans that result in the devices being susceptible to vulnerabilities that have not been patched by vendors. Technologies used in public transportation, and transportation in general, may face similar security challenges. The mix of new and older technologies (e.g., Internet-connected equipment on the same network as equipment intended for private network use) may especially open systems up to unexpected vulnerabilities.

References

[1] National Academies of Sciences, Engineering, and Medicine, *Protection of Transportation Infrastructure from Cyber Attacks: A Primer*. Washington, DC: The National Academies Press, 2016 [Online]. Available: https://doi.org/10.17226/23516. [Accessed: 20-Jul-2018]

[2] American Public Transportation Association, *Securing Control and Communications Systems in Transit Environments: Part 1: Elements, Organization and Risk Assessment/Management*, (APTA-RP-CCS-1-RT-001-10), American Public Transportation Association, Washington, DC, Jul. 2010 [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.644.9557&rep=rep1&type=pdf

[3] N. L. Georggi, S. Barbeau, and A. Joslin, (Mar. 2016), *Assessment of Mobile Fare Payment Technology for Future Deployment in Florida*, (Florida Department of Transportation Research Report BDV-943-39), University of South Florida, Tampa, FL.

[4] B. Ferris, K. Watkins, and A. Borning, "OneBusAway: results from providing real-time arrival information for public transit," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, Atlanta, Georgia, USA, 2010, pp. 1807–1816 [Online]. Available: http://doi.acm.org/10.1145/1753326.1753597

[5] Gartner, "Operational Technology (OT)," *Gartner IT Glossary*, Nov-2012. [Online]. Available: https://www.gartner.com/it-glossary/operational-technology-ot/. [Accessed: 15-Jul-2018]

[6] B. Gregory-Brown and D. Harp, *Security in a Converging IT/OT World*, SANS Institute, Nov. 2016 [Online]. Available: https://www.sans.org/reading-room/whitepapers/analyst/membership/37382. [Accessed: 01-Jul-2018]

[7] E. Lee, "Cyber-Physical Systems - a Concept Map," *Ptolemy Project*. [Online]. Available: https://ptolemy.berkeley.edu/projects/cps/. [Accessed: 24-Sep-2019]

[8] T. Chuang, "Ransomware strikes CDOT for second time even as agency still recovering from first SamSam attack," *The Denver Post*, 01-Mar-2018. [Online]. Available: https://www.denverpost.com/2018/03/01/cdot-samsam-ransomware-attack/. [Accessed: 19-Jul-2018]

[9] American Public Transportation Association, "Security and Emergency Management Standards," *American Public Transportation Association*, 07-Dec-2018. [Online]. Available: https://www.apta.com/research-technical-resources/standards/security/. [Accessed: 24-Sep-2019]

[10] American Public Transportation Association, *Securing Control and Communications Systems in Transit Environments: Part II: Defining a Security Zone Architecture for Rail Transit and Protecting Critical Zones*, (APTA-SS-CCS-RP-002-13), Washington, DC, Jun. 2013.

[11] J. L. Western and B. Ran, *Information Technology in Transportation Key Issues and a Look Forward*, (A5003), Transportation Research Board, Committee on Information Systems and Technology, Washington, DC, 2000 [Online]. Available: http://onlinepubs.trb.org/onlinepubs/millennium/00054.pdf

[12] E. Fok, "Protecting Your Transportation Management Center," *ITE Journal*, vol. 85, no. 2, pp. 32–36, Feb. 2015 [Online]. Available: https://www.ite.org/pub/?id=898748dd-0c0c-2cb9-c9db-0cac2bc3bd7d

[13] "Report Phishing Sites," *US-CERT*. [Online]. Available: https://www.us-cert.gov/report-phishing. [Accessed: 22-Sep-2019]

[14] Florida Center for Cybersecurity and Gartner, *The State of Cybersecurity in Florida*, Florida Center for Cybersecurity, 2017 [Online]. Available: https://cyberflorida.org/2018/06/19/the-state-of-cybersecurity-in-florida/
[15] Florida Center For Cybersecurity, "Cyber Florida," *Cyber Florida*, 22-May-2019. [Online]. Available: https://cyberflorida.org. [Accessed: 20-Sep-2019]
[16] "What is Spear Phishing? - Definition," *Kaspersky Lab*. [Online]. Available: https://usa.kaspersky.com/resource-center/definitions/spear-phishing. [Accessed: 21-Sep-2019]
[17] "Unifying the Global Response to Cybercrime," *Anti-Phishing Working Group*, 2019. [Online]. Available: https://www.antiphishing.org/. [Accessed: 24-Sep-2109]
[18] "Ransomware and Recent Variants," *US-CERT*, 31-Mar-2016. [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA16-091A. [Accessed: 24-Sep-2109]
[19] G. O'Gorman and G. McDonald, *Ransomware: A Growing Menace*, Symantec, Mountain View, California, Nov. 2012 [Online]. Available: https://www.symantec.com/connect/blogs/ransomware-growing-menace
[20] M. Korolov, "93% of phishing emails are now ransomware," *CSO Online*, 01-Jun-2016. [Online]. Available: https://www.csoonline.com/article/3077434/security/93-of-phishing-emails-are-now-ransomware.html. [Accessed: 24-Sep-2019]
[21] S. Meehan, K. Rector, and Baltimore Sun, "In Wake of Baltimore 911 Cyberattack, Officials Urge Layered Protections," *Government Technology*, Mar-2018. [Online]. Available: http://www.govtech.com/security/In-Wake-of-Baltimore-911-Cyberattack-Officials-Urge-Layered-Protections.html. [Accessed: 24-Sep-2019]
[22] S. Ferguson, "Atlanta's Ransomware Attack Cost Around $2.6M – Report," *Security Now*, 24-Apr-2018. [Online]. Available: https://www.securitynow.com/author.asp?section_id=613&doc_id=742502. [Accessed: 24-Sep-2019]
[23] S. Barbeau and J. Begley, (Mar. 2013), *SunRail Electronic Trip Planning Study Final Report*, USF Center for Urban Transportation Research, Tampa, FL [Online]. Available: http://www.locationaware.usf.edu/wp-content/uploads/2013/04/SunRail-Electronic-Trip-Planning-Study-Final-Report.pdf
[24] C. Brakewood and K. Watkins, "A literature review of the passenger benefits of real-time transit information," *Transport Reviews*, vol. 39, no. 3, pp. 327–356, 2019 [Online]. Available: https://doi.org/10.1080/01441647.2018.1472147
[25] "OneBusAway," *OneBusAway*, 2019. [Online]. Available: https://onebusaway.org/. [Accessed: 20-Jul-2018]
[26] S. J. Barbeau and A. Antrim, *The Many Uses of GTFS Data – Opening the Door to Transit and Multimodal Applications*, USF Center for Urban Transportation Research [Online]. Available: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.391.5421. [Accessed: 24-Sep-2019]
[27] "GTFS Static Overview," *Google Developers*, Oct-2017. [Online]. Available: https://developers.google.com/transit/gtfs/. [Accessed: 22-Jun-2018]
[28] "GTFS Overview," *Google Developers*, Oct-2017. [Online]. Available: https://developers.google.com/transit/gtfs/reference/. [Accessed: 22-Jun-2018]
[29] "GTFS Realtime Overview," *Google Developers*, Oct-2017. [Online]. Available: https://developers.google.com/transit/gtfs-realtime/. [Accessed: 22-Jun-2018]

[30] S. J. Barbeau, “Quality Control - Lessons Learned from Deployment and Evaluation of GTFS-realtime Feeds,” presented at the 97th Annual Meeting of the Transportation Research Board, Washington, DC, 2018 [Online]. Available: https://trid.trb.org/view/1496848
[31] “Protocol Buffers,” *Google Developers*, Oct-2017. [Online]. Available: https://developers.google.com/protocol-buffers/. [Accessed: 22-Jun-2018]
[32] “OpenTripPlanner,” *OpenTripPlanner*, 2009. [Online]. Available: http://www.opentripplanner.org/. [Accessed: 22-Jun-2018]
[33] S. Barbeau and J. Begley, “Web-based Trip Planner Options for Transit Agencies,” USF Center for Urban Transportation Research, 18-Apr-2013 [Online]. Available: https://www.cutr.usf.edu/wp-content/uploads/2013/04/CUTR-Webcast-Handout-04.18.13.pdf. [Accessed: 24-Sep-2019]
[34] “OWASP Overview,” *OWASP Foundation*, 19-Sep-2019. [Online]. Available: https://www.owasp.org/index.php/Main_Page. [Accessed: 24-Sep-2019]
[35] K. Turner, “Google Maps: Goofs, Hacks And Losing Our Sense Of Direction,” *Hartford Courant*, 11-Apr-2016. [Online]. Available: http://www.courant.com/consumer/hc-ls-tech-google-maps-errors-0410-20160411-story.html. [Accessed: 21-Jun-2018]
[36] C. Payne, “On the security of open source software,” *Information Systems Journal*, vol. 12, no. 1, pp. 61–78, Feb. 2002.
[37] M. Mezghani, *Study on electronic ticketing in public transport (Final Report)*, European Metropolitan Transport Authorities, May 2008 [Online]. Available: https://www.emta.com/IMG/pdf/EMTA-Ticketing.pdf. [Accessed: 24-Sep-2019]
[38] A. Samuely, “Mobile ticketing transaction volume to double by 2019,” *Retail Dive*, 2017. [Online]. Available: https://www.retaildive.com/ex/mobilecommercedaily/mobile-ticketing-to-dominate-digital-transactions-by-more-than-50pc-report. [Accessed: 24-Sep-2019]
[39] M. Puhe, M. Edelmann, and M. Reichenbach, “Integrated urban e-ticketing for public transport and touristic sites,” *Transportation Research Procedia*, vol. 4, pp. 494–504, 2014 [Online]. Available: https://doi.org/10.1016/j.trpro.2014.11.038
[40] W. Narzt, S. Mayerhofer, O. Weichselbaum, S. Haselböck, and N. Höfler, “Be-In/Be-Out with Bluetooth Low Energy: Implicit Ticketing for Public Transportation Systems,” in *2015 IEEE 18th International Conference on Intelligent Transportation Systems*, IEEE, Las Palmas, Spain, 2018, pp. 1551–1556 [Online]. Available: https://ieeexplore.ieee.org/document/7313345
[41] R. Ryan, Z. Anderson, and A. Chiesa, “Anatomy of Subway Hack,” DEFCON 16, Las Vegas, Nevada, Aug-2008 [Online]. Available: http://tech.mit.edu/V128/N30/subway/Defcon_Presentation.pdf. [Accessed: 24-Sep-2019]
[42] Z. Anderson, “Boston Subway MBTA Security Research,” *Zack.Anderson*, 2013. [Online]. Available: http://web.mit.edu/zacka/www/mbta.html. [Accessed: 24-Sep-2019]
[43] D. Surendran, “An Overview of Smart Card Security,” *Architectural Challenges Of Smart Card Design*, 2000. [Online]. Available: https://people.cs.uchicago.edu/dinoj/smartcard/security.html. [Accessed: 24-Sep-2019]
[44] J. Abbott, *Smart Cards: How Secure Are They?*, SANS Institute, Mar. 2002 [Online]. Available: https://www.sans.org/reading-room/whitepapers/authentication/paper/131
[45] H. J. Mahanta, A. K. Azad, and A. K. Khan, “Power analysis attack: A vulnerability to smart card security,” in *2015 International Conference on Signal Processing and Communication*

Engineering Systems, IEEE, Guntur, India, 2015, pp. 506–510 [Online]. Available: https://ieeexplore.ieee.org/document/7058206

[46] F. Kerschbaum, H. W. Lim, and I. Gudymenko, "Privacy-preserving billing for e-ticketing systems in public transportation," in *Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society*, ACM, 2013, pp. 143–154.

[47] A.-R. Sadeghi, I. Visconti, and C. Wachsmann, "User Privacy in Transport Systems Based on RFID E-Tickets," in *PiLBA*, CEUR, Malaga, Spain, 2008, vol. 397 [Online]. Available: https://www.semanticscholar.org/paper/User-Privacy-in-Transport-Systems-Based-on-RFID-Sadeghi-Visconti/e75e7650de7d15275d76901903f50749139e5b31

[48] E. Tavilla, *Transit Mobile Payments: Driving Consumer Experience and Adoption*, Federal Reserve Bank of Boston, Feb. 2015 [Online]. Available: https://www.bostonfed.org/-/media/Documents/PaymentStrategies/publications/2015/transit-mobile-payments.pdf

[49] Passenger Transport, "First urges bus users to swap cash for mTickets," *Passenger Transport*, 12-Dec-2016. [Online]. Available: http://www.passengertransport.co.uk/2016/12/first-urges-bus-users-to-swap-cash-for-mtickets/. [Accessed: 20-Jul-2018]

[50] "Bus Passes on Your Phone," *Token Transit*, 2018. [Online]. Available: https://www.tokentransit.com/. [Accessed: 20-Jul-2018]

[51] DENSO WAVE, "QRcode.com," *QR Code*, 2018. [Online]. Available: http://www.qrcode.com/en/. [Accessed: 30-Jul-2018]

[52] L. Finžgar and M. Trebar, "Use of NFC and QR code identification in an electronic ticket system for public transport," in *SoftCOM 2011, 19th International Conference on Software, Telecommunications and Computer Networks*, IEEE, Split, Croatia, 2011, pp. 1–6 [Online]. Available: https://ieeexplore.ieee.org/document/6064445/

[53] "Bluetooth Technology Website," *Bluetooth*, 2018. [Online]. Available: https://www.bluetooth.com/. [Accessed: 25-Jul-2018]

[54] P. Kieseberg *et al.*, "QR code security," in *Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia*, ACM, Paris, France, 2010, pp. 430–435.

[55] K. Conger, "Rare Malware Targeting Uber's Android App Uncovered," *Gizmodo*, 03-Jan-2018. [Online]. Available: https://gizmodo.com/rare-malware-targeting-ubers-android-app-uncovered-1821753862. [Accessed: 31-Jul-2018]

[56] R. J. Baker, J. Collura, J. Dale, K. Head, and B. Hemily, *An Overview of Transit Signal Priority*. Washington, DC: ITS America, 2002 [Online]. Available: https://trid.trb.org/view/723986

[57] J. A. Bonneson, S. R. Sunkari, M. P. Pratt, and P. Songchitruksa, *Traffic signal operations handbook*, (0–6402), Texas Transportation Institute, Texas A & M University System, College Station, Texas, 2009 [Online]. Available: https://static.tti.tamu.edu/tti.tamu.edu/documents/0-6402-P1.pdf

[58] Econolite, "Cobalt ATC Traffic Controller," *Econolite*, 2018. [Online]. Available: https://www.econolite.com/products/controllers/cobalt/. [Accessed: 18-Jul-2018]

[59] M. M. Dobersek, "An operational comparison of pre-time, semi-actuated, and fully actuated interconnected traffic control signal systems," Marquette University, Milwaukee, Wisconsin, 1998 [Online]. Available: https://search.proquest.com/docview/304418147

[60] H. R. Smith, B. Hemily, and M. Ivanovic, *Transit Signal Priority (TSP): A Planning and Implementation Handbook*. Washington, DC: ITS America, 2005 [Online]. Available: http://www.fta.dot.gov/documents/TSPHandbook10-20-05.pdf

[61] C.-F. Liao and G. Davis, "Simulation Study of a Bus Signal Priority Strategy Based on GPS/AVL and Wireless Communications," *Transportation Research Record*, vol. 2034, pp. 82–91, Dec. 2007 [Online]. Available: http://www.menet.umn.edu/~cliao/86TRB_BSP_07_0444.pdf

[62] H. R. Al-Zoubi, S. Z. Shatnawi, A. I. Kalaf, and B. A. Mohammad, "A Wireless Mobile-Phone Approach to Traffic Signal Preemption for Faster Service of Emergency Vehicles," *International Journal of Computer Applications (0975 – 8887)*, vol. 46, no. 3, pp. 35–41, May 2012.

[63] Fla. Stat. § 316.0775, *Interference with official traffic control devices or railroad signs or signals*. 2000 [Online]. Available: http://www.leg.state.fl.us/Statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0300-0399/0316/Sections/0316.0775.html

[64] L. Tebow, "Choose Who Has Control of the Traffic Signals," *IMSA Journal*, vol. L, no. 4, pp. 28–30, Jul. 2012 [Online]. Available: http://www.imsasafety.org/journal/ja12/15.pdf. [Accessed: 24-Sep-2019]

[65] B. Ziegler, "Signal Cabinet Electronic Locks," *MoboTrex*, Apr-2016. [Online]. Available: https://www.mobotrex.com/2016/04/18/signal-cabinet-peace-mind/. [Accessed: 20-Jun-2018]

[66] B. Ghena, W. Beyer, A. Hillaker, J. Pevarnek, and J. A. Halderman, "Green Lights Forever: Analyzing the Security of Traffic Infrastructure," in *8th USENIX Workshop on Offensive Technologies (WOOT 14)*, USENIX Association, San Diego, CA, 2014.

[67] C. Cerrudo, "Hacking US traffic control systems," DEFCON 22, Las Vegas, Nevada, 2014 [Online]. Available: https://www.defcon.org/images/defcon-22/dc-22-presentations/Cerrudo/DEFCON-22-Cesar-Cerrudo-Hacking-Traffic-Control-Systems-UPDATED.pdf. [Accessed: 20-Jun-2018]

[68] C. Cerrudo, *An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks*, Ioactive Labs, 2015 [Online]. Available: https://ioactive.com/pdfs/IOActive_HackingCitiesPaper_CesarCerrudo.pdf. [Accessed: 20-Jun-2018]

[69] A. Ghafouri, W. Abbas, Y. Vorobeychik, and X. Koutsoukos, "Vulnerability of fixed-time control of signalized intersections to cyber-tampering," in *2016 Resilience Week (RWS)*, IEEE, Chicago, IL, USA, 2016, pp. 130–135 [Online]. Available: https://ieeexplore.ieee.org/document/7573320. [Accessed: 20-Jun-2018]

[70] A. Laszka, B. Potteiger, Y. Vorobeychik, S. Amin, and X. Koutsoukos, "Vulnerability of Transportation Networks to Traffic-signal Tampering," in *Proceedings of the 7th International Conference on Cyber-Physical Systems*, IEEE Press, Piscataway, NJ, USA, 2016, pp. 16:1–16:10.

[71] K. Poulsen, "Traffic Hackers Hit Red Light," *Wired*, 12-Aug-2005. [Online]. Available: Traffic Hackers Hit Red Light. [Accessed: 20-Jun-2018]

[72] C. Schweiger, *Real-Time Bus Arrival Information Systems*, Transit Cooperative Research Program (TCRP) Synthesis Report 48, Transportation Research Board, Washington, DC, Jan. 2003 [Online]. Available: http://onlinepubs.trb.org/onlinepubs/tcrp/tcrp_syn_48.pdf

[73] *Introduction to Variable Message Signs Student Handbook*. Wisconsin: Wisconsin State Department of Transportation, 2000 [Online]. Available: http://www4.uwm.edu/cuts/itsdm/chap6.pdf. [Accessed: 24-Sep-2019]
[74] Ohio Department of Transportation, "Dynamic Message Signs (DMS)," *Ohio Department of Transportation*. [Online]. Available: http://www.dot.state.oh.us/Divisions/Operations/Traffic/FAQs/Pages/DMS.aspx. [Accessed: 24-Sep-2019]
[75] "Employ web-enabled variable message signs for your real-time conditional messaging needs," *All Traffic Solutions*, 24-Jan-2018. [Online]. Available: http://www.alltrafficsolutions.com/blog/employ-web-enabled-variable-message-signs-real-time-conditional-messaging-needs/. [Accessed: 22-Jun-2018]
[76] K. P. Heaslip, M. Foruhandeh, and K. B. Kelarestaghi, "Transportation Cyber-Physical Security: Things We Should Know," T3e Webinar Overview, 10-May-2018 [Online]. Available: https://www.pcb.its.dot.gov/t3/s180510_Transportation_Cyber-Physical_Security.aspx. [Accessed: 24-Sep-2019]
[77] B. Wojdyla, "How To Hack An Electronic Road Sign," *Jalopnik*, Jan-2009. [Online]. Available: https://jalopnik.com/5141430/how-to-hack-an-electronic-road-sign. [Accessed: 14-Jun-2018]
[78] M. Bennett, "Vulgar Messages Shown On Delaware County Road Sign: Reports," *Patch*, May-2018. [Online]. Available: https://patch.com/pennsylvania/radnor/vulgar-messages-shown-delaware-county-road-sign-reports. [Accessed: 20-Jul-2018]
[79] J. Scharr, "Hacking an Electronic Highway Sign is Way Too Easy," *Toms Guide*, Jun-2014. [Online]. Available: https://www.tomsguide.com/us/highway-signs-easily-hacked,news-18915.html. [Accessed: 20-Jun-2018]
[80] B. Krebs, "They Hack Because They Can," Jun-2014. [Online]. Available: https://krebsonsecurity.com/2014/06/they-hack-because-they-can/
[81] M. Noch, "Security Cameras / Security Systems Fact Sheet," *Intelligent Transportation Systems*, 2018. [Online]. Available: https://www.pcb.its.dot.gov/factsheets/security/sec_overview.aspx#page=common. [Accessed: 20-May-2018]
[82] "CCTV Cameras in Transit Systems: Aiming to improve safety and security," *Global Mass Transit Report*, 01-Jul-2014. [Online]. Available: https://www.globalmasstransit.net/archive.php?id=16680. [Accessed: 20-Jul-2018]
[83] Transportation Research Board and National Academies of Sciences, Engineering, and Medicine, *Practices to Protect Bus Operators from Passenger Assault*. Washington, DC: The National Academies Press, 2011 [Online]. Available: https://www.nap.edu/catalog/14609/practices-to-protect-bus-operators-from-passenger-assault
[84] American Public Transportation Association, *Selection of Cameras, Digital Recording Systems, Digital High-Speed Networks and Trainlines for Use in Transit-Related CCTV Systems*, (APTA IT-CCTV-RP-001-11), American Public Transportation Association, Washington, DC, Jun. 2011 [Online]. Available: https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-IT-CCTV-RP-001-11.pdf
[85] A. Costin, "Security of CCTV and Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations," in *Proceedings of the 6th International Workshop on Trustworthy*

Embedded Devices, ACM, Vienna, Austria, 2016, pp. 45–54 [Online]. Available: http://doi.acm.org/10.1145/2995289.2995290

[86] A. Cui and S. J. Stolfo, "A quantitative analysis of the insecurity of embedded network devices: results of a wide-area scan," in *Proceedings of the 26th Annual Computer Security Applications Conference*, ACM, Austin, Texas, USA, 2010, pp. 97–106 [Online]. Available: http://doi.acm.org/10.1145/1920261.1920276

[87] "Shodan," *Shodan*, 2019. [Online]. Available: https://www.shodan.io/. [Accessed: 25-Sep-2019]

[88] T. B. Brown, D. Mané, A. Roy, M. Abadi, and J. Gilmer, "Adversarial Patch," in *31st Conference on Neural Information Processing Systems*, Long Beach, CA, USA, 2017.

[89] J. Vincent, "These stickers make computer vision software hallucinate things that aren't there," *The Verge*, 03-Jan-2018. [Online]. Available: https://www.theverge.com/2018/1/3/16844842/ai-computer-vision-trick-adversarial-patches-google. [Accessed: 20-Jul-2018]

[90] C. Cárdenas and F. Camacho, "User Statistics and Traffic Analysis of Public Internet Access in Buses," in *Ubiquitous Computing and Ambient Intelligence. Context-Awareness and Context-Driven Interaction*, Springer International Publishing, Cham, 2013, vol. 8276, pp. 390–393 [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-319-03176-7_53

[91] A. Balasubramanian, R. Mahajan, and A. Venkataramani, "Augmenting mobile 3G using WiFi," in *Proceedings of the 8th international conference on Mobile systems, applications, and services*, ACM, San Francisco, California, USA, 2010, pp. 209–222 [Online]. Available: http://doi.acm.org/10.1145/1814433.1814456

[92] A. Gupta and R. K. Jha, "Security threats of wireless networks: A survey," in *International Conference on Computing, Communication Automation*, IEEE, Noida, India, 2015, pp. 389–395 [Online]. Available: https://ieeexplore.ieee.org/document/7148407

[93] K. H. Johansson, M. Törngren, and L. Nielsen, "Vehicle Applications of Controller Area Network," in *Handbook of Networked and Embedded Control Systems*, D. Hristu-Varsakelis and W. S. Levine, Eds. Boston, MA: Birkhäuser Boston, 2005, pp. 741–765.

[94] S. Checkoway *et al.*, "Comprehensive experimental analyses of automotive attack surfaces," in *Proceedings of the 20th USENIX conference on Security*, USENIX Association, San Francisco, CA, 2011, pp. 6–6 [Online]. Available: http://dl.acm.org/citation.cfm?id=2028067.2028073

[95] Transportation Research Board and National Academies of Sciences, Engineering, and Medicine, *Computer-Aided Scheduling and Dispatch in Demand-Responsive Transit Services*. Washington, DC: The National Academies Press, 2004 [Online]. Available: https://doi.org/10.17226/23335

[96] Transportation Research Board and National Academies of Sciences, Engineering, and Medicine, *AVL Systems for Bus Transit: Update*. Washington, DC: The National Academies Press, 2008 [Online]. Available: https://doi.org/10.17226/22019

[97] J. Fortunati, "Transit agencies have a path forward in modernizing real-time arrival information," *Mobility Lab*, 22-Feb-2018. [Online]. Available: https://mobilitylab.org/2018/02/22/transit-agencies-path-forward-modernizing-real-time-arrival-information/. [Accessed: 20-Jul-2018]

[98] S. Babcock, "City: Cyber attack against Baltimore's 911 computer-aided dispatch system was ransomware," *Technical.ly*, Mar-2018. [Online]. Available:

https://technical.ly/baltimore/2018/03/29/city-cyber-attack-baltimores-911-computer-aided-dispatch-system-ransomware/. [Accessed: 20-Jul-2018]
[99] Transportation Research Board and National Academies of Sciences, Engineering, and Medicine, *Passenger Counting Systems*. Washington, DC: The National Academies Press, 2008 [Online]. Available: https://doi.org/10.17226/14207
[100] Intelligent Transportation Systems, "Intelligent Transportation Systems (ITS) Professional Capacity Building Program," *Intelligent Transportation Systems*, 2018. [Online]. Available: https://www.pcb.its.dot.gov/factsheets/apc/apc_overview.aspx#page=tech. [Accessed: 20-Jul-2018]
[101] The Federal Transit Administration, "National Transit Database Provides Key Stats on Public Transportation in the U.S," *U.S. Department of Transportation*, 18-Jan-2018. [Online]. Available: https://www.transportation.gov/connections/national-transit-database-provides-key-stats-public-transportation-us. [Accessed: 20-Jul-2018]
[102] X. Chu, "Ridership Accuracy and Transit Formula Grants," *Transportation Research Record*, vol. 1986, no. 1, pp. 2–10, Jan. 2006 [Online]. Available: https://doi.org/10.1177/0361198106198600101
[103] M. Pilipovic, D. Spasojevic, I. Velikic, and N. Teslic, "Toward Intelligent Driver-Assist Technologies and Piloted Driving: Overview, Motivation and Challenges," in *X International Symposium on Industrial Electronics (INDEL'14)*, 2014, pp. 10–14.
[104] "CV Pilot Deployment Program," *Intelligent Transportation Systems*, 2018. [Online]. Available: https://www.its.dot.gov/pilots/cv_pilot_apps.htm. [Accessed: 20-Jul-2018]
[105] "Connected Vehicle Pilot Deployment Program," *Intelligent Transportation Systems*, 2018. [Online]. Available: https://www.its.dot.gov/pilots/index.htm. [Accessed: 20-Jul-2018]
[106] "Wyoming DOT Connected Vehicle Pilot," *Wyoming DOT Connected Vehicle Pilot*, 2017. [Online]. Available: https://wydotcvp.wyoroad.info/. [Accessed: 20-Jul-2018]
[107] "Connected Vehicle technology is coming to the streets of New York City!," *NYC Connected Vehicle Project*, 2018. [Online]. Available: https://cvp.nyc/. [Accessed: 20-Jul-2018]
[108] "THEA Connected Vehicle Pilot," *THEA Connected Vehicle Pilot*, 2018. [Online]. Available: https://www.tampacvpilot.com/. [Accessed: 20-Jul-2018]
[109] "Automated and Connected Vehicles," *Center for Advanced Automative Technology*, 2018. [Online]. Available: http://autocaat.org/Technologies/Automated_and_Connected_Vehicles/. [Accessed: 20-Jul-2018]
[110] "IEEE Standard for Information technology– Local and metropolitan area networks– Specific requirements– Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments," *IEEE Std 802. 11p-2010 (Amendment to IEEE Std 802. 11-2007 as amended by IEEE Std 802. 11k-2008, IEEE Std 802. 11r-2008, IEEE Std 802. 11y-2008, IEEE Std 802. 11n-2009, and IEEE Std 802. 11w-2009)*, pp. 1–51, Jul. 2010.
[111] "IEEE 1609 - Family of Standards for Wireless Access in Vehicular Environments (WAVE) Fact Sheets," *Intelligent Transportation Systems*, 2018. [Online]. Available: https://www.standards.its.dot.gov/factsheets/factsheet/80. [Accessed: 20-Jul-2018]
[112] J. B. Kenney, "Dedicated Short-Range Communications (DSRC) Standards in the United States," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011 [Online]. Available: https://doi.org/10.1109/JPROC.2011.2132790

[113] L. Hausermann, “Connected car: all the vulnerabilities in one infographic,” *Sentryo*, 19-Sep-2016. [Online]. Available: https://www.sentryo.net/infographic-vulnerabilities-connected-car/. [Accessed: 20-Jul-2018]
[114] K. Koscher *et al.*, “Experimental Security Analysis of a Modern Automobile,” in *2010 IEEE Symposium on Security and Privacy*, IEEE, Berkeley/Oakland, CA, USA, 2010, pp. 447–462 [Online]. Available: https://doi.org/10.1109/SP.2010.34
[115] Q. A. Chen, Y. Yin, Y. Feng, Z. M. Mao, and H. X. Liu, “Exposing Congestion Attack on Emerging Connected Vehicle based Traffic Signal Control,” in *Proceedings of the 25th Network and Distributed System Security Symposium (NDSS’18)*, San Diego, CA, 2018.
[116] A. S. Elmaghraby and M. M. Losavio, “Cyber security challenges in Smart Cities: Safety, security and privacy,” *Journal of Advanced Research*, vol. 5, no. 4, pp. 491–497, 2014 [Online]. Available: http://www.sciencedirect.com/science/article/pii/S2090123214000290
[117] T. Hunt, “Controlling vehicle features of Nissan LEAFs across the globe via vulnerable APIs,” *Troy Hunt*, Feb-2016. [Online]. Available: https://www.troyhunt.com/controlling-vehicle-features-of-nissan/. [Accessed: 20-Jul-2018]
[118] “Automated Vehicle Research,” *Intelligent Transportation Systems*, 2018. [Online]. Available: https://www.its.dot.gov/automated_vehicle/index.htm. [Accessed: 20-Jul-2018]
[119] T. Litman, “Autonomous Vehicle Implementation Predictions: Implications for Transport Planning,” presented at the Transportation Research Board 94th Annual Meeting, Washington, DC, 2018.
[120] A. Caplan, “Self-driving shuttle hits the streets,” *Gainesville Sun*, 03-May-2018. [Online]. Available: http://www.gainesville.com/news/20180503/self-driving-shuttle-hits-streets. [Accessed: 20-Jul-2018]
[121] MET Staff, “HART, May Mobility demo autonomous vehicle tech in downtown Tampa,” *Metro Magazine*, 01-Mar-2018. [Online]. Available: http://www.metro-magazine.com/technology/news/728711/hart-may-mobility-demo-autonomous-vehicle-tech-in-downtown-tampa. [Accessed: 20-Jul-2018]
[122] E. Brown, “New driverless shuttles to hit the roads in Babcock Ranch,” *Wink News*, 12-Jan-2018. [Online]. Available: http://www.winknews.com/2018/01/12/new-driverless-shuttles-hit-roads-babcock-ranch/. [Accessed: 20-Jul-2018]
[123] *J3016A: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*, (J3016_201609), SAE International, Sep. 2016 [Online]. Available: https://www.sae.org/standards/content/j3016_201609
[124] L. Brooke, “U.S. DoT chooses SAE J3016 for vehicle-autonomy policy guidance,” *SAE Articles*, Sep-2016. [Online]. Available: http://articles.sae.org/15021/. [Accessed: 20-Jul-2018]
[125] A. M. Wyglinski, X. Huang, T. Padir, L. Lai, T. R. Eisenbarth, and K. Venkatasubramanian, “Security of Autonomous Systems Employing Embedded Computing and Sensors,” *IEEE Micro*, vol. 33, no. 1, pp. 80–86, Jan. 2013.
[126] S. Riisgaard and M. R. Blas, *SLAM for Dummies: A Tutorial Approach to Simultaneous Localization and Mapping*, MIT Open Courseware [Online]. Available: https://dspace.mit.edu/bitstream/handle/1721.1/119149/16-412j-spring-2005/contents/projects/1aslam_blas_repo.pdf
[127] E. Guizzo, “How Google’s Self-Driving Car Works,” *IEEE Spectrum*, 18-Oct-2011. [Online]. Available: https://spectrum.ieee.org/automaton/robotics/artificial-intelligence/how-google-self-driving-car-works. [Accessed: 20-Jul-2018]

[128] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, “Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR,” presented at the Black Hat Europe, 2015 [Online]. Available: https://www.blackhat.com/docs/eu-15/materials/eu-15-Petit-Self-Driving-And-Connected-Cars-Fooling-Sensors-And-Tracking-Drivers-wp1.pdf
[129] M. Harris, “Researcher Hacks Self-driving Car Sensors,” *IEEE Spectrum*, 04-Sep-2015. [Online]. Available: https://spectrum.ieee.org/cars-that-think/transportation/self-driving/researcher-hacks-selfdriving-car-sensors. [Accessed: 20-Jul-2018]
[130] T. Simonite, “Self-Driving Cars’ Spinning-Laser Problem,” *MIT Technology Review*, 20-Mar-2017. [Online]. Available: https://www.technologyreview.com/s/603885/autonomous-cars-lidar-sensors/. [Accessed: 20-Jul-2018]
[131] R. N. Charette, “Commercial Drones and GPS Spoofers a Bad Mix,” *IEEE Spectrum*, Jun-2012. [Online]. Available: https://spectrum.ieee.org/riskfactor/aerospace/aviation/commercial-drones-and-gps-spoofers-a-bad-mix. [Accessed: 20-Jul-2018]
[132] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, “Internet of Things (IoT): Taxonomy of security attacks,” in *2016 3rd International Conference on Electronic Design (ICED)*, IEEE, Phuket, Thailand, 2016, pp. 321–326 [Online]. Available: https://doi.org/10.1109/ICED.2016.7804660
[133] M. B. Sinai, N. Partush, S. Yadid, and E. Yahav, “Exploiting Social Navigation,” *CoRR*, vol. abs/1410.0151, 2014 [Online]. Available: https://arxiv.org/abs/1410.0151
[134] M. Akers, “How does downtown’s autonomous bus work?,” *Las Vegas Sun*, 05-Apr-2018. [Online]. Available: https://lasvegassun.com/news/2018/apr/05/how-does-downtowns-autonomous-bus-work/. [Accessed: 15-Oct-2018]
[135] M. T. Garip, M. E. Gursoy, P. Reiher, and M. Gerla, “Congestion Attacks to Autonomous Cars Using Vehicular Botnets,” in *NDSS Workshop on Security of Emerging Networking Technologies (SENT)*, San Diego, CA, 2015.
[136] B. Owens, “Florida Law Creates Opportunity for AVs in the Sunshine State,” *Fisher Phillips*, 10-Oct-2018. [Online]. Available: https://www.fisherphillips.com/autonomous-vehicles-blog/florida-law-creates-opportunity-for-avs-in. [Accessed: 18-Oct-2018]
[137] M. Laris, “Trump administration pushing to ease roll-out of driverless cars and trucks,” *Washington Post*, 04-Oct-2018. [Online]. Available: https://www.washingtonpost.com/transportation/2018/10/04/trump-administration-pushing-ease-roll-out-driverless-cars-trucks. [Accessed: 19-Oct-2018]
[138] C. Watson, “Statistical Analysis of Crashes Occurring At Intersections in Malfunction Flash,” Georgia Institute of Technology, 2008 [Online]. Available: https://smartech.gatech.edu/bitstream/handle/1853/26508/watson_christopher_e_200712_mast.pdf
[139] R. Elvik, “How much do road accidents cost the national economy?,” *Accident Analysis & Prevention*, vol. 32, no. 6, pp. 849–851, 2000 [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0001457500000154
[140] K. Rector, “Baltimore 911 dispatch system hacked, investigation underway, officials confirm,” *Baltimore Sun*, 27-Mar-2018. [Online]. Available: http://www.baltimoresun.com/news/maryland/crime/bs-md-ci-911-hacked-20180327-story.html. [Accessed: 14-Oct-2018]

[141] K. Rector, “Hack of Baltimore’s 911 dispatch system was ransomware attack, city officials say,” *Baltimore Sun*, 28-Mar-2018. [Online]. Available: http://www.baltimoresun.com/news/maryland/crime/bs-md-ci-hack-folo-20180328-story.html. [Accessed: 14-Oct-2018]
[142] D. Sheehan, “What is Emotet? The virus that hit Allentown computers is widespread and dangerous,” *The Morning Call*, 21-Feb-2018. [Online]. Available: https://www.mcall.com/news/local/allentown/mc-nws-allentown-virus-follow-20180221-story.html. [Accessed: 18-Oct-2018]
[143] S. Schick, “Insider Threats Account for Nearly 75 Percent of Security Breach Incidents,” *SecurityIntelligence*, 28-Aug-2017. [Online]. Available: https://securityintelligence.com/news/insider-threats-account-for-nearly-75-percent-of-security-breach-incidents/. [Accessed: 18-Oct-2018]
[144] M. Satter, “The ransomware dilemma: Pay up or fight back?,” *State Scoop*, 04-Apr-2018. [Online]. Available: https://statescoop.com/the-ransomware-dilemma-pay-up-or-fight-back. [Accessed: 14-Oct-2018]
[145] “Vendor Vulnerability Reporting and Disclosure Policy,” *Cisco Security Threat and Vulnerability Intelligence*, 10-Nov-2014. .
[146] “Android,” *Android*, 2019. [Online]. Available: https://www.android.com/. [Accessed: 14-May-2019]
[147] ibotpeaches, “APKtool,” *APKTool Docs*, 2019. [Online]. Available: https://ibotpeaches.github.io/Apktool/. [Accessed: 23-Apr-2019]
[148] “Virtualbox,” *Oracle VM Virtualbox*, 2019. [Online]. Available: https://www.virtualbox.org/. [Accessed: 14-May-2019]
[149] “Passport Parking,” *Passport Parking Mobile Application*, 2019. [Online]. Available: https://ppprk.com/park/. [Accessed: 23-Apr-2019]
[150] “MyJTA Mobile Application,” *MyJTA Mobile Application*, 2019. [Online]. Available: http://myjta.com/. [Accessed: 23-Apr-2019]
[151] “How Google Handles Security Vulnerabilities,” *Google Application Security*, 2019. [Online]. Available: https://www.google.com/about/appsecurity/. [Accessed: 24-Jun-2019]
[152] “MMU-16E | EDI,” *EDI Traffic*. [Online]. Available: https://www.editraffic.com/products-page/mmu-16e/. [Accessed: 24-Jun-2019]
[153] “RS900 - Industrial Communication - Siemens,” *Siemens*. [Online]. Available: https://w3.siemens.com/mcms/industrial-communication/en/rugged-communication/ruggedcom-portfolio/switches-routers-layer-2/compact-switches/pages/rs900.aspx. [Accessed: 24-Jun-2019]
[154] Countermeasures Assessment & Security Experts, LLC and Western Management and Consulting, LLC, *Security 101: A Physical and Cybersecurity Primer for Transportation Agencies*, (Pre-publication draft of NCHRP Research Report 930), Transportation Research Board, Washington, DC, 2019 [Online]. Available: http://www.trb.org/Main/Blurbs/179516.aspx. [Accessed: 26-Sep-2019]
[155] “Chapter 501 Section 171 - 2014 Florida Statutes - The Florida Senate,” *The Florida Senate*. [Online]. Available: https://www.flsenate.gov/Laws/Statutes/2014/501.171. [Accessed: 24-Jun-2019]
[156] N. van der Meulen, S. Gunashekar, S. Soesanto, and E. Jo, “Good Practice Guide on Vulnerability Disclosure,” Jan. 2016 [Online]. Available: https://www.enisa.europa.eu/publications/vulnerability-disclosure

[157] J. Godfrey, P. Goyette, J. Bowden, and B. Pearl, “TCRP Project F-27: Characteristics and Elements of Non-Punitive Safety Reporting Systems for Public Transportation,” Embassy Suites Tampa - USF/Near Busch Gardens, 03-Jun-2019 [Online]. Available: https://www.cutr.usf.edu/fpta/. [Accessed: 24-Jun-2019]

Appendix A: Email Invitations for Project Survey

A.1: First Email from FDOT to Transit Agencies

From: Gabrielle Matthews

To: Florida Transit Planning Network

Cc: Sean Barbeau; Jarred Ligatti; Kevin Dennis; Maxat Alibayev

Subject: Transit Cybersecurity Survey

Dear Transit IT Specialists and Planners,

The Florida Department of Transportation is conducting a survey on the current state of cybersecurity in transit technologies. The purpose of this study is to provide agencies with better resources to address the challenges of cybersecurity.

We would like your participation in a brief 10-15-minute survey:

https://www.surveymonkey.com/r/ENHCSPBTR

If you know someone at your agency who is better suited to answer questions about IT systems, please forward this email to them.

Responses are due by Friday, May 18th. When the study is finished, we will send all participating agencies a copy of the final report.

Thanks very much for your help!

Gabe Matthews
Transit Planning Administrator
Florida Department of Transportation
605 Suwannee Street, MS 26
Tallahassee, FL 32399
(850)414-4803
gabrielle.matthews@dot.state.fl.us

A.2: Reminder Email from FDOT to Transit Agencies

From: Gabrielle Matthews

To: Florida Transit Planning Network

Cc: Sean Barbeau; Jarred Ligatti; Kevin Dennis; Maxat Alibayev

Subject: Transit Cybersecurity Survey

Dear Transit IT Specialists and Planners,

This is a reminder to participate in the Florida Department of Transportation's survey on the current state of cybersecurity in transit technologies. We have extended the deadline to Friday, May 25th. When the study is finished, we will send all participating agencies a copy of the final report.

The 10-15-minute survey can be found at:

https://www.surveymonkey.com/r/ENHCSPBTR

If you know someone at your agency who is better suited to answer questions about IT systems, please forward this email to them.

Thanks very much for your help,

Gabe Matthews
Transit Planning Administrator
Florida Department of Transportation
605 Suwannee Street, MS 26
Tallahassee, FL 32399
(850)414-4803
gabrielle.matthews@dot.state.fl.us

Appendix B: Survey Questions

1. Contact information

Your name
(will not be included in any publications)

Email address

Phone number

* 2. Agency name

The star (*) indicates that a response is required to proceed.

* 3. Please select which of the below technologies are ***currently deployed*** at your agency or in your region:

- [ ] Automatic Vehicle Location (AVL) and/or Computer Aided Dispatch (CAD)
- [ ] Automatic Passenger Counter (APC)
- [ ] On-Board Wi-Fi
- [ ] Fare payment (such as on-vehicle and/or mobile app, ticket vending machine)
- [ ] Online Trip Planner maintained by agency (not 3rd party apps like Google or Apple Maps)
- [ ] Communications system (such as regular radio, VoIP)
- [ ] CCTV Security Cameras (such as on-vehicle cameras)
- [ ] Traffic Signal Preemption/Priority (TSP)
- [ ] Signal Phasing and Timing for Connected Vehicles
- [ ] Traffic Management Software (such as Centracs)
- [ ] Traffic Light Controllers
- [ ] Traffic enforcement cameras (such as red light cameras)
- [ ] Other (please specify)

4. Are there Autonomous Vehicles (AVs) deployed at your agency?

- ◯ Yes
- ◯ No

5. Are there Connected Vehicles (CVs) deployed at your agency, such as V2I, V2V, or V2P?

- ◯ Yes
- ◯ No

6. Please identify the vendor(s) of the technologies being used at your agency

Autonomous Vehicles (if deployed)	
Connected Vehicles (if deployed)	
Automatic Vehicle Location (AVL) and/or Computer Aided Dispatch (CAD)	
Automatic Passenger Counter (APC)	
On-Board Wi-Fi	
Fare payment (such as on-vehicle and/or mobile app, ticket vending machine)	
Online Trip Planner maintained by agency (not 3rd party apps like Google or Apple Maps)	
CCTV Security Cameras (such as on-vehicle cameras)	
Traffic Signal Preemption/Priority (TSP)	
Communications system (such as regular radio, VoIP)	
Signal Phasing and Timing for Connected Vehicles	
Traffic Management Software (such as Centracs)	
Traffic Light Controllers	
Traffic enforcement cameras (such as red light cameras)	
Other from question 3	

7. Please select which of the below technologies are ***being considered*** for use at your agency:

- [ ] Automatic Vehicle Location (AVL) and/or Computer Aided Dispatch (CAD)
- [ ] Automatic Passenger Counter (APC)
- [ ] On-Board Wi-Fi
- [ ] Fare payment (such as on-vehicle and/or mobile app, ticket vending machine)
- [ ] Online Trip Planner maintained by agency (not 3rd party apps like Google or Apple Maps)
- [ ] Communications system (such as regular radio, VoIP)
- [ ] CCTV Security Cameras (such as on-vehicle cameras)
- [ ] Traffic Signal Preemption/Priority (TSP)
- [ ] Signal Phasing and Timing for Connected Vehicles
- [ ] Traffic Management Software (such as Centracs)
- [ ] Traffic Light Controllers
- [ ] Traffic enforcement cameras (such as red light cameras)
- [ ] Other (please specify)

8. With what probability would you estimate these **deployed** technologies are susceptible to attack or circumvention?

	0 - 25% (very unlikely)	26 - 50% (somewhat unlikely)	51 - 75% (somewhat likely)	76 - 100% (very likely)
Automatic Vehicle Location (AVL) and/or Computer Aided Dispatch (CAD)	○	○	○	○
Automatic Passenger Counter (APC)	○	○	○	○
On-Board Wi-Fi	○	○	○	○
Fare payment (such as on-vehicle and/or mobile app, ticket vending machine)	○	○	○	○
Online Trip Planner maintained by agency (not 3rd party apps like Google or Apple Maps)	○	○	○	○
Communications system (such as regular radio, VoIP)	○	○	○	○
CCTV Security Cameras (such as on-vehicle cameras)	○	○	○	○
Traffic Signal Preemption/Priority (TSP)	○	○	○	○
Signal Phasing and Timing for Connected Vehicles	○	○	○	○
Traffic Management Software (such as Centracs)	○	○	○	○
Traffic Light Controllers	○	○	○	○
Traffic enforcement cameras (such as red light cameras)	○	○	○	○
Other from question 3	○	○	○	○

9. With what probability would you estimate these technologies **under consideration** are susceptible to attack or circumvention?

	0 - 25% (very unlikely)	26 - 50% (somewhat unlikely)	51 - 75% (somewhat likely)	76 - 100% (very likely)
Automatic Vehicle Location (AVL) and/or Computer Aided Dispatch (CAD)	◯	◯	◯	◯
Automatic Passenger Counter (APC)	◯	◯	◯	◯
On-Board Wi-Fi	◯	◯	◯	◯
Fare payment (such as on-vehicle and/or mobile app, ticket vending machine)	◯	◯	◯	◯
Online Trip Planner maintained by agency (not 3rd party apps like Google or Apple Maps)	◯	◯	◯	◯
Communications system (such as regular radio, VoIP)	◯	◯	◯	◯
CCTV Security Cameras (such as on-vehicle cameras)	◯	◯	◯	◯
Traffic Signal Preemption/Priority (TSP)	◯	◯	◯	◯
Signal Phasing and Timing for Connected Vehicles	◯	◯	◯	◯
Traffic Management Software (such as Centracs)	◯	◯	◯	◯
Traffic Light Controllers	◯	◯	◯	◯
Traffic enforcement cameras (such as red light cameras)	◯	◯	◯	◯
Other from question 7	◯	◯	◯	◯

10. How critical are the following **deployed** technologies from an **operational** perspective?

	Not critical	Somewhat critical	Moderately critical	Very critical	Extremely critical
Automatic Vehicle Location (AVL) and/or Computer Aided Dispatch (CAD)	○	○	○	○	○
Automatic Passenger Counter (APC)	○	○	○	○	○
On-Board Wi-Fi	○	○	○	○	○
Fare payment (such as on-vehicle and/or mobile app, ticket vending machine)	○	○	○	○	○
Online Trip Planner maintained by agency (not 3rd party apps like Google or Apple Maps)	○	○	○	○	○
Communications system (such as regular radio, VoIP)	○	○	○	○	○
CCTV Security Cameras (such as on-vehicle cameras)	○	○	○	○	○
Traffic Signal Preemption/Priority (TSP)	○	○	○	○	○
Signal Phasing and Timing for Connected Vehicles	○	○	○	○	○
Traffic Management Software (such as Centracs)	○	○	○	○	○
Traffic Light Controllers	○	○	○	○	○
Traffic enforcement cameras (such as red light cameras)	○	○	○	○	○
Other from question 3	○	○	○	○	○

11. How critical are the following **deployed** technologies from a **financial** perspective?

	Not critical	Somewhat critical	Moderately critical	Very critical	Extremely critical
Automatic Vehicle Location (AVL) and/or Computer Aided Dispatch (CAD)	○	○	○	○	○
Automatic Passenger Counter (APC)	○	○	○	○	○
On-Board Wi-Fi	○	○	○	○	○
Fare payment (such as on-vehicle and/or mobile app, ticket vending machine)	○	○	○	○	○
Online Trip Planner maintained by agency (not 3rd party apps like Google or Apple Maps)	○	○	○	○	○
Communications system (such as regular radio, VoIP)	○	○	○	○	○
CCTV Security Cameras (such as on-vehicle cameras)	○	○	○	○	○
Traffic Signal Preemption/Priority (TSP)	○	○	○	○	○
Signal Phasing and Timing for Connected Vehicles	○	○	○	○	○
Traffic Management Software (such as Centracs)	○	○	○	○	○
Traffic Light Controllers	○	○	○	○	○
Traffic enforcement cameras (such as red light cameras)	○	○	○	○	○
Other from question 3	○	○	○	○	○

12. How critical are the following technologies **under consideration** from an **operational** perspective?

	Not critical	Somewhat critical	Moderately critical	Very critical	Extremely critical
Automatic Vehicle Location (AVL) and/or Computer Aided Dispatch (CAD)	○	○	○	○	○
Automatic Passenger Counter (APC)	○	○	○	○	○
On-Board Wi-Fi	○	○	○	○	○
Fare payment (such as on-vehicle and/or mobile app, ticket vending machine)	○	○	○	○	○
Online Trip Planner maintained by agency (not 3rd party apps like Google or Apple Maps)	○	○	○	○	○
Communications system (such as regular radio, VoIP)	○	○	○	○	○
CCTV Security Cameras (such as on-vehicle cameras)	○	○	○	○	○
Traffic Signal Preemption/Priority (TSP)	○	○	○	○	○
Signal Phasing and Timing for Connected Vehicles	○	○	○	○	○
Traffic Management Software (such as Centracs)	○	○	○	○	○
Traffic Light Controllers	○	○	○	○	○
Traffic enforcement cameras (such as red light cameras)	○	○	○	○	○
Other from question 7	○	○	○	○	○

13. How critical are the following technologies **under consideration** from a **financial** perspective?

	Not critical	Somewhat critical	Moderately critical	Very critical	Extremely critical
Automatic Vehicle Location (AVL) and/or Computer Aided Dispatch (CAD)	○	○	○	○	○
Automatic Passenger Counter (APC)	○	○	○	○	○
On-Board Wi-Fi	○	○	○	○	○
Fare payment (such as on-vehicle and/or mobile app, ticket vending machine)	○	○	○	○	○
Online Trip Planner maintained by agency (not 3rd party apps like Google or Apple Maps)	○	○	○	○	○
Communications system (such as regular radio, VoIP)	○	○	○	○	○
CCTV Security Cameras (such as on-vehicle cameras)	○	○	○	○	○
Traffic Signal Preemption/Priority (TSP)	○	○	○	○	○
Signal Phasing and Timing for Connected Vehicles	○	○	○	○	○
Traffic Management Software (such as Centracs)	○	○	○	○	○
Traffic Light Controllers	○	○	○	○	○
Traffic enforcement cameras (such as red light cameras)	○	○	○	○	○
Other from question 7	○	○	○	○	○

14. Is your agency considering deploying Autonomous Vehicles (AVs)?

- ◯ Yes
- ◯ No

15. When is your agency considering deploying Autonomous Vehicles (AVs)?

- ◯ In 0 - 2 years
- ◯ In 3 - 5 years
- ◯ In 6 years or more

16. Is your agency considering deploying Connected Vehicles (CVs)?

- ◯ Yes
- ◯ No

17. When is your agency considering deploying Connected Vehicles (CVs)?

- ◯ In 0 - 2 years
- ◯ In 3 - 5 years
- ◯ In 6 years or more

* 18. Which of the following types of data are collected and/or stored by your agency (in local or cloud-based systems)? Check all that apply.

- ☐ Customer information (including mobile fare payment information, IP address, MAC address)
- ☐ Employee information (including SmartCard ID, driver schedule)
- ☐ AVL/CAD operation data (including driver login info)
- ☐ Scheduling/planning resources (including daily schedules)
- ☐ Employee email
- ☐ Security camera records
- ☐ Other (please specify)

19. Where do you keep the following types of data?

	Local storage	Cloud storage	Both
Customer information (including mobile fare payment information, IP address, MAC address)	○	○	○
Employee information (including SmartCard ID, driver schedule)	○	○	○
AVL/CAD operation data (including driver login info)	○	○	○
Scheduling/planning resources (including daily schedules)	○	○	○
Employee email	○	○	○
Security camera records	○	○	○
Other from question 18	○	○	○

20. Do you share the following data with any third party?

	Yes	No	Don't know
Customer information (including mobile fare payment information, IP address, MAC address)	○	○	○
Employee information (including SmartCard ID, driver schedule)	○	○	○
AVL/CAD operation data (including driver login info)	○	○	○
Scheduling/planning resources (including daily schedules)	○	○	○
Employee email	○	○	○
Security camera records	○	○	○
Other from question 18	○	○	○

21. Do you encrypt the following data in your agency?

	Yes	No	Don't know
Customer information (including mobile fare payment information, IP address, MAC address)	○	○	○
AVL/CAD operation data (including driver login info)	○	○	○
Employee information (including SmartCard ID, driver schedule)	○	○	○
Scheduling/planning resources (including daily schedules)	○	○	○
Employee email	○	○	○
Security camera records	○	○	○
Other from question 18	○	○	○

22. How frequently is the data for your agency backed up? Multiple responses per row are available.

	Daily	Weekly	Monthly	Every 6 months	Yearly	Less than once a year
Customer information (including mobile fare payment information, IP address, MAC address)	☐	☐	☐	☐	☐	☐
AVL/CAD operation data (including driver login info)	☐	☐	☐	☐	☐	☐
Employee information (including SmartCard ID, driver schedule)	☐	☐	☐	☐	☐	☐
Scheduling/planning resources (including daily schedules)	☐	☐	☐	☐	☐	☐
Employee email	☐	☐	☐	☐	☐	☐
Security camera records	☐	☐	☐	☐	☐	☐
Other from question 18	☐	☐	☐	☐	☐	☐

23. How long is the backup data kept? Multiple responses per row are available.

	1 month	3 months	6 months	1 year	2 years or more
Customer information (including mobile fare payment information, IP address, MAC address)	☐	☐	☐	☐	☐
AVL/CAD operation data (including driver login info)	☐	☐	☐	☐	☐
Employee information (including SmartCard ID, driver schedule)	☐	☐	☐	☐	☐
Scheduling/planning resources (including daily schedules)	☐	☐	☐	☐	☐
Employee email	☐	☐	☐	☐	☐
Security camera records	☐	☐	☐	☐	☐
Other from question 18	☐	☐	☐	☐	☐

24. (Optional) Have your agency or its vendors been affected by any cybersecurity issues in the past?

25. (Optional) In your opinion, what are the biggest challenges for implementing good security in your agency?

Appendix C: Workshop Agendas

C.1: Mobile Fare Payment Workshop Agenda

Enhancing Cybersecurity in Public Transportation
Collaborative Cybersecurity Event Agenda

Friday, November 9, 2018
USF Kopp Engineering Building (ENG), room 003
5:00-6:00 pm – Speaker
6:00-7:00 pm – Student hands-on session

- This event is a part of the "Enhancing Cybersecurity in Public Transportation" project conducted by CUTR and the USF CSE department, and is funded by FDOT.
- The event is coordinated in partnership with SOFWERX[1], USF Whitehatters Computer Security Club[2], and Cyber Florida[3].
- The goal of the event is to bring together students, transportation professionals, and cybersecurity professionals to discuss and evaluate the security of public transportation mobile apps (e.g., fare payment apps).
- Students will have the opportunity to participate in a hands-on session, investigating vulnerabilities and mitigations in mobile applications deployed by Florida transportation agencies.

Please email Kevin Dennis (kevindennis@mail.usf.edu) and/or Maxat Alibayev (alibayevm@mail.usf.edu) with any questions.

Link to a list of mobile fare payment apps:

- https://docs.google.com/spreadsheets/d/17pabYzVRJxPfH84Y_GxrH7nxX-4ABl9lIiOEY_QNRcI/edit#gid=0

Recommended tools to install before the event:

- https://www.telerik.com/fiddler
- https://developer.android.com/studio/
- https://ibotpeaches.github.io/Apktool/

[1] https://www.sofwerx.org/
[2] https://www.wcsc.usf.edu/
[3] https://cyberflorida.org/

C.2: Traffic Cabinet Security Workshop

Enhancing Cybersecurity in Public Transportation
Collaborative Cybersecurity Event Agenda

Friday, January 25, 2019
Center for Urban Transportation Research, Room 202

- 5:00-5:30 pm – USF – Traffic Controller Overview
- 5:30-6:00 pm – Mission Secure – Vulnerability Overview
- 6:00-7:00 pm – Demo session with Traffic Controller

This event is a part of the "Enhancing Cybersecurity in Public Transportation" project conducted by CUTR and the USF CSE department, and is funded by FDOT. The event is coordinated in partnership with Mission Secure[1] and USF Whitehatters Computer Security Club[2]. The goal of the event is to bring together students, transportation professionals, and cybersecurity professionals to discuss and evaluate the security of traffic signal controller. Thanks to the City of Tampa[3] for providing a traffic cabinet and controller used in this event.

Remote connection information:

JOIN WEBEX MEETING
https://meetmsi.my.webex.com/meetmsi.my/j.php?MTID=m64f6b4043cf9269eb48154741e0e65e1
Meeting number (access code): 625 710 919 Meeting password: 6RB5zmwr

JOIN FROM A VIDEO SYSTEM OR APPLICATION
Dial sip:625710919@meetmsi.my.webex.com
You can also dial 173.243.2.68 and enter your meeting number.

JOIN BY PHONE
+1-510-338-9438 USA Toll
Tap here to call (mobile phones only, hosts not supported): tel:%2B1-510-338-9438,,*01*625710919%23%23*01*

Global call-in numbers:
https://meetmsi.my.webex.com/meetmsi.my/globalcallin.php?serviceType=MC&ED=757860527&tollFree=0

---

[1] https://www.missionsecure.com/
[2] https://www.wcsc.usf.edu/
[3] https://www.tampagov.net/

C.3: Cybersecurity in Public Transportation Workshop

Enhancing Cybersecurity in Public Transportation

Workshop on Security in Public Transportation

Agenda

	Opening Remarks
9:30 - 10:00	Introductions and Opening Remarks
	Presentations
10:00 - 10:20	USF Research Team • Enhancing Cybersecurity in Public Transportation • No session scribe
10:20 - 10:40	Dr. Yuguang Fang, University of Florida • Manage the Security Ecosystem of Public Transportation • Session Notes by: Dr. Christophe Bobda
10:40 - 11:00	Dr. Yasin Yilmaz, University of South Florida • Real-time Detection and Mitigation of Cyber-attacks in Intelligent Transportation Systems • Session Notes by: Dr. Arturo Bretas
11:00 - 11:20	Dr. Zoleikha Biron, University of Florida • Secure Control and Energy Management of Connected Vehicles with Integration of Power Grid • Session Notes by: Dr. Shigang Chen
11:20 - 11:40	Dr. Charalambos (Harrys) Konstantinou, Florida State University • Cybersecurity Challenges in Public Transportation • Session Notes by: Dr. Kemal Akkaya
11:40 - 12:00	Dr. Yier Jin, University of Florida • Sensor Security of Autonomous Public Transportation Systems • Session Notes by: Dr. Dong Chen
12:00 - 1:00	Lunch Break
1:00 - 1:20	Dr. Sandip Ray, University of Florida • Cybersecurity for Connected, Autonomous Vehicles: Impending Challenges And Integrative Solutions • Session Notes by: Dr. Yuguang Fang
1:20 - 1:40	Dr. Prabhat Mishra, University of Florida • Security and Trust Validation for Automotive SoCs • Session Notes by: Dr. Yasin Yilmaz

FDOT CUTR USF UNIVERSITY OF SOUTH FLORIDA

1:40 - 2:00	Dr. Sriram Chellappan, University of South Florida • Security, Privacy and Safety in ITS • Session Notes by: Dr. Zoleikha Biron
2:00 - 2:20	Dr. Christophe Bobda, University of Florida • Preventing Drone Hijacking using Hardware Sandboxing • Session Notes by: Dr. Charalambos (Harrys) Konstantinou
2:20 - 2:40	Dr. Arturo Bretas, University of Florida • Enhancing Cybersecurity of Scada Systems: Hybrid Physics Based Model Data Driven Algorithms for Security Enhancement • Session Notes by: Dr. Yier Jin
2:40 - 3:00	Dr. Shigang Chen, University of Florida • Security and Privacy in the Internet of Transportation-related Things • Session Notes by: Dr. Sandip Ray
3:00 - 3:20	Dr. Kemal Akkaya, Florida International University • Forensics and Interoperability for Secure Public-Transportation Operations • Session Notes by: Dr. Prabhat Mishra
3:20 - 3:40	Dr. Dong Chen, Florida International University • Preventing Electrical Vehicle Attacks and Faults using Data-driven Approach • Session Notes by: Dr. Sriram Chellappan
	Closing and Final Remarks
3:40 - 3:50	10 Minute Break
3:50 - 4:20	Review of Session Notes
4:20 - 4:30	Closing Remarks

Appendix D: Workshop Presentation Summaries

Manage the Security Ecosystem of Public Transportation

Presented by: Dr. Yuguang Fang, University of Florida
Session Scribe: Dr. Christophe Bobda, University of Florida

The presenter stated at the beginning of his presentation that he had no previous experience neither in transportation nor in security. The purpose of the talk was more visionary, to provide hints and potential directions in designing future secured transportation systems.

The constant introduction of edge devices is making life more enjoyable and solving many problems. However, many challenges are equally created, one of the most important being privacy. Dr. Fang provided a quick review of attacks models from physical (bomb attacks) corrupted data, jamming, network attacks (distributed denial of service) to fake transportation facilities that can cause substantial and damaging delays. Research have sought to address the previous-enumerated challenges in the past, however, increased attack surface are being created with the constant insertion of new devices at the edge.

The second part of the talk addressed the vision of system design and considerations for security. The main challenges in system design today is the integration of systems from various vendors and difficulty in isolating responsibility. Dr Fang then provide a short overview of traditional approach for system design with various domains and various issues that must be overcome for each domain. The main concern comes from the unknown edge devices that are later included into the system.

Dr. Fang presented his core research, namely “Location-based security” that rely on ID-based cryptography. Keys are created locally and tagged with spatiotemporal information. Authentication is location based and can be important in public transportation. Dr. Fang briefly presented his further research in 1) secure and power efficient protocols for reliable data delivery that uses agility for data transmission, thus making it capable to overcome jamming in the network, 2) cross-domain authentication with the goal of authenticate over domains with different security paradigms and implementations, 3) security in crowdsourcing that seeks to maintain the privacy of participants and 4) distributed big data machine learning. The talk ended with the vision of a management system for smart city ecosystems with devices embedded in infrastructure, roads and vehicles. Since security aspects are not yet considered, Dr. Fang was very interested in possible collaboration.

Questions 1: How do the security aspect is envisioned in the smart city ecosystem
Answer: Devices have communication and computation capability. Managers in charge of administering security rights handle all request related to security.

Follow up: Centralized point of management will cause single point of attack.
Answer: Not centralize but hybrid.

The speaker once again reiterated his willingness to participate in collaborative research in the broad field of smart cities.

Real-Time Detection and Mitigation of Cyber-Attacks in Intelligent Transportations Systems

Presented by: Dr. Yasin Yilmaz, University of South Florida
Session Scribe: Dr. Arturo Bretas, University of Florida

University of South Florida researchers are currently studying detection and mitigation strategies for cyber-attacks on transportation systems. The overall goal of the research is to make the transportation system smarter and more secure through a hybrid data driven model based solution.

Dr. Yilmaz began the presentation by introducing that his topic of study is anomaly detection, identification and mitigation. The project's focus is on intelligent transportation systems and vehicular ad-hoc network (VANET). Dr. Yilmaz then introduced the main types of attacks the research is interested in, as denial of service, distributed denial of service attack and false data injection attack.

Dr. Yilmaz then discussed a discovery, that the DDoS attack is more difficult to mitigate than the DoS attacks. He stated that the low rate DDoS attacks are a very dangerous kind of attack, because one would not see the future flooding consequence in the server. Dr. Yilmaz talked about how the FDI is more difficult to generate, however the consequences are potentially larger. Stated that the FDI attacks are harder to detect than the DoS attack.

Dr. Yilmaz stated that his solution, RAPID, is able to detect the low rate DDoS attack. He stated that his solution is systemic, meaning it analyzes all sensors data. One question was made during the presentation, as how the cumulative rate approach was used considering the DDoS attack, which is very difficult to detect. Yasin said this case of attack is difficult to detect however that his approach was able to detect such attack type.

Dr. Yilmaz presented RAPID, the anomaly detection framework he proposed. The algorithm is a hybrid approach based on machine learning, GEM and cumulative sum.

On training stage, the critical threshold value is obtained. This value is used on the cumulative sum for attack detection.

The detection part is cumulative, meaning that after some time if the value is above the threshold, the attack is detected.

Dr. Yilmaz stated that RAPID is not affected by the number of attackers. Several simulation results are presented in comparison with the state of the art.

Secure Control and Energy Management of Connected Vehicles with Integration of Power Grid

Presented by: Dr. Zoleikha Biron, University of Florida
Session Scribe: Dr. Shigang Chen, University of Florida

Dr. Biron presented her doctoral and postdoc research on security aspects of cyber-physical systems under two research thrusts: resilient control of connected vehicles and energy management of electric vehicles. The physical settings of her research were smart cities with a cyber space that manages smart grid, smart manufacturing, smart transportation, smart buildings, etc. She pointed out security issues in such cyber-physical systems (CPS) with examples of cyber attacks that caused physical damages without physical access.

The presentation discussed secure control of CPS for sustainability, energy efficiency and reliability, and moved on to connected autonomous vehicles and electric vehicles, which served as the context for joining security with energy management in her research.

One security challenge, DoS attack analysis and delay-based diagnostics, was addressed in length for a platoon of connected vehicles. Also discussed are electrical vehicle integration with power grid, charging and discharging optimization, and energy management of connected hybrid electrical vehicles.

The presentation was ended with a question on timing and threshold of DoS attack detection. Dr. Biron elaborated on the challenge of DoS attack analysis over unknown delay with limited parameter knowledge on modeling.

Cybersecurity Challenges in Public Transportation

Presented by: Dr. Charalambos Konstantinou, Florida State University
Session Scribe: Dr. Kemal Akkaya, Florida International University

The presentation started with motivating the fact that computing is evolving for the last 50 years and we are in the realm of cyber-physical systems (CPS) where everything is becoming smart and connected. However, this also increases the attack surface for the devices and systems deployed in CPS. There is also a move from electromechanical systems to microprocessor-based devices with COTS parts.

After this background, the presenter motivated the cybersecurity incident with power systems including Ukraine power grid attacks in 2015 and 2016 to differentiate between localized and centralized control. This requires that cybersecurity measures should be considered when deploying CPS. The presenter then focused on two issues: scalable testbed for cybersecurity assessment and GPS spoofing attacks.

For the cybsersecurity testbed, the presentation motivated the need for rich features other than the traditional network security aspects since there are new components in CPS. Given the lack of such cybersecurity testbeds especially for CPS, there is a need for realistic, scalable testbeds that can be used for research development and training. The presenter focused on the hardware in the loop (HIL) testbed. In HIL, there is a hardware controller, which is connected to a simulation environment that simulates the data collection and communications. While HIL testbeds are used widely for power systems, the presenter stressed that it will be good to have a HIL for transportation domain.

The presentation then detailed the elements of GPS spoofing attack. Initially, there was a good motivating example case, which happened on April 24, 2019. Basically, there was a GPS app for vehicles, which can be remotely compromised and lead to attacks including stopping engines. In power systems, phasor measurement units (PMUs) are used for data collection and they have a GPS module. According to the IEEE C37.118 standard, there is an error threshold for time phases. The presenter demonstrated how GPS spoofing can be realized in a power system using software defined radios and open source software for generating GPS signals. The goal was to introduce a delay to increase PMU errors (i.e., signal angle). This impact was also realized in a realistic testbed including HIL. The presentation concluded that we also need to consider physical properties of the system for addressing cybersecurity in a comprehensive manner.

The audience asked about the impact of PMU on the system in general. The presenter indicated that when there is an attack on PMU, it can unnecessarily trigger certain operations in substations. There was also a comment from the audience that traffic control units also utilize GPS devices and this attack can be also possible there.

Sensor Security and Autonomous Public Transportation System

Presented by: Dr. Yier Jin, University of Florida
Session Scribe: Dr. Dong Chen, Florida International University

The growing complexity of a modern car has added another potential point of failure in the form of cyber or sensor attacks. Recently, University of Florida researchers have been looking at that vulnerability in vehicle's software or sensing units could enable them to remotely alter the intended operation of the vehicle sensors.

The presentation first introduced the history of autonomous transportation. The autonomous transportation was first mentioned in 1913. It has a wide range of benefits for people in daily life, for example, severing as the fast and last mile solution and mitigating driver shortage problem. Modern autonomous public transportation systems have hundreds of hard components, such as Lidar, Radar, PCM, GPS receiver, Embedded units and etc. However, what will happened if these sensors are not reliable and fail? Recently, the hardware component failure incidents have already caused train crash and airplane crash.

The team then discussed a set of sensor cyber-attacks that might could occur due to failure of sensors during an attack in autonomous transportation: (1) GPS spoofing and Jamming spoofing

replay in train control systems. (2) Stealthy Jamming Attack: decrease the performance of the platoon. Especially, their experiments on real Lidar data show the need of security in public transportation, including improving resiliency to cyber-incidents and reducing the cyber threats.

The team then presented three novel techniques that can mitigate those sensor-based attacks.

- Active attack detection using amplitude detector data;
- Attack detection and estimation using thresholding approaches without any hardware modification;
- Distributed system sensor attack detection using resilient distributed state estimators.

The presentation ended with a discussion of what kind of data are used to evaluate these attacks. The researchers at University of Florida use simulation of radar readings to verify their approaches. Participants also suggested more real data might be used to verify and enhance the preventing techniques.

Cybersecurity for Connected, Autonomous Vehicles: Impending Challenges and Integrative Solutions

Presented by: Dr. Sandip Ray, University of Florida
Session Scribe: Dr. Yuguang Fang, University of Florida

Dr. Sandip Ray from the University of Florida presented his research on cybersecurity of connected and autonomous vehicles (CAVs) from security of platooning control to malicious detection messages by applying machine learning techniques. He reviewed some of his research efforts and briefly discusses his ongoing projects.

The talk starts with the review of automobile electronics and control systems, then identifies what are needed to protect in public transportation: sensing and real-time data collection, connectedness (communications), and autonomy. Based on where attacks would happen: car hacks or infrastructure hacks, he discusses the general attacks and vulnerability of CAVs. Particularly, he identifies a few challenges in cybersecurity of CAVs such as security-aware design of autonomous subsystems, interactive/integrative management under adversarial attacks, robust automotive SoC design, and resilient V2X communications.

The talk continues with the review of the current solutions and the problems, points out the weakness (e.g., the requirement of detailed model), and then presents his solution, the machine learning based solution. The idea is to identify the potentially malicious attacks by learning the normal behavior of driving. Initial study over autonomous vehicle testbed is also presented.

The talk ends up with some future research directions. One particular challenge is to investigate where and how the machine learning algorithms are implemented. How to leverage cloud and onboard processing units should be studied.

Security and Trust Validation for Automotive SoCs

Presented by: Dr. Prabhat Mishra, University of Florida
Session Scribe: Dr. Yasin Yilmaz, University of South Florida

Main idea: Verifying the security of System-on-Chip (SoC) components in automobiles.
Key details:

1) Embedded systems in automobiles are complex including analog computing, digital computing, software, etc.
2) More electronics mean more vulnerability
3) Security threat models must be known to generate verification scenarios
4) Some verification techniques:

- Logic Testing: statistical approach - statistical test generation
- FSM (Finite state machine) Anomaly detection
- Equivalence checking
- Proof-carrying hardware
- Side channel analysis for vulnerability detection
- Logic testing + side-channel analysis

Conclusion:

1. Security means protected components.
   This is in contrast with verification because debugging requires full observability.
   How to debug if you cannot observe any signals in the security model?
2. Long lifetime for automobiles is a problem since decades-old cars can be hacked easily by unsophisticated adversaries.

Security, Privacy and Safety in ITS

Presented by: Dr. Sriram Chellappan, University of South Florida
Session Scribe: Dr. Zoleikha Biron, University of Florida

Vulnerabilities of intra- vehicles components.

Vulnerabilities of communications in ITS and also focusing on trains to use camera and more intelligent information to make a safer train- reducing the liability.

Dr. Chellappan proposed Machine learning techniques to make ITS safer.

Dr. Chellappan mentioned that more than 70 ECE, with billions of lines of coding + apps

Focus mainly on communications in-vehicle two different communication lines (high and low CAN) and components talking to each other all time, we cannot isolate them. Faulty component sends info for all.

Dr. Chellappan also explained the scenarios of hacking the car, external adversary apart from the personal intentions to hack the car

Research in University of California San Diego hacking the car in the paper. Showing all possible cyber-attacks while the access to the car is possible. Moreover, he introduced other possible attacks, e.g., DOS, multiple identity attack, and privacy challenge

After that, Dr. Chellappan proposed PUFs high degree hardware security- figureprint in hardware for countermeasures.

Questions on CAN vulnerabilities and the law for the suicide incidents that Dr. Chellappan addressed the questions and mentioned that the liability reduction is major objective for the train industries and the information can be used to defend drivers that they took correct reactions.

Preventing Drone Hijacking Using Hardware Sandboxing

Presented by: Dr. Christophe Bobda, University of Florida
Session Scribe: Dr. Charalambos (Harrys) Konstantinou, Florida State University

University of Florida researchers, and particularly Dr. Bodba, are currently studying the security of embedded systems and presented a jamming prevention method using hardware sandboxing. The project focuses on drone and UAV systems. Such systems are becoming complex nowadays due to the increased desired functionality and the optimization necessities for different design metrics such as unit cost, size, power, performance, flexibility, etc.

The presentation introduced the motivation for the talk being the fact that UAV are becoming more and more commonplace. Such devices are often remote-controlled and their operation is based on RF communications.

Dr. Bodba then presented different types of jammers (constant, random, reactive, intelligent) and raised the question how research should focus on securing drone flights from such jammers. Anti-jamming technology and detection methods such as comparing signal to noise ratio, comparing packet loss in transmission, etc. exist to address the issue. However, Dr. Bodha presented an approach that relies on hardware as a root-of-trust without relying on software or network solutions. The goal this project approach is to ensure jamming detection and response regardless of type of attacker knowledge. The methodology is based on hardware sandboxing which build rules to monitor signals and protocols at run-time. The concept is based on software sandboxing, and being applying to the hardware layer: ensure security policy at the interface of components and IPs while providing isolated, virtual resources that are managed by the sandbox.

The structure of the hardware sandbox consists of four modules: a management module, a property-based checker based on Open Verification Library (OVL) (i.e., a library of assertion checkers), virtual resources (for complying with protocols), and registers related with the status and the configuration of the system. The concept is applied to System-on-Chips (SoC) to sandbox hardware IP components which can be considered untrustworthy in order to ensure isolation and prevent jamming. The testing was focus on a hexacopter-based UAV application with RF transmitters and receivers with FPGA implementation. The hardware sandbox is incorporated

between the RF receiver module and receiver control of the UAV device. The drone-specific hardware sandbox solution demonstrated via jamming simulations that can block attack values.

Participants asked Dr. Bodba about protocols compliance for UAV systems and how hardware trojans can be considered an abnormality if they are not within the specifications of the protocol guidelines. Dr. Bodba explained that how functional and non-functional data can be used with machine learning to address such issues.

Enhancing Cybersecurity of SCADA Systems: Hybrid Physics Based Model Data Driven Algorithms for Security Enhancement

Presented by: Dr. Arturo Bretas, University of Florida
Session Scribe: Dr. Yier Jin, University of Florida

Dr. Arturo Bretas is currently studying SCADA systems security. A Typical SCADA systems consist of: 1) Input and output devices; 2) Remote terminal units; 3) Programming logic controllers; 4) Centralized computers; 5) Communications systems and interfaces (RS-232, RS-485, Ethernet, etc.); 6) User Interfaces; and 7) Standard and/or custom SCADA or HMI software. SCADA systems collect sensor measurements and operational data from the field, process and display this information and relay control commands to local and remote equipment.

The presentation introduced cyber physical threats on SCADA systems due to the following reasons: 1) Technical information available – public information about the infrastructure and controls systems in available online; 2) Remote connections are vulnerable – connections as VPSs and wireless networks are used for remote diagnosis, maintenance and examination of system status; and 3) Networking of control systems – organizations have increased connectivity though the integration of their control systems and enterprise networks.

Dr. Arturo Bretas then discussed the problem formulation and solutions based on the Gauss-Newton method. The threat of fault data injection (FDI) was also introduced. After that, Dr. Bretas presented the machine learning based solution for SCADA system security. Multiple challenges were solved which including the following:

- Dimensional Reduction:
    - Feature extraction: transformers the existing features into a lower dimension space by finding the highest value eigenvalues and corresponding eigenvectors;
    - Feature subset selection: determines a strong correlated subset of features based on a “goodness” criterion without transforming the original data set;
- Principal Component Analysis:
    - Reduce the dimensionality of the data set while retaining as much as possible the variation present in the data;
- Forward Feature Selection – SFFS Algorithm:
    - Floating algorithms have an additional exclusion or inclusion step to remove features once they are included or excluded, so a large number of subset feature combinations can be sampled;

The presentation ended with a discussion on how to apply the developed theoretical methods in industrial systems. Collaborations among universities, industry and government agencies were urgently needed to secure SCADA systems.

Security and Privacy in the Internet of Transportation-related Things

Presented by: Dr. Shigang Chen, University of Florida
Session Scribe: Dr. Sandip Ray, University of Florida

Two topics:

- Privacy-preserving traffic measurement
- Anonymous use of IoTT

Measuring point-to-point traffic:

- Camera or other sensors
- How to measure traffic volume between two points or through an arbitrary set of selected points as a function of time
    - Can be used to address congestion and improve infrastructure
- One approach:
    - Each vehicle transmits its ID to road-side equipment (RSE), or phone/GPS transmits its ID to a server
    - Point-to-point Traffic: Compare the IDs collected by two RSEs
- But that leads to privacy challenges.
    - Drivers can be tracked, entire travel history day by day
- Privacy preserving approaches:
    - Probabilistic bitmap encoding for privacy protection:
        - When vehicle passes a location you encode a bit. Do this at different locations. Look at this bitmap and see the common 1.
        - But the index becomes id.
        - So need to create uncertainty while still having statistical signature.
        - System parameter controls the trade-off between privacy and measurement accuracy.

IoTT:

- Tagged cars or tickets, to enable old cars/tickets or any other to IoT vision.
- They can track objects, environment, authentication too.
    - But privacy?
- Do RFID tag anonymously
- Various anonymity:
    - Weak Anonymous Model
    - Strong Anonymous Model
    - Group Anonymous Models
    - Weak group anonymous model
    - Strong group anonymous model
- Weak anonymous:
    - Prevent eavesdroppers or unauthorized readers from tracking tag carriers
- Strong:

    - Prevent authorized readers or compromised server from tracking tag carriers
- Threat Model:
    - Eavesdropping
    - Unauthorized readers
    - Unauthorized use of data or compromised server
    - Captured tags
    - Denial of service
    - Replay attack
- Cipher:
- Experiments:

Forensics and Interoperability for Secure Public Transportation Operations

Presented by: Dr. Kemal Akkaya, Florida International University
Session Scribe: Dr. Prabhat Mishra, University of Florida

University of South Florida researchers are currently studying the attacks and countermeasures of public transportation systems. Dr. Akkaya began the presentation introducing smart vehicles with a wide variety of components. This presentation addressed two major challenges in enabling secure public transportation systems: forensics and interoperability.

The first part of the presentation deals with vehicular forensics. The basic idea is to effectively use the data collected through a wide variety of sensors in the vehicle as well as by the infrastructure. While existing methods utilize machine learning for data analysis, this talk motivated the need for effective use of data for vehicular forensics.

When there is an accident in public transportation, there would be liability. Dr. Akkaya used an example from traditional forensics effort where a police arrives after an incident (e.g., car accident), and collects information through samples, pictures and interviews with the witnesses. Once the data collection is done, data is analyzed and report is prepared, which may be used in a court. Lack of data (e.g., UBER incidence) or tampered data can lead to unintended consequences. Therefore, a mechanism for ensuring tamper-proof data is necessary.

The presentation described Block4Forensics that considers all stakeholders including vehicles, insurance companies, manufacturers, etc. While data mainly comes from the vehicle, but a service provider (e.g., maintenance) can also add data. The presentation outlined how a blockchain technology can be utilized to ensure that the data is tamper proof. It described different components including leader, validator, etc. Various practical aspects were discussed such as storing only summary of data (such as hash) instead of storing a lot of data in block chain.

The second part of the presentation deals with control security for public transportation. It starts with the observation that SCADA is used for energy systems as well as many transportation systems. Since SCADA cannot be changed frequently, an important challenge is how to add resources to enable secure communication. It described the design of an efficient and interoperable infrastructure that communicates with IP network as well as SCADA network. The

presentation also covered efficient key management techniques since the communication infrastructure has limited resources. The presentation concluded with results, which demonstrated that the proposed interoperable framework outperforms the existing approaches.

Preventing Electrical Vehicle Attacks and Faults using a Data Driven Approach

Presented by: Dr. Dong Chen, Florida International University
Session Scribe: Dr. Sriram Chellappan, University of South Florida

Smart-phone apps (designed by manufacturers) that are integrated into smart cars collect a significant volume of data related to how user operates car. Not necessarily to infer braking patterns or turning patterns or paths taken, but rather how much AC is used, how often music was on, whether or not hand brakes were used and so on. Dr. Dong Chen presented research on how this data could be used to profile driver behavior. This may have some applications related to theft detection when the cloud is looking for anomalies. But for this application, real-time data must be shared, which we are not sure of. We are not sure if these applications are in mind at the cloud when it is collecting such data. What is concerning though is users sharing all this data to the cloud without being aware of how such data can be used. Can such data be used to decide insurance rates, the mental health of a subject etc. There are clear possibilities for privacy breaches here.

Dr. Dong Chen also presented some research perspective on how users could compromise amount of power they draw from charging stations that are solar powered, so that they draw more power, but pay less. He presented preliminary ideas using correlation calculations to catch such attacks.