CYBERSECURITY IN PUBLIC TRANSPORTATION: A LITERATURE REVIEW

Kevin Dennis, Maxat Alibayev, Sean J. Barbeau, Ph.D., Jay Ligatti, Ph.D.
Computer Science and Engineering Department and Center for Urban Transportation Research
University of South Florida
Tampa, FL 33620
813-974-7208
{kevindennis, alibayevm}@mail.usf.edu, barbeau@cutr.usf.edu, ligatti@usf.edu

November 14, 2018

6,821 words

Abstract

Transportation information technologies (IT) 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. This paper reviews the existing literature regarding the state of cybersecurity in public transportation, focusing on the technical aspects of security previously published in technical venues. In particular, the paper examines transit technologies, equipment, and protocols for known vulnerabilities and defenses. Existing attack and vulnerabilities were identified for the following technologies: connected vehicles (CVs), autonomous vehicles (AVs), electronic ticketing systems, traffic signal controllers, traffic signal priority/preemption (TSP), and dynamic message signs (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 authors believe that it is reasonable to expect that security vulnerabilities do exist in these technologies as well. Several directions for future work are discussed, including better employee training, architecture of on-board Wi-Fi systems used for critical operational purposes, and data encryption and sharing policies at the agency, especially as related to customer data.

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. Public transportation vehicles 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.

This paper reviews existing transit technologies, including equipment and protocols, for known vulnerabilities and defenses. The review focuses on technologies deployed at Florida transit agencies as well as those considered for future deployment.

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.

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 the Related Reports section.

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 and did not pay the ransom because their files were backed up before the attack. A week later, the same ransomware struck them again. It mutated into a new virus and re-infected the computers.

Related Reports

Securing Control and Communications Systems in Transit Environments [2]

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.

Protection of Transportation Infrastructure from Cyber Attacks: A Primer [1]

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.

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].

Agencies should consider the risks involved with each of the following technologies, including the likelihood of the technologies being attacked and the consequences of successful attacks. Agencies should also consider the differences between OT and IT. For example, operational technologies such as traffic cabinet controllers or autonomous vehicles have a greater risk of causing physical damage than information technologies such as mobile fare payment, but may have less exposure to attackers than information technologies. Separate work will provide an in-depth analysis of the risks associated with each technology.

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 sensitive information at a web link provided in the email.

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 [14]. 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 [15]. Ransomware is often distributed in phishing attempts; 93% of phishing emails contain ransomware [16]. The US-CERT [14] lists several preventative measures, including developing and executing proper backup and data recovery plans, and staying up-to-date with system updates.

Botnets are becoming increasingly problematic as the number of Internet of Things (IoT) devices continues to increase [18]. 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").

New attacks on IT systems have been discovered with the growing popularity of cryptocurrencies, including cryptojacking. Cryptojacking takes place when unauthorized software generates, or "mines," cryptocurrency on a computer. Cryptojacking may be deployed via a botnet. Agencies will see a drop in machine performance on computers impacted by cryptojacking due to extra CPU load. The agency servers may need to be temporarily brought down to prevent the spread of malware or other attacks [19]. Zimba et al. [17] describe a sophisticated strategy for crypto mining attacks that, unlike the previously discussed phishing and ransomware attacks, do not depend on intermediary factors in the attack chain (e.g., bypassing intrusion detection systems or persuading the end user to launch it). The malware is injected into a web server and is run by the browser of the user who visits the infected website. This strategy avoids any intrusion detection systems as the malware is not permanently stored on the victim's machine but instead is dynamically loaded and executed by the client machine when the user visits the website. The generated cryptocurrency is then sent to the attacker. The method also impacts mobile devices (e.g., smartphones, tablets) that visit the same site via their internet browsers. Cryptojacking can also be implemented in native mobile or personal-computer apps that masquerade as games, utilities, or other legitimate applications.

Insider threats make up nearly 75% of security breach incidents [20]. Insider threats refer to employees or other authorized users that intentionally or accidentally 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.

TRANSIT TECHNOLOGIES

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 [21]. 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" [22]. Real-time arrival information may increase passenger satisfaction, ridership, and perception of personal security, and reduce time spent waiting [4], [22].

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 [23] 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 [24].

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 [25].

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 [26].

Online trip planners have been moving toward open-source solutions in recent years. Popular examples include OpenTripPlanner [27] and OneBusAway [23]. 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 [21], [28].

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) [29] 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.

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 [30] 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 and benefits, as the bug-discovery process for both attackers and defenders is improved. Payne [31] provides a more in depth review of the benefits and risks presented by open source software.

Electronic Ticketing and Mobile Fare Payment Systems

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 [32].

A survey from 2016 [3] 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" [32].

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 [32].

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) [33] or Bluetooth Low Energy (BLE) [34].

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 [35], [36] 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.

Smart cards employ cryptographic ciphers in their communications, for example using DES, AES, or RSA [37]. Abbott [38] lists vulnerabilities that may be exploited to break the cryptographic implementations in smart cards, such as differential power analysis [39], 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. [40] 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. [41] further describe potential attacks against electronic ticketing systems, such as impersonation and tracing, and analyze existing electronic ticketing systems.

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].

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).

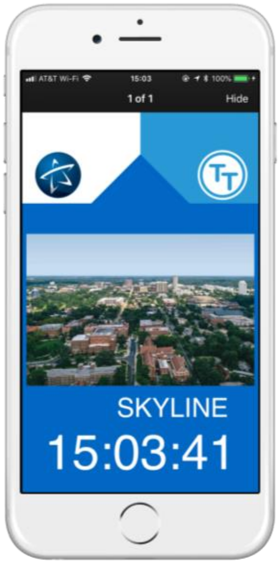

Figure 1 **Example of a visual validation screen from Token Transit [42]**

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 1 shows an example of a screen from Token Transit [42], 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 [43] 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 [44].

Security Considerations 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. [45] 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. 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 [46] have found malware that was spoofing Uber's Android application. 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.

Field Devices

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 [47]. 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 [48].

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. Traffic controllers are also becoming increasingly connected [49], communicating over private networks back to the agency monitoring the intersection and to other traffic signal controllers in the area.

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 [50]. 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 [51]. Wireless cellular phones are also seen in the literature as an alternative to infrared [52].

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. 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 [53].

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 [54]. 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 [55].

Traffic signal controllers are also susceptible to remote attack. Ghena et al. [56] 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.

Due to the lack of authentication and encryption, traffic signal controllers are also sensitive to falsified data. Cerrudo [57], [58] 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 [59]. Laszka et al. developed a "polynomial-time heuristic algorithm for computing approximately optimal attacks" [60], 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 (e.g., 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 [61].

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 [62]. 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 [63], [64].

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 [63] 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 [63].

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 [63]. Some DMS devices are now

Internet-enabled over IP, allowing any device with Internet browser support to login and manage the DMS device [65].

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 [66]. Attacking a DMS and modifying the message has become a popular prank. Online guides [67] have been published on the Internet giving detailed instructions on how a layperson can change the message of these signs.

The online guide [67] lists a number of security issues present with DMS devices and how they can be taken advantage of. Figure 2 presents a compromised DMS found in the online guide's gallery of compromised DMSs [67]. 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 [68].

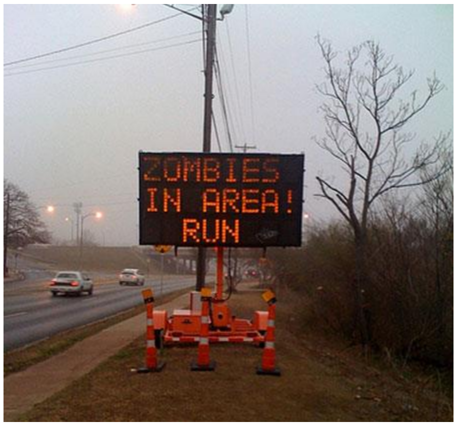

Figure 2 **A compromised DMS from an online guide on exploiting DMSs [67]**

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 [69]. 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 [70]. CCTV may reduce transit worker assaults and "was considered the most effective technology by survey participants in the prevention of operator assaults" [71].

Implementation CCTV may be monitored in real time or used for forensic investigation [70]. The American Public Transportation Association (APTA) created a recommended practice [72] 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.

Security Considerations Costin [73] 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 [74], allowing attackers to gain access to these systems.

Shodan [75], 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 [73], 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.

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 [76]. 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 [77].

Security Considerations User privacy is the primary concern for public Wi-Fi expressed in the literature. Gupta and Jha [78] 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.

Operations and Fleet Management

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 [22].

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 [79], [80].

Security Considerations No literature could be found detailing vulnerabilities in CAD/AVL technologies. In Baltimore, Maryland, the police CAD system was disabled, but the issue was unrelated to the CAD system [81].

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 [82] 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 [82].

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 [83]. 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.

Security Considerations No papers were found that discussed the security of APCs in detail. APC devices that provide wireless connections 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).

Emerging Technologies

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) [84], Vehicle-to-Infrastructure (V2I) safety, and Vehicle-to-Vehicle (V2V) safety [85].

In September 2016, the USDOT initiated the Design/Build/Test phase of the Connected Vehicle (CV) Pilot Deployment Program [86], providing over $45 million to Wyoming [87], New York City [88], and Tampa [89] 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.

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) [90]. Connected vehicles communicate using a variety of protocols including IEEE 802.11p Wireless Access in Vehicular Environments (WAVE) [91], [92], GPS, cellular, Bluetooth [93], and Wi-Fi. Kenney [94] 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 [95] created an infographic that summarizes all of the potential attack surfaces into one image. Mobile applications, infotainment systems, and the on-board diagnostics (OBD) port are marked as high-threat areas. This marking aligns with the reports by Koscher et al. [96] and Checkoway et al. [97], which describe how these systems can be exploited to gain full control of the vehicles.

Koscher et al. [96] found several vulnerabilities that allowed the researchers with physical access to CVs to gain full control of the vehicles. Checkoway et al. [97], 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 [98] 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 high as 68.1% [98].

Privacy concerns are also present in connected vehicles. Elmaghraby and Losavio [99] 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 [99]. In February, 2016, security researcher Troy Hunt posted on his blog [100] 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).

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 [101]. There are various levels of automation, ranging from not automated to fully automated.

Litman [102] 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.

Implementation SAE J3016 [103] was chosen as the official reference for the levels of vehicle autonomy by the USDOT [104]. 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) [105].

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” [106].

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) [107].

Security Considerations As with connected vehicles, AVs may have vulnerabilities similar to those discovered by Checkoway et al. [97] if wireless access to the vehicle is enabled, allowing an attacker to gain remote control of the vehicle. Wyglinski et al. [106] 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.

Google researchers [108], [109] were 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 [110]. 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 [111]. Considering that LiDAR is considered a vital ingredient in most AV systems [112], LiDAR-based vulnerabilities may prove to be a primary cybersecurity concern in AV deployments. Petit et al. 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 [110]. GPS is also susceptible to spoofing [113].

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, and 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 authors believe that it is reasonable to expect that security vulnerabilities do exist in these technologies as well.

Based on information gathered during this literature review as well as from a survey of Florida public transportation agencies conducted during this project, several themes have emerged for future areas of study. First, agencies should frequently update firmware and software for all computers, including embedded devices. Second, 11 out of 15 Florida transit agencies said that they "were not impacted by cybersecurity issues" and two of the 15 responded that they were not aware of any cybersecurity impacts. The remaining two agencies reported phishing attacks as well as a hacked agency website and Facebook page. Additional training for employees to help recognize and respond to potential cybersecurity issues, including phishing attempts and social engineering, would be helpful. The most commonly reported challenge for implementing good security practices was employee training, followed by funding. Future work should examine the architecture of on-board Wi-Fi systems used for critical operational purposes to determine whether these systems are susceptible to attack. Increased scrutiny should be given to operationally critical Wi-Fi systems that are also used for on-board Internet access by riders. Further investigation is also recommended to determine where agencies have protected data using encryption and where they have not (e.g., differentiating encryption of "data at rest" vs "data in flight"). 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.

As part of this research project, a taxonomy classifying transportation technologies by their risks and liabilities will be developed based on information gathered in this literature review. In addition, a working group including transit agencies and cybersecurity professionals is being organized in Florida to better understand the risks and mitigations currently considered by transit agencies. As a part of the project, mobile fare payment applications and a traffic controller will be analyzed for new vulnerabilities. A final report will be developed that consolidates this information, and summarizes the vulnerabilities and risks in public transportation technologies. It is hoped that this study will improve the cybersecurity posture of public transportation systems.

ACKNOWLEDGEMENTS

This paper is part of the "Enhancing Cybersecurity in Public Transportation" project funded by the Florida Department of Transportation and National Center for Transit Research. The opinions, findings, and conclusions expressed in this publication are those of the author(s) and not necessarily those of the Florida Department of Transportation or the U.S. Department of Transportation. The authors would like to thank Gabrielle Matthews for serving as the FDOT Project Manager. The authors would also like to thank Vik Bhide from the City of Tampa for sharing his expertise on the subject.

The authors confirm contribution to the paper as follows: study conception and design: S. Barbeau, J. Ligatti; data collection: K. Dennis, M. Alibayev; analysis and interpretation of results: K. Dennis, M. Alibayev, S. Barbeau, J. Ligatti; draft manuscript preparation: K. Dennis. All authors reviewed the results and approved the final version of the manuscript.

REFERENCES

[1] Countermeasures Assessment and Security Experts LLC and Western Management and Consulting LLC, National Cooperative Highway Research Program, T. C. R. Program, T. R. Board, and National Academies of Sciences, Engineering, and Medicine, *Protection of Transportation Infrastructure from Cyber Attacks: A Primer*. THE NATIONAL ACADEMIES PRESS, 2016.

[2] American Public Transportation Association, “Securing Control and Communications Systems in Transit Environments: Part 1: Elements, Organization and Risk Assessment/Management,” 1666 K Street, NW, Washington, DC, 20006-1215, APTA-RP-CCS-1-RT-001-10, Jul. 2010.

[3] N. L. Georggi, S. Barbeau, and A. Joslin, “Assessment of Mobile Fare Payment Technology for Future Deployment in Florida,” Florida Department of Transportation, Mar. 2016.

[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*, 2010, pp. 1807–1816.

[5] “Operational Technology (OT),” Nov-2012. [Online]. Available: https://www.gartner.com/it-glossary/operational-technology-ot/

[6] B. Gregory-Brown and D. Harp, “Security in a Converging IT/OT World,” SANS Institute, Nov. 2016.

[7] “Cyber-Physical Systems - a Concept Map.” [Online]. Available: https://ptolemy.berkeley.edu/projects/cps/

[8] T. Chuang, “Ransomware strikes CDOT for second time even as agency still recovering from first SamSam attack,” *The Denver Post*, Mar. 2018.

[9] “Security for Transit Systems Standards Program.” [Online]. Available: http://www.apta.com/resources/standards/security/Pages/default.aspx

[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,” 1666 K Street, NW, Washington, DC, 20006-1215, APTA-SS-CCS-RP-002-13, Jun. 2013.

[11] J. L. Western and B. Ran, “Information Technology in Transportation Key Issues and a Look Forward.”

[12] E. Fok, “Protecting Your Transportation Management Center,” *ITE Journal*, Feb. 2015.

[13] “Report Phishing Sites.” [Online]. Available: https://www.us-cert.gov/report-phishing

[14] “Ransomware and Recent Variants.” [Online]. Available: https://www.us-cert.gov/ncas/alerts/TA16-091A

[15] G. O’Gorman and G. McDonald, “Ransomware: A Growing Menace,” Symantec.

[16] M. Korolov, “93% of phishing emails are now ransomware,” Jun-2016. [Online]. Available: https://www.csoonline.com/article/3077434/security/93-of-phishing-emails-are-now-ransomware.html

[17] A. Zimba, Z. Wang, M. Mulenga, and N. H. Odongo, “Crypto Mining Attacks in Information Systems: An Emerging Threat to Cyber Security,” *Journal of Computer Information Systems*, vol. 0, no. 0, pp. 1–12, 2018 [Online]. Available: https://doi.org/10.1080/08874417.2018.1477076

[18] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, “DDoS in the IoT: Mirai and Other Botnets,” *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[19] 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

[20] 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/

[21] S. Barbeau and J. Begley, “SunRail Electronic Trip Planning Study Final Report,” USF Center for Urban Transportation Research, Mar. 2013.

[22] C. Brakewood and K. Watkins, “A literature review of the passenger benefits of real-time transit information,” *Transp. Rev.*, vol. 0, no. 0, pp. 1–30, 2018.

[23] “OneBusAway.” [Online]. Available: https://onebusaway.org/

[24] S. J. Barbeau and A. Antrim, “The Many Uses of GTFS Data – Opening the Door to Transit and Multimodal Applications.”

[25] “GTFS Static Overview | Static Transit | Google Developers.” [Online]. Available: https://developers.google.com/transit/gtfs/

[26] “Overview | Static Transit | Google Developers.” [Online]. Available: https://developers.google.com/transit/gtfs/reference/

[27] “OpenTripPlanner.” [Online]. Available: http://www.opentripplanner.org/

[28] S. Barbeau and J. Begley, *Web-based Trip Planner Options for Transit Agencies*. 2013.

[29] “OWASP Overview.” [Online]. Available: https://www.owasp.org/index.php/Main_Page

[30] K. Turner, “Google Maps: Goofs, Hacks And Losing Our Sense Of Direction,” Apr-2016. [Online]. Available: http://www.courant.com/consumer/hc-ls-tech-google-maps-errors-0410-20160411-story.html

[31] C. Payne, “On the security of open source software,” *Information Systems Journal*, vol. 12, no. 1, pp. 61–78, Feb. 2002.

[32] M. Mezghani, “Study on electronic ticketing in public transport (Final Report),” European Metropolitan Transport Authorities, May 2008.

[33] M. Puhe, M. Edelmann, and M. Reichenbach, “Integrated urban e-ticketing for public transport and touristic sites,” *Science and Technology Options Assessment*, 2014.

[34] 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*, 2015, pp. 1551–1556.

[35] R. Ryan, Z. Anderson, and A. Chiesa, *Anatomy of Subway Hack*. 2008.

[36] Z. Anderson, “Boston Subway MBTA Security Research.” [Online]. Available: http://web.mit.edu/zacka/www/mbta.html

[37] D. Surendran, “An Overview of Smart Card Security.” [Online]. Available: https://people.cs.uchicago.edu/ dinoj/smartcard/security.html

[38] J. Abbott, “Smart Cards: How Secure Are They?,” SANS Institute, Mar. 2002.

[39] H. J. Mahanta, A. K. Azad, and A. K. Khan, *Power analysis attack: A vulnerability to smart card security*. 2015.

[40] 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*, 2013, pp. 143–154.

[41] A.-R. Sadeghi, I. Visconti, and C. Wachsmann, *User Privacy in Transport Systems Based on RFID E-Tickets*. .

[42] “Bus Passes on Your Phone.” [Online]. Available: https://www.tokentransit.com/

[43] “QRcode.com | DENSO WAVE.” [Online]. Available: http://www.qrcode.com/en/

[44] E. Tavilla, “Transit Mobile Payments: Driving Consumer Experience and Adoption,” Federal Reserve Bank of Boston, Feb. 2015.

[45] P. Kieseberg *et al.*, “QR code security,” in *Proceedings of the 8th International Conference on Advances in Mobile Computing and Multimedia*, 2010, pp. 430–435.

[46] K. Conger, “Rare Malware Targeting Uber’s Android App Uncovered,” Jan-2018. [Online]. Available: https://gizmodo.com/rare-malware-targeting-ubers-android-app-uncovered-1821753862

[47] R. J. Baker, J. Chang, H. R. Smith, I. A. A. T. M. S. Committee, and I. A. A. P. T. S. Committee, *An Overview of Transit Signal Priority*. ITS America, 2002.

[48] J. A. Bonneson, S. R. Sunkari, M. P. Pratt, and Others, “Traffic signal operations handbook,” Texas Transportation Institute, Texas A & M University System, 2009.

[49] M. M. Dobersek, “An operational comparison of pre-time, semi-actuated, and fully actuated interconnected traffic control signal systems,” PhD Thesis, Marquette University, 1998.

[50] H. R. Smith, B. Hemily, and M. Ivanovic, *Transit Signal Priority (TSP): A Planning and Implementation Handbook*. ITS America, 2005.

[51] C.-F. Liao, “Simulation Study of a Bus Signal Priority Strategy Based on GPS/AVL and Wireless Communications,” 2006.

[52] 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.

[53] L. Tebow, “Choose Who Has Control of the Traffic Signals,” *IMSA Journal*, pp. 28–30, 2012.

[54] V. Bhide, Feb-2018.

[55] B. Ziegler, “Signal Cabinet Electronic Locks,” Apr-2016. [Online]. Available: https://www.mobotrex.com/2016/04/18/signal-cabinet-peace-mind/

[56] 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)*, San Diego, CA, 2014.

[57] C. Cerrudo, “Hacking US traffic control systems,” 2014.

[58] C. Cerrudo, “An Emerging US (and World) Threat: Cities Wide Open to Cyber Attacks,” Ioactive Labs, 2015.

[59] 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)*, 2016, pp. 130–135.

[60] 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, Piscataway, NJ, USA, 2016, pp. 16:1–16:10.

[61] K. Poulsen, “Traffic Hackers Hit Red Light,” *Wired*, Aug. 2005.

[62] C. Schweiger, “Real-Time Bus Arrival Information Systems,” TCRP, Jan. 2003.

[63] *Introduction to Variable Message Signs Student Handbook*. Washington State Department of Transportation, 2010.

[64] *Dynamic Message Signs (DMS)*. [Online]. Available: https://www.dot.state.oh.us/Divisions/Operations/Traffic/FAQs/Pages/DMS.aspx

[65] “Employ web-enabled variable message signs for your real-time conditional messaging needs,” Jan-2018. [Online]. Available: http://www.alltrafficsolutions.com/blog/employ-web-enabled-variable-message-signs-real-time-conditional-messaging-needs/

[66] K. P. Heaslip, M. Foruhandeh, and K. B. Kelarestaghi, *Transportation Cyber-Physical Security: Things We Should Know*. 2018.

[67] B. Wojdyla, “How To Hack An Electronic Road Sign,” Jan-2009. [Online]. Available: https://jalopnik.com/5141430/how-to-hack-an-electronic-road-sign

[68] B. Krebs, “They Hack Because They Can,” Jun-2014. [Online]. Available: https://krebsonsecurity.com/2014/06/they-hack-because-they-can/

[69] “Security Cameras / Security Systems Fact Sheet.” [Online]. Available: https://www.pcb.its.dot.gov/factsheets/security/sec_overview.aspx#page=common

[70] *CCTV Cameras in Transit Systems: Aiming to improve safety and security*. [Online]. Available: https://www.globalmasstransit.net/archive.php?id=16680

[71] T. R. Board, National Academies of Sciences, and Medicine, *Practices to Protect Bus Operators from Passenger Assault*. Washington, DC: The National Academies Press, 2011.

[72] American Public Transportation Association, “Selection of Cameras, Digital Recording Systems, Digital High-Speed Networks and Trainlines for Use in Transit-Related CCTV Systems,” 1666 K Street, NW, Washington, DC, 20006-1215, APTA IT-CCTV-RP-001-11, Jun. 2011.

[73] 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*, 2016, pp. 45–54.

[74] 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*, 2010, pp. 97–106.

[75] “Shodan.” [Online]. Available: https://www.shodan.io/

[76] 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*, Cham, 2013, pp. 390–393.

[77] 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*, 2010, pp. 209–222.

[78] A. Gupta and R. K. Jha, “Security threats of wireless networks: A survey,” in *International Conference on Computing, Communication Automation*, 2015, pp. 389–395.

[79] Transportation ResearchBoard and National Academies of Sciences, Engineering, and Medicine, *Computer-Aided Scheduling and Dispatch in Demand-Responsive Transit Services*. 2004.

[80] Transportation Research Board and National Academies of Sciences, Engineering, and Medicine, *AVL Systems for Bus Transit: Update*. 2008.

[81] S. Babcock, “City: Cyber attack against Baltimore’s 911 computer-aided dispatch system was ransomware,” Mar-2018. [Online]. Available: https://technical.ly/baltimore/2018/03/29/city-cyber-attack-baltimores-911-computer-aided-dispatch-system-ransomware/

[82] Transportation Research Board and National Academies of Sciences, Engineering, and Medicine, *Passenger Counting Systems*. Washington, DC: The National Academies Press, 2008.

[83] T. I. P. Program, “Intelligent Transportation Systems (ITS) Professional Capacity Building Program.” [Online]. Available: https://www.pcb.its.dot.gov/factsheets/apc/apc_overview.aspx#page=tech

[84] 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.

[85] “CV Pilot Deployment Program.” [Online]. Available: https://www.its.dot.gov/pilots/cv_pilot_apps.htm

[86] “Connected Vehicle Pilot Deployment Program.” [Online]. Available: https://www.its.dot.gov/pilots/index.htm

[87] “Wyoming DOT Connected Vehicle Pilot.” [Online]. Available: https://wydotcvp.wyoroad.info/

[88] “Connected Vehicle technology is coming to the streets of New York City!” [Online]. Available: https://cvp.nyc/

[89] “Tampa Connected Vehicle Pilot.” [Online]. Available: https://www.tampacvpilot.com/

[90] *Automated and Connected Vehicles*. [Online]. Available: http://autocaat.org/Technologies/Automated_and_Connected_Vehicles/

[91] “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.

[92] “IEEE 1609 - Family of Standards for Wireless Access in Vehicular Environments (WAVE) Fact Sheets.” [Online]. Available: https://www.standards.its.dot.gov/factsheets/factsheet/80

[93] “Bluetooth Technology Website.” [Online]. Available: https://www.bluetooth.com/

[94] J. B. Kenney, “Dedicated Short-Range Communications (DSRC) Standards in the United States,” *Proc. IEEE*, vol. 99, no. 7, pp. 1162–1182, Jul. 2011.

[95] L. Hausermann, “Connected car: all the vulnerabilities in one infographic,” Sep-2016. [Online]. Available: https://www.sentryo.net/infographic-vulnerabilities-connected-car/

[96] K. Koscher *et al.*, “Experimental Security Analysis of a Modern Automobile,” in *2010 IEEE Symposium on Security and Privacy*, 2010, pp. 447–462.

[97] S. Checkoway *et al.*, “Comprehensive experimental analyses of automotive attack surfaces,” in *Proceedings of the 20th USENIX conference on Security*, 2011, pp. 6–6.

[98] 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.

[99] 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.

[100] T. Hunt, "Controlling vehicle features of Nissan LEAFs across the globe via vulnerable APIs," Feb-2016. [Online]. Available: https://www.troyhunt.com/controlling-vehicle-features-of-nissan/

[101] *Automated Vehicle Research*. [Online]. Available: https://www.its.dot.gov/automated_vehicle/index.htm

[102] T. Litman, "Autonomous Vehicle Implementation Predictions: Implications for Transport Planning," Victoria Transport Policy Institute, Apr. 2018.

[103] *J3016A: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles*. 2016 [Online]. Available: https://www.sae.org/standards/content/j3016_201609

[104] L. Brooke, "U.S. DoT chooses SAE J3016 for vehicle-autonomy policy guidance," Sep-2016. [Online]. Available: http://articles.sae.org/15021/

[105] "Levels of Driving Automation Are Defined in New SAE International Standard J3016," SAE.

[106] 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.

[107] S. Riisgaard and M. R. Blas, "SLAM for Dummies: A Tutorial Approach to Simultaneous Localization and Mapping," MIT Open Courseware.

[108] T. B. Brown, D. Mané, A. Roy, M. Abadi, and J. Gilmer, "Adversarial Patch," Dec. 2017.

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

[110] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR," 2015.

[111] M. Harris, *Researcher Hacks Self-driving Car Sensors*. IEEE Spectrum, 2015 [Online]. Available: https://spectrum.ieee.org/cars-that-think/transportation/self-driving/researcher-hacks-selfdriving-car-sensors

[112] T. Simonite, "Self-Driving Cars' Spinning-Laser Problem," *MIT Technology Review*, Mar. 2017.

[113] R. N. Charette, *Commercial Drones and GPS Spoofers a Bad Mix*. IEEE Spectrum, 2012 [Online]. Available: https://spectrum.ieee.org/riskfactor/aerospace/aviation/commercial-drones-and-gps-spoofers-a-bad-mix