Understanding Security Issues in Vehicle Transportation Systems in a Holistic, Context-aware Manner

Anwesh Tuladhar
Department of Computer Science and Engineering
University of South Florida
Tampa, USA
atuladhar@mail.usf.edu

Xinming Ou
Department of Computer Science and Engineering
University of South Florida
Tampa, USA
xou@usf.edu

***Abstract*—Technology is revolutionizing vehicle transportation systems with the goal to improve efficiency, mobility, safety, and comfort. While there has been research looking into cyber security issues in transportation systems, such efforts are often fragmented targeting specific segments of the system, and lack a coherent framework that captures the overarching context. The vehicle transportation system is a complex ecosystem of diverse technologies, residing in myriad types of components dispersed over a wide geographic range. Understanding security issues in such systems requires capturing the many ways technologies in the ecosystem may interact. Systemizing security issues that may arise through these interactions will benefit not only the management and operation of such systems, but also the design process of future systems and system components, which are undergoing a rapid technological advancement in this domain. In this paper we provide such a systemization. The primary driving force of our effort is an in-depth, six-month embedding in a traffic management center (TMC) of a mid-size city in the U.S., where we gained first-hand knowledge of the inner workings of the vehicle transportation ecosystem. This effort involves interacting with people from multiple engineering disciplines including transportation, traffic engineering, computer and communications, and others. Although each of these fields have a unique role to play in this ecosystem, all of them play a part in security. One observation from our embedding in the TMC is the existence of silos of each discipline, making it difficult to understand and communicate the security impact one can have in the context of the whole transportation ecosystem. This echoes what we find in the relevant research literature, where in many cases security issues identified stem from assumptions made about other aspects of the ecosystem, regardless of whether such assumptions can hold or not. In our systematization approach we identify the key components, technologies, and stakeholders in the whole ecosystem, and that forms the basis of understanding attack scenarios and their mitigations. This methodology helps to put security analysis into the context of the transportation ecosystem and provides a common platform for communication to help breakdown the silos existing both in research and in practice.**

1. Introduction

Vehicle transportation infrastructure is undergoing fundamental changes with the converging of traditional closed systems and the Internet-driven new technologies to improve efficiency, mobility, safety, comfort, and convenience. It is a multi-disciplinary field with combined contributions from the civil & transportation engineering, traffic engineering, electrical engineering, communications engineering, and computer science and engineering. With rapid advancements in technology and improved connectivity, introduction of connected and autonomous vehicles is leading the technology-driven revolution of the transportation systems. The increased connectivity within and between vehicles, and between vehicles and the transportation infrastructure is driving the transformation at an accelerated pace. These advancements have made possible vast improvements and created an enormous market for rapid deployment of feature-rich vehicles and infrastructure equipment. Like in all domains, the dramatic increase in the use of technology and connectivity also opens up new threats from cyber attacks.

A significant challenge in understanding the cybersecurity risk in a system like vehicle transportation is that it requires the understanding of an ecosystem consisting of multiple non-trivial physical systems as well as the various stake holders involved in their design and operation. A vehicle is made by manufacturers and driven by humans (and/or computer programs) on the road, whose road-side infrastructures are built and maintained by public entities such as municipal and state governments. These days both cars and infrastructures can communicate with third-party vendors in the cloud, providing/receiving information that impact their operations. With the influx of technology in every component and increase in the connectivity between them, the influence of each component on the other is greater than ever before. The dependencies thus created means that security vulnerabilities are no longer isolated to a particular component, thus making it much harder to contemplate without understanding the whole transportation ecosystem. It is not surprising that security risks in such a complex and inter-connected system can be both numerous and nuanced. Existing work in vehicle transportation cybersecurity has tended to focus on parts of the overall ecosystem, e.g., vehicles, traffic lights, etc [1]–[4]. While (not surprisingly) many attack avenues were discovered, it is not often clear why these problems are there in the first place (beyond blaming users or developers), how to prevent them from being introduced, and how to mitigate them through cost-effective methods if elimination is not a practical option. To answer these questions a holistic framework to systematize cybersecurity issues in the vehicle transportation ecosystem is beneficial. With such a framework one can have a better understanding of the potential vulnerabilities when designing a system, have a quicker grasp of the risk when operating on the systems, and have a more meaningful perspectives on how to mitigate them in reality.

The intricacy of cybersecurity issues in vehicle transportation system is illustrated in the work of Chen et al. [4]. In this case, although the component itself was designed with security in mind, exploitation of another component in the ecosystem led to an unexpected vulnerability. In particular, Intelligent Traffic Signal System (I-SIG) is a USDOT sponsored Connected Vehicle (CV) transportation system developed and deployed for testing in three major cities in the U.S. I-SIG uses real-time vehicle trajectory data to intelligently control the traffic signal timing with the goal of reducing vehicle delay. Chen et al. showed that the trade-offs made in the implementation of the algorithm used in this system made it vulnerable to data-spoofing attacks, which leads to far worse congestion than would be caused without using the system at all. This vulnerability was exploited by infiltrating the trusted computing base of the roadside component through the vulnerability in the vehicle component. Better knowledge of security in the context of the whole ecosystem would be valuable to help identify and prevent such security issues, especially when decisions regarding trade-offs have to be made.

We conducted a six-month embedding in a traffic management center (TMC) run by a medium-size U.S. city, during which we observed the TMC operations on a daily basis. We also talked to both operators and management to further understand the transportation ecosystem at large. We found that the multi-disciplinary nature of the transportation ecosystem poses another challenge in understanding the security issues. The lack of a holistic framework presented a major hurdle in communication. Different disciplines involved tend to view this ecosystem from their own unique lenses and at different levels of detail, creating silos of knowledge within operations, research, and development. This lack of a common perspective makes communication and information sharing difficult. The first step to better identify security risks and evaluate different approaches is to establish a common understanding of the different security challenges and place them in the context of the whole ecosystem.

Based on our observations in the TMC and study of the existing literature, we propose a systematization approach to providing a holistic context to evaluate security issues in the vehicle transportation ecosystem, and a common platform to share knowledge between the diverse disciplines within the ecosystem. Our systematization makes the following contributions.

- We propose a two-tiered framework to study and evaluate the security posture of the transportation system as a whole. This approach breaks down the transportation ecosystem along two dimensions: components and enabling technologies. We then utilize this framework to identify threats and extract common attack categories. We also identify the main stakeholders and their responsibilities for prevention and mitigation.
- We present our observations from the embedding in the TMC which led to this framework.
- We put existing transportation security research literature within our framework to understand existing threats, attack techniques, mitigations, and the stakeholders responsible for prevention and mitigation. We use this process to identify reasons for the discovered vulnerabilities and evaluate the suggested countermeasures where possible.

The rest of the paper is organized as follows. In section 2 we describe our fieldwork effort in the TMC. In section 3 we present the overview of the transportation ecosystem and introduce our systematization approach. Section 4 presents the threat model. In section 5 we apply the systematization approach to present the findings from our field work along with relevant literature. In section 6 we discuss our findings and how our systematization can be used for future work. We review the related work in section 7, and conclude in section 8.

2. Fieldwork in TMC

The center of operations for vehicle transportation is the transportation management center, or TMC. It is typically operated by local and state authorities and covers a specific geographic ranges based on its jurisdiction. TMC provides a direct lens into understanding the domain knowledge needed to systematize security issues in the overall transportation ecosystem. It is for this reason that we conducted an in-depth fieldwork where researchers were embedded in a TMC run by a medium-size U.S. city, with the goal of understanding the basics of traffic engineering, city-scale traffic management, and the cybersecurity challenges faced by the transportation ecosystem. Researchers spent a few days every week, depending on the schedule of the TMC operators, for a duration of six months, observing daily operational activities and participating where possible.

2.1. Background

The TMC operates all the traffic signals with the goal of optimizing the travel time throughout the city. A combination of fiber optics cables, twisted copper pair, and wireless communication networks connect hundreds of traffic cabinets to the central TMC. The TMC houses dedicated servers to run software applications used by the traffic engineers to monitor real-time traffic and operate the signal cabinets. It uses an in-house test cabinet to train new employees and test any updated signal timings. At the beginning, we went through a basic traffic engineering training followed by training on various tools used during daily operations. After this, we participated in daily operations, during which we collected data in the form of fieldnotes. Our observations involved creating/updating signal timing, operation of reversible lane, monitoring and analyzing signal timing reports and incident response (failures, accidents, and client complaints). We maintained the fieldnote to record the details of our observation of the daily work, the systems used in the various tasks, and our interaction with the civil and traffic engineers in the TMC. The fieldnote data is then analyzed by the

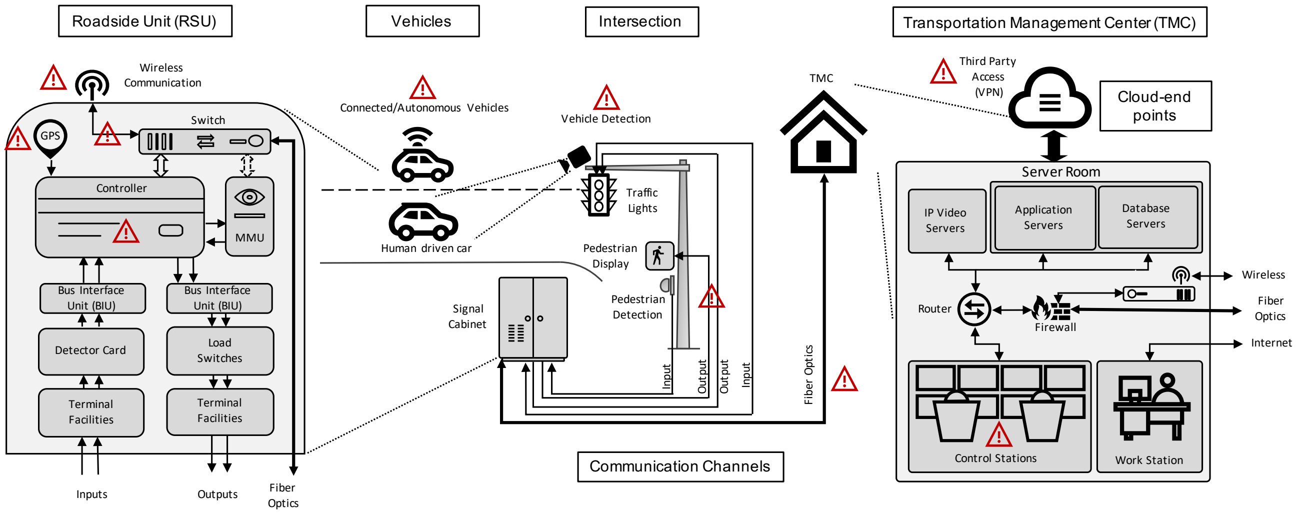


Figure 1. Overview of the Transportation System. The figure shows all the components of the transportation ecosystem and it's enabling technologies.

research team, the outcome of which serves the basis for the systematization we present in this paper.

2.2. Challenges

We encountered/observed some substantial challenges during our fieldwork. First, communication was a major challenge as field operators, computer, civil, and traffic engineers were all working in the same environment. The perspective of the transportation infrastructure is different for each individual. Take for example a discussion on signal cabinet and security. The field operator focuses on how a person can access the signal cabinet; the traffic engineer focuses on the potential undesired conditions that may arise due to changes in the signal timings; the computer engineer focuses on the signal controller, software running on it, and network connection; and the civil engineer focuses on the planning aspect and the impact it may have on the entire road network. In this case, the field operator asked "can attackers physically access the signal cabinets?" The traffic engineer asked "what damage can attackers cause if given access to signal cabinets?" The computer engineer asked "can attackers gain access to devices in signal cabinets?" And the civil engineer asked "what can be the impact of such malicious actions?" All these points-of-view are valid and important to understand in order to perform a security risk analysis of the transportation system. Working on a real system with potential for physical consequences in a live environment also meant a lot of restrictions in-terms of investigation and experimentation. For this reason we could only perform a non-invasive security evaluation, the knowledge we gained from which was valuable for us to come up with this systematization approach as well as to gain insights on prevalent security practices and their status.

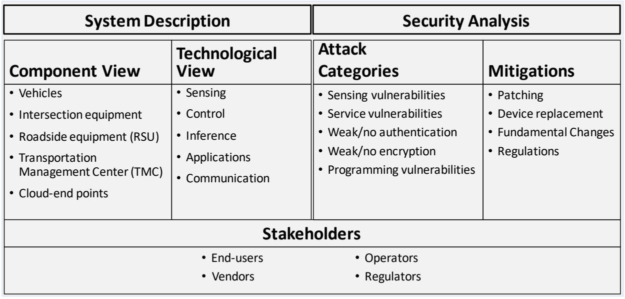
3. Transportation Ecosystem Overview

The transportation ecosystem can be viewed as in Fig. 1. The main component is the millions of vehicles on the road, including specialized public transit and emergency response vehicles. Vehicles dominate the transportation ecosystem in terms of both the number and the technological advancement and research. Vehicles have evolved from traditional mechanical systems to complex computing-mechanical systems consisting of hundreds of sensors, dozens of control devices from electronic control units, or ECUs, to infotainment systems, and now to connected and automated vehicles (CAVs) capable of communicating amongst each other and with the infrastructure and cloud services that provides large-scale data analytics and inference capabilities. Dozens of vendors contribute to the manufacturing and development of vehicles, driven by the demands from end-user customers.

The vehicles, end-users, and the transportation infrastructure interface with each other mainly through the devices on the road intersections such as vehicle detectors, traffic lights, and dynamic message signs (DMS). This interface capability is extended by the use of mobile devices and various applications and further improved by the introduction of connected vehicles. The input interface for the transportation system are the sensing technologies, feeding data into the roadside component. Based on these inputs, the roadside equipment in turn control the output interfaces.

In order to maintain efficient and safe traffic flow throughout, the roadside equipment are connected to each other through various communication channels (fiber optics, wireless, etc.) and to the TMC. Daily monitoring and efficient operation of the transportation system is the responsibility of the TMC operators. TMC may host several servers supporting the operations of the roadside units and various applications utilized by the operators to perform their daily tasks. They might also be connected to other third-party cloud services through virtual private networks (VPNs).

Transportation system is a critical infrastructure of the modern society with practically everyone utilizing its services. Hence, regulators at various levels enforce standards and rules to ensure safe and secure functioning of this system. This includes standards and rules imposed on the end-users (traffic laws), operators (procedures to follow) and vendors (types of technology to use and standards to



System Description		Security Analysis	
Component View	Technological View	Attack Categories	Mitigations
• Vehicles • Intersection equipment • Roadside equipment (RSU) • Transportation Management Center (TMC) • Cloud-end points	• Sensing • Control • Inference • Applications • Communication	• Sensing vulnerabilities • Service vulnerabilities • Weak/no authentication • Weak/no encryption • Programming vulnerabilities	• Patching • Device replacement • Fundamental Changes • Regulations
Stakeholders			
• End-users • Vendors	• Operators • Regulators		

Figure 2. Systematization Approach. *System description*: The transportation ecosystem is separated into components which are described using the abstraction of enabling technologies in order to capture a holistic point-of-view without having to know the implementation details. *Security analysis*: Identified common attack categories and possible mitigation strategies. *Stakeholders*: The parties involved in maintaining a safe and secure transportation ecosystem.

maintain).

3.1. Systematization Approach

The transportation system is a technological ecosystem: a complex interconnected network of multiple components interacting with each other, utilizing various types of independent and interdependent technologies which are influenced by different stakeholders at various stages of development. We propose a systematization approach to provide a holistic context for the transportation ecosystem. The holistic view makes it easier to capture the interactions between the elements of the ecosystem and provides a coherent framework to evaluate the security properties of the ecosystem.

Our systematization utilizes a two-dimensional view of the transportation ecosystem to facilitate discussion and understanding. We call the first dimension *component view*, whereby we categorize the transportation ecosystem into *components*, providing the logical separation of the various aspects of the ecosystem. The second dimension is called *technological view*, whereby we identify the key classes of *technologies* that enable the functionality of these components. To aid security analysis, we identify key security issues faced by these classes of technologies, common mitigation approaches used, and the stakeholders involved. This approach is illustrated in Fig. 2.

We emphasize that both dimensions are important in our systematization. The logical dimension provides the context in which a component resides in the overall transportation ecosystem, thus the same type of security issues will have varying implications based on the different contexts; the functional dimension captures the similarities among the possible attacks on the same type of technologies, despite the fact that the same type of technology could be used in different components, and thus under different contexts and with different security impacts. We believe this two-tier approach to look at security issues will allow one to both generalize those problems based on their similarities, and at the same time not lose the intricacy and diversity of possible attacks when it comes to the interactions among components in the overall system. We describe these two views of the transportation system below in the next two sub sections.

3.2. Component View

Based on the roles they play, the transportation ecosystem can be divided into the following components.

3.2.1. Vehicle. Vehicles have traditionally only been "users" of the transportation infrastructure. With CAV technologies, they form an integral part of the transportation ecosystem. The connected infrastructure relies on trajectory data collected by sensors in each vehicle to optimize traffic flow. Vehicles, in turn, rely on the infrastructure for safety advisory and navigation.

3.2.2. Intersection. Transportation infrastructure and vehicles/pedestrians exchange information at the intersections and hence serve as the input/output interface. Infrastructure receives input from vehicles/pedestrians using detection systems, vehicle-to-infrastructure (V2I) communication, video surveillance, toll gantries, etc. Information is conveyed back to vehicles/pedestrians using traffic lights, dynamic message signs (DMS), infrastructure-to-vehicle communication, and mobile applications.

3.2.3. Roadside Unit (RSU). RSU hosts devices responsible for safe and efficient operation of the intersection. These include signal controllers that manage the signal timings, Malfunction Management Unit (MMU) which ensures safety conditions, and network equipment for communicating with other intersections and the TMC.

3.2.4. Transportation Management Center (TMC). TMC is a regional hub that serves as the mission control for urban transportation and highway networks. TMC operators collect real-time data and combine with other operational and control data in order to monitor roadways, proactively optimize traffic conditions, provide incident management, dissipate traveler information and coordinate with other authorities for daily traffic, special events, accidents and emergencies [5]–[7].

3.2.5. Cloud end-point. Modern systems require heavy computational capabilities and rely on cloud-based infrastructure to host them. Existing usage of such services include vehicle diagnostics, real-time navigation, fleet management, and data-driven traffic monitoring services, with more such services emerging.

3.3. Technological View

Each component relies upon one or more technologies to function. In many cases, similar functionality is required across different components. Hence, based on the function provided, we group them into different classes of technologies: sensing, control, inference, application, and communication. Examining the transportation ecosystem based on these abstractions of technologies provides an opportunity to understand common attack patterns across components. This provides the basis for cybersecurity discussions amongst experts from different domains, that would otherwise be inhibited by technical details involving the differing domains. In addition, contextualization of those technologies within the transportation ecosystem aids in identifying attack goals, attack paths, and impacts that would otherwise be overlooked. An example of this is further discussed in section 5.3.3. We describe each of these technologies below.

3.3.1. Sensing. The class of technologies used to detect its surrounding environment. This includes traditional sensor devices as well as communication-based sensing such as vehicle-to-infrastructure (V2I) devices.

3.3.2. Control. Technologies operating actuators. Additionally, indirect form of control through informing end-users to take certain actions.

3.3.3. Inference. Technologies used to extract insights from data that are collected through both sensing and communication.

3.3.4. Applications. Mobile, web, and desktop applications used throughout the vehicle transportation ecosystem.

3.3.5. Communication. Communication and networking technologies.

3.4. Stakeholders Involved

The transportation ecosystem is influenced by a number of stakeholders at various stages, each with their own responsibilities. We categorize the stakeholders as follows.

1) End-users: the public using the roadways and the transportation technologies available to them.
2) Vendors: software and hardware providers for the transportation system.
3) Operators: individuals responsible for daily operation and maintenance of the transportation system.
4) Regulators: regulatory authorities and policy makers.

4. Threat Model

With the proliferation of technology usage, transportation ecosystem is an attractive target for cyber attacks. On a large scale, cyber attacks can lead to extreme congestion condition and safety hazard for the travelers. Congestion is not simply an annoyance for the public in terms of time loss but also has massive impact on daily operations of the entire city, finances, and environment as well. Projecting into the future, with the rapid development and deployment of connected technologies, additional assets could become targets of cyber attacks, especially the massive amounts of data that can be misused by attackers for financial gain or for privacy violations and tracking. On a small scale, attackers may target the transportation system for personal gain such as fast tracking through traffic lights. Increased reliance on data for traffic management can also open opportunities for malicious actors to divert traffic away from their competing businesses. This type of problems have already been seen through fake review attacks [8]. The rate of change of technology in transportation is accelerating and if no adequate attention is paid to cybersecurity, transportation system is likely to be easy targets for cyber criminals.

5. Systematization of Knowledge

In this section, we apply our approach to systematize the findings from the fieldwork in the TMC along with the relevant literature. We observe that natures of cyber attacks are driven by the technologies involved. As such, in our systemization of security issues facing transportation infrastructure, we start from discussing common attack patterns impacting the various enabling technologies as described in section 3.3. We then explain those attacks in the context of the various components in the transportation system. The reader can see that although attacks may happen at different components in the overall transportation system, the same patterns are often observed involving the same technologies. What differs is the impact the attack may have, and what mitigation methods are effective.

5.1. Attacks on Sensing

5.1.1. Types of Sensing Technologies Used in the Transportation System. Adoption of sensing technologies is most pronounced in vehicles and intersections. Sensing in the *intersections* is primarily for detecting vehicles and pedestrians to control signal timing. Data collected from these sensors are also aggregated to measure volume, speed, and travel time which are further analyzed, the insights from which can inform system-wide signal timing performance improvement [9]. Other sensors include special devices installed for detecting radio waves emitted from transit buses, trains, and emergency vehicles to give them priority in passing. Automatic vehicle identification systems are used for toll collection, red light violation, etc. There are also sensors for highway ramp metering, measuring truck weight, and the increasing trend of sensors for monitoring the surrounding environment such as air quality. Sensing in the *roadside unit (RSU)* is primarily used for time synchronization. It is necessary for important tasks such as switching of signal timing plans based on time-of-day, and coordinating signal timing across multiple intersections along a corridor to achieve continuous traffic flow [10]. Since the transportation networks at this time are “mostly” isolated from the internet, RSUs typically achieve time synchronization using microwave links or a GPS at a regular pre-set time [11].

5.1.2. Mechanisms for Sensing. We found a number of means to sensing for transportation systems: a) specialized technologies: e.g., inductive loop, magnetometer, electromagnet sensors, infrared sensors, GPS, microwave radar, etc. b) communication-based detection: e.g., ISM band radios (900Mhz/4.9Ghz/5.8 GHz) or advanced vehicle-to-infrastructure (V2I) communication. c) video-based detection: e.g., video cameras capture and process images and convert it into traffic data (vehicle detection/identification). The deployment of these technologies may also involve additional communication technologies to transmit the captured data to other components.

5.1.3. Attack Categories. Regardless of the concrete implementation of these sensing technologies, the goals of the adversary are: a) to cause erroneous readings, b) to disrupt the detection (Denial of service (DoS)/jamming).

Adversaries can achieve these goals by exploiting different *sensing vulnerabilities*:

Pre-acquisition Attack. For this attack we mean the adversary deliberately forge/alter/introduce data/signals the sensors rely upon, leading to erroneous readings, malfunction, or jamming. This is most pronounced for communication-based detection. Attacks include *capture* (intercept a message/signal), *replay*, *delay*, *signal forgery*, and jamming. Sometimes it can also be achieved by controlling the source of the data/signal. One example such attacks is demonstrated by Chen et al. [4], who demonstrated a practical pre-acquisition attack on an Intelligent Traffic Signal System (I-SIG) by sending fake vehicle trajectory data into the infrastructure. Such messages sent from V2I are normally hard to tamper with given authentication methods applied. This attack bypasses the security mechanism of I-SIG (security credential management system (SCMS) [12]) by compromising an authenticated data transmitter (i.e. the vehicle) and fools the sensor into accepting false data. As discussed in section 1, this example shows the need for a holistic view of the transportation ecosystem to evaluate the security properties across multiple components. For the future, connected vehicle applications in RSU's could rely on GPS data to validate incoming V2I data. In such scenarios, known security vulnerabilities in GPS leading to incorrect navigation [13], [14], and replay, data spoofing and jamming attacks against GPS [15]–[17] poses threats which must be accounted for during design and security analysis. Yan et al. [18] demonstrated another type of pre-acquisition attack that results in jamming. One such attack is against millimeter-wave (MMW) radars used in Tesla cars, and the other is against video-based vehicle detection vulnerable to malicious light sources. Both attacks lead to existing vehicles not being detected (*blinding attacks*). For MMW, electromagnetic waves in the same frequency band as the sensors (76 - 77 GHz) flood the receiver, whereas in the video-based attack, LED and visible laser light sources are used to flood the camera. Petit et al. [19] additionally showed erratic detection by cameras by using bursts of light to confuse the automatic exposure control of the camera. While these works are focused on sensors on vehicles, similar attacks can be effective for sensors used in intersections.

Attack on Sensing Device. The sensing device can be directly manipulated with physical or remote access. This can lead to miscalibration that cause erroneous readings, data injection/rejection, or damage the device completely. During our embedding in the TMC, we were able to cause erroneous time reading on a test signal controller by short-circuiting two pins on the GPS, thereby sending a signal to reset the controller's local clock to the programmed reference time. This can greatly impact the traffic flow and at the same time do not trigger any faults or alerts. While in our experiments we do have physical access to the RSU, the victim devices can also be accessed from close proximity, or even remotely through the network as discussed in section 5.5. With such access, adversaries can mis-calibrate sensors, install malicious firmware, or gain access to other devices that trust it. With the rapid increase in use of technologies in transportation, it is becoming increasingly likely that sensing devices can be compromised remotely.

Post-acquisition Attack. In cases where sensed data need to be communicated to remote entities, attacks can be launched against the communication channel. These attacks are facilitated by weaknesses on the receiving end. Cerrudo [2] found that the access point that received data from in-pavement wireless vehicle detectors built by Sensys Networks [20] did not require any authentication, allowing false data injection attacks. Similarly, cameras send video to cloud services that perform inference to extract traffic flow data. Obermaier et al. [21] found that weak authentication in surveillance cameras allowed the adversaries to impersonate as the camera to the cloud service and trigger motion detection events, inject forged video streams, or deny the camera of the cloud service completely (DoS attack).

5.1.4. Impacts of Attacks on Sensing.

Since sensed data are used in inference algorithms to control the transportation infrastructure, successful attacks on sensing can cause undesirable impact in terms of traffic flow and safety. We give a few examples below through our embedding in TMC and from the published literature.

Through conversations with TMC engineers, we learned that incorrect sensing data are already causing problems in the transportation system. These are caused by malfunctions, but deliberate attacks can achieve the same effect.

One such scenario is pedestrian button being stuck in the ON position, which is equivalent to producing a fake sensing data on a non-existing pedestrian. The maximum impact occurs at intersections between a major corridor and a rarely used side-street activated only on vehicle/pedestrian detection. This causes unnecessary red lights on the main corridor while the side street is always serviced even when no vehicles/pedestrians are present.

We encountered another example when dealing with a public complaint incident. The complaint reported that a particular intersection was skipping the left turn green phase even when vehicles were present in the lane during certain evening time windows. On observing the live signal timing during the complaint time interval, the left turn green phase was indeed skipped. When investigating the incident, we verified the signal timings to be as expected and didn't find any issues which would suggest cyber tampering of any kind. On further discussion, the reason turned out to be much simpler: the skipped phase was on the east-west corridor of an intersection using video detection which suffered from a sun-glare at evening time causing missed detections. The pre-acquisition attack discussed earlier by Yan et al. [18] could have achieved the same effect.

As can be seen, the impact in the second case is more apparent than that in the first, as expected signal is not provided. A temporary mitigation strategy is to update the controller settings to always place a call on the left turn lane during that time which essentially converts it into the less efficient scenario in the first case – In the first case the impacts are longer term and harder to observe as operators have to analyze travel time data to observe sub-optimal traffic conditions.

Ernst et al. [11], using simulation, evaluate the impact of destabilizing time synchronization in a six intersection coordinated corridor and find that travel time can grow linearly with time causing significant queuing. The experiment we discussed earlier regarding attack on sensing device could be used to achieve this undesirable outcome.

5.1.5. Possible Mitigations. Mitigating attacks on sensing comes with various challenges due to natures of attacks, financial burdens, and the large number of legacy systems. Pre-acquisition attacks are hard to prevent since they happen outside of the system's boundary. Improving data validation and noise reduction in the sensing technology could thwart some of these attacks [22], [23], but may not always be effective. Use of redundant sensing devices or technologies can also make it harder for the adversaries [24], but comes with financial cost in terms of additional devices and computational cost required to merge multiple data sources.

For attacks on devices, the devices can be hardened using existing security measures. For instance, the security issues disclosed by Cerrudo [2] are not new to the security community and can be fixed by applying textbook security measures. But this work exposes the real world consequence of deploying insecure devices and the impracticality of post deployment retrofitting in a large scale: 1) more than 200,000 devices are deployed throughout many countries; 2) The issue is not easily solvable by patching since communication is not encrypted, and updates are not signed, making the patching process itself an attack vector; 3) The only real solution becomes massive device replacement, complicated by the fact that these devices are buried under the pavement and meant to operate for tens of years. It also requires coordination with other agencies that deal with the pavement, and the resulting costs can be prohibitive for the stake holders.

5.2. Attacks on Control

5.2.1. Types of Control Technologies Used in the Transportation System. Control technologies are most prominent in vehicles with hundreds of electronic control units (ECU) digesting different sensing data and user input to control the vehicle. In intersections, traffic signals are controlled by devices in RSU based on sensed objects on the road, signal timing programs, and in some cases insights from inference technologies.

5.2.2. Mechanisms for Control. The control function is vastly different for vehicles and the remaining transportation components. ECUs control all aspects of a vehicle's movement, whereas in the transportation infrastructure, control technologies mainly direct traffic flow. Here we focus on the transportation infrastructure as vehicles have been well studied.

The transportation infrastructure controls traffic flow by sending various types of directives to vehicles/pedestrians: a) visual-based: traffic signals and dynamic message signs (DMS); b) communication-based: infrastructure-to-vehicle (I2V) communication; c) cloud-based: devices (embedded in vehicles or carried by humans) receive directives through the cloud. Regardless of the method of delivery, the core logic driving these output interfaces are implemented by control technologies either housed on-board like in DMS and RSU, or hosted on the cloud endpoints. They perform the following functions: a) actuate visual interfaces: DMS controller or mobile devices; b) implement signal timing: signal controller which implements the core traffic engineering logic; c) conflict monitoring: typically performed by specialized devices such as Malfunction Management Unit (MMU) or Cabinet Monitor Unit (CMU). They check for and prohibit the creation of unsafe conditions such as conflicting greens or violation of minimum red and yellow times. When such conditions are detected, the intersection is turned into all-way flashing red. d) interfacing with I/O connections: e.g., Serial Interface Unit or Bus interface Unit (BIU) which converts the I/O signals to the 24V synchronous data link control (SDLC) serial bus [25].

5.2.3. Attack Categories. Despite the myriad types of controls discussed above, control technologies always include a computing component that converts input signals to output actuation actions. These days the computing component is typically general-purpose computers with standard processors and Linux based operating systems [26]. Hence they are attractive targets for adversaries. By launching common cyber attacks, adversaries can gain control of the system or use it to infiltrate into other parts of the ecosystem. These devices have different ways of receiving input data from users, operators, or other devices through a communication channel. These are: i) Direct access: e.g., front panel of the device or upload from external storage (data key or USB sticks); ii) Proximity access: e.g., through local communication channels like WiFi using mobile or desktop applications, or from other devices communication through a local network; iii) Remote access: e.g., through the wide area networks or internet. Vehicles have been shown to be hacked using all of these accesses [27]–[31] and are not discussed further here.

Attack through Direct Access. Directly accessing the devices on the roadside exposes the adversary the threat of being caught, but such incidents have occured in the past. Typically, control panels and RSUs are protected by standardized locks (Corbin style with #2 keys), keys to which are readily available for purchase [32]. Once the control interface is accessed, there is lack of adequate protection against accessing and manipulating the software, with the most common issue being the lack of proper authentication. During our embedding in the TMC, we found that although signal controllers provide password protection and access control capabilities, they are not utilized in practice as different field operators work on them and managing individual credentials is cumbersome for daily operations. Even when used, default settings are never updated as found in RSUs [3] and in DMS signs [33]. Control panels of DMS signs have been broken into multiple times and messages successfully altered, with adversaries preferring to display amusing messages [34]. These DMS hacks only required layman knowledge with most simply exploiting the use of default credentials to update the messages displayed [33], [35]–[38]. Even with complex passwords, some DMS devices expose vulnerable password reset service without having to authenticate first.

With physical access to the RSU, it is trivial to send the intersection into flashing red state which is safe but inefficient. During our embedding, we were able to demonstrate such attacks by removing a load switch, or changing signal timings to trigger conflicting phases so that the MMU triggers flashing red. The safety impact of attacks on signal controllers are largely limited by the MMU/CMU which serves as a fail-safe unit. If the controller violates the basic safety conditions: minimum yellow time, minimum all red time, and no conflicting greens, MMU/CMU sends the intersection into conflict flash (all way stop), a safe state. The conflict status is identified through hard-wired programming card [39] or a serial memory key (datakey) [40]. However, with the knowledge of how the permissive states are defined in MMU/CMU, adversaries who can physically tamper with the unit can modify or replace it so that unsafe conditions would be allowed. This, combined with attacks on controls to create an actual unsafe signal scenario (e.g., conflicting greens), would result in catastrophic conditions.

Attack through Proximity and Remote Access. Attacks on controllers through proximity and remote access requires first gaining access to the communication network in use, which is covered in section 5.5. Once on the network, adversaries can look to exploit vulnerabilities commonly found in computing systems. For controllers used in transportation infrastructures, there are a number of security issues that are commonly found in these types of embedded or internet-of-things (IoT) devices, such as no/weak authentication and vulnerable services. DMS devices are reported to expose vulnerable services like open telnet ports, publicly accessible web-interfaces, and use of older Simple Network Management Protocols (SNMP) which are known to have security issues [33], [35]–[38]. RSU devices face similar challenges as study by Ghena et al. [3] and Zhang et al. [41] showed. They include: i) weak authentication: default and hardcoded credentials; ii) vulnerable services: exposed SSH, FTP and telnet services, remote login (rlogin), remote task management service, and debug service using Wind river DeBug protocol (WBD) – all could be exploited to gain access to the signal controller devices. On our inspection of RSU signal controllers by Econolite, we discovered vulnerable SSH service setup that uses default user name and password with root access. Using this we could trigger system reboots or modify/remove essential programs.

Although MMU/CMU maintains safe conditions which requires physical tampering for complete bypass, unsafe conditions can still be created by pushing the signal timing to the edge of conflict condition. During our embedding, we were able to program a signal timing with minimal green light time of one second without triggering the MMU as it only checks for minimum all red and yellow phases and has no restriction for the green phase. By minimizing all three phases we obtained flickering greens, which at the very least, can lead to confusion and annoyance to the public at intersections with low speed limit but may lead to fatal accidents when the speed limits are higher and the vehicles are unable to stop in time. Independently, Ning et al. [42] achieved a stronger attack on MMU/CMU by carefully timing the conflicting greens down to 200ms, which is the transient time required to trigger a conflict state. This results in a flickering green and solid green on two conflicting routes, highly likely to lead to severe crashes in the intersection. These results show that remote attacks can drive intersections into unsafe signal conditions, even with MMU/CMU present as the final line of defense.

5.2.4. Impacts of Attacks on Control.

With access to control devices through any of the above means, adversaries can manipulate it with malicious intent and the outcome depends on the function of the device.

Outcomes of attacking visual interfaces can be: i) Distractions; ii) Safety issues due to incorrect information (traffic directives or speed advisories); iii) Further compromise of the transportation infrastructure: some DMS devices are connected to the transportation network, in which case it may be used as pivots into the infrastructure. DMS is extensively utilized to deliver advisory information to road users such as real-time traffic conditions, variable speed limits, weather conditions, travel times, and optional routes. Studies have shown that the credibility of DMS is important to achieve efficient operations as well as ensure safety of workers with automated work zone information systems (AWIS) [43]–[45]. Hence even distracting messages can have long-term impact because of lack of trust in the system and future ignorance of important safety messages. Malicious misinformation are even more dangerous as it can cause unsafe road conditions, traffic diversions, and general degradation of traffic performance.

Outcomes of attacking signal controllers includes: i) Disabling traffic signal; ii) Inefficient or unsafe signal timing; iii) Further compromise of the transportation infrastructure. iv) Others, e.g., attacking controls can disrupt time synchronization across RSUs, as the attacks from section 5.1.3 can do. Inefficient signal timing is a concern as it has direct impact of increased delay, but also has environmental and financial impacts with increased emission and fuel consumption [46]–[48]. The flickering green attack is the most worrisome as it violates the safety condition of an intersection and can lead to accidents.

5.2.5. Possible Mitigations.

For attacks that require direct physical access, use of separate locks for each cabinet provides stronger physical security and utilizing strong user name and passwords on the devices can remedy most attacks. But this may not be applicable in practice as it is infeasible for field workers to carry around hundreds of keys and remember so many passwords. Use of RFID-based locks might be another solution but requires updating hundreds of cabinets and is a financial burden for many municipalities. Apart from that, we also have to account for extreme cases such as power outage due to unforeseen circumstances in which case physical keys might be preferred.

Mitigation of remote attacks is possible (in theory) simply by following best practices. Disabling unnecessary vulnerable services, avoiding use of hard-coded or weak authentication mechanisms, using virtual private network (VPN), and minimizing network exposure in general should harden the security posture of the transportation infrastructure [3], [37]. These are neither new issues nor new mitigation strategies but are still present in real world due to various reasons. Some of them include the ignorance of the role of these technologies in the context of the ecosystem, over reliance on the closed nature of these systems (until now), and the perception that certain security measures are not suitable or applicable here. These challenges demonstrate the utility of a systematic framework for understanding security issues within a holistic context of the transportation ecosystem.

5.3. Inference Technologies

5.3.1. Inference Technologies Used in the Transportation System. Data-driven approaches are used throughout the transportation ecosystem to inform control technologies, and provide insights to operators. Telemetry data from dozens of sensors in vehicles are utilized for fleet management, route optimization, and predictive vehicle diagnostics [49]. RSUs utilize real-time streams of trajectory data collected from V2I sensors to generate optimal local signal timing plans. In TMC, data collected from various sensors are aggregated and analyzed to evaluate vehicle counts, throughput, travel times, and traffic trends to further improve the system-wide performances. Data sharing agreements between the TMCs/end-users and third parties also facilitates commercial applications for end-users and operators. Several real-time traffic signal prediction and advisory applications have been developed such as GreenDrive [50] and SignalGuru [51]. Mobile applications such as Connected Signals' Enlighten [52] provides red light countdowns and green-wave speed[1] advisories of multiple signals ahead to the driver based on inferences from predictive models [53], [54]. Waycare [55] combines data from multiple sources to provide real-time traffic monitoring with predictions of future congestion and potential accident risk areas. Aggregate information such as live traffic, accident locations, speed traps, and speed limits are also provided by applications such as Google Maps and Waze.

5.3.2. Mechanisms of Inference. Inference technologies derive insights from both online real-time data, and offline historical data. One example of the former is Connected vehicle (CV) based Intelligent Traffic Signal System (I-SIG), which calculates optimal signal timings at intersections in real-time based on trajectory data collected by V2I sensors at the intersections. Example in the offline scenario include inference systems deployed at TMC that produce aggregate information from multiple sources to produce insights for operators to use for traffic monitoring, incidence response, and system-wide planning [55]–[58].

5.3.3. Attack Categories. Inference technologies may be housed in the RSU, TMC, or cloud-endpoints, each presenting different security challenges. Nonetheless, we find the following attacker goals to be applicable to all scenarios: a) to influence the insights extracted; b) to force real-time prediction to miss deadlines so rendering them useless; c) to disable the system altogether. Adversaries can achieve these goals through malicious input data, or through devices on which the inference systems are running. The attacks can be: i) direct: data injection through the communication channel, or the compromised host on which the inference system is running; ii) indirect: malicious data flow through other components of the ecosystem. Unlike with control technologies, attacks requiring direct device access are usually limited to insider threats due to the location of these devices. However, communication channels for data input/output, and remote maintenance provides avenues for remote access.

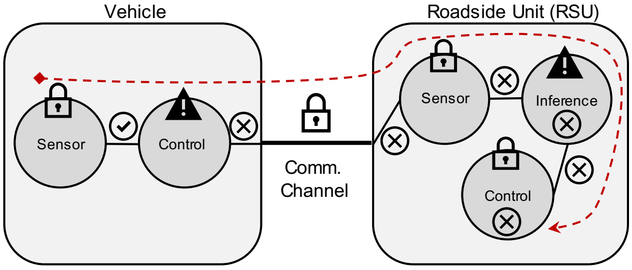


Figure 3. False data injection attack against the I-SIG inference system. The figure shows I-SIG enabled RSU with additional context information for the vehicle. Arrow shows the data-flow path from the vehicle to the I-SIG system. In this case, vehicle's control technology responsible for sensor data transmission is compromised, allowing malicious data-flow through to otherwise secure RSU.

Direct Attack. Inference systems are typically hosted on remote servers and expose application programming interfaces (API) for data exchange, and remote access services for maintenance and updates. As seen in the IoT domain, deploying such endpoints tend to expose vulnerable services through weak authentications, insecure implementation of APIs, and mis-configurations [59]. Such vulnerabilities allow post-acquisition sensing attacks leading to malicious data injection into the inference system. As discussed in section 5.1, fake video injected post-acquisition can lead to the inference system incorrectly triggering motion detection events and false alarms.

Indirect Attack. Adversaries can also manipulate input data sources to inference technologies by attacking another component of the transportation ecosystem. These attacks are difficult to consider during the system design as the input sources are typically out of the designer's control and often assumed to be trustworthy. For example, Chen at el. [4] discovered that certain edge-case input data are not handled optimally by the inference system used in I-SIG. I-SIG has real-time requirements for computing the updated optimal signal timing within two seconds. With only limited computational power available in the RSU device, the developers implemented a less optimal algorithm to satisfy the real-time requirements by assuming input from another part of the system is always correct. Crafted malicious data can be injected into the system through the pre-acquisition attack discussed in section 5.1.3, leading to inefficient signal timing to be generated. The path of malicious data flow into the system is shown in Fig. 3. Additionally, adversaries can disable the inference system by depriving it of input data by carrying out DoS/jamming attacks against input sources (section 5.1.3). Also, flooding the system with large volumes of input can increase the computational load leading to missed deadlines in real-time systems.

5.3.4. Impacts of Attack on Inference. Based on the use case of inference systems, attacks can have impacts on performance, safety, or both. Both performance and safety impacts are high in real-time systems. The attack

[1] Speed at which vehicles are likely to encounter continuing green lights in a coordinated corridor.

on the above I-SIG system resulted in 23.4% degradation in travel time of vehicles through the attacked intersection compared to the base system without it [4]. This is a significant drop in performance, completely reversing the benefits of the system. Unreliable insights generated from false data injections also impact the decision making process of the TMC operators and lead to performance and safety impacts. The impacts are catastrophic when inference systems are used for real-time safety critical decisions such as self-driving cars, as illustrated by some high-profile accidents that happened in the recent past [60], [61]. In this case the vehicle's control technologies rely upon the output of inference system to make critical driving decisions, but the inference system failed to provide accurate data. The same problem could happen to both vehicles and transportation infrastructures due to malicious act.

5.3.5. Possible Mitigations. The primary method to mitigate security issues in inference systems is to protect the platform on which it is running. Similar to the case in control technologies, vulnerable services exposed on the network by the platform is the primary threat to inference systems. Developers must disable unnecessary vulnerable services to reduce attack surface. Secure APIs must be designed so that it does not leak unnecessary data and should also be protected with proper authentication and encryption techniques. With the platform secured, the inference system itself must be designed to be resilient against malicious data inputs. Since these devices are more powerful than sensing devices, they should reinforce data validation, and noise reduction to reject malicious inputs. Other solutions require fundamental changes in design such as use of multiple or redundant data sources. For example, Dedinsky at el. [62] propose a system with video as a redundant data source to identify false data injections from connected vehicles, which is applicable to the I-SIG system. Such solutions, however, can increase the attack surface further with additional devices as well as create supplementary problems such as which data source to trust in case of conflicting information.

5.4. Applications

5.4.1. Applications Used in the Transportation System. The increase of third-party involvement in transportation ecosystem has increased the number of applications available for end-users and operators. Applications are used for interfacing with other technologies, configuring and managing network connected devices, and collecting data in the transportation ecosystem. Applications come in the forms of mobile apps, web apps, and desktop apps. Mobile apps for end-users provide advisory information like signal timing, speed limits, route planning, early warning, etc. Operators at the TMC use multiple applications to monitor traffic conditions and analyze data generated by the inference systems. Applications provide easy access to sensing and control devices for configuration and management.

5.4.2. Attack Categories and Impacts. Applications are attractive targets for adversaries due to the prevalence of software vulnerabilities. Security issues with mobile, web, and desktop applications, and the proper mitigations are well known to the security community and are not discussed in detail here. We focus on the threat posed by applications towards the the component they are used in. We discuss the applications and their security considerations we encountered during our fieldwork in TMC, along with appropriate supporting literature.

Vehicle and Intersection Applications. The most widely used applications in the transportation ecosystem are for navigation such as Google Maps and Waze. They transfer location data to cloud-based inference systems and this process provides adversaries opportunities for post-acquisition attacks. By exploiting the implicit trust placed on them by the cloud counterparts, adversaries can carry out false data injection attacks leading to manipulation of real-time traffic data and sub-optimal routing [63]–[65]. Equal care must also be given on the cloud-endpoints as we discussed in section 5.3.5. Other applications rely on data from the infrastructure and relay information to the end-users. Connected signals app [52], for example, displays the duration of traffic lights at approaching intersections estimated using data collected from the transportation network. Such applications can potentially have safety implication if they display unreliable information to an inattentive driver, which may lead to traffic violations or accidents.

RSU Applications. Companion applications provide easy access to control and sensing technologies for configuration changes and updates over the network. Unauthorized access to such applications must be prevented by using strong authentication and authorization mechanisms, without which adversaries can directly use them for malice [42]. Even with such safeguards, these applications can leak information which can be leveraged to eavesdrop on the system, extract configuration settings, user credentials, or reverse engineer communication protocols.

TMC Applications. Operators at the TMC utilize a wide range of applications to perform daily tasks such as monitoring traffic, maintaining and updating signal timings, operating DMS signs, toll gantries and/or reversible lanes, identifying and responding to road incidents, and analyzing collected data to improve overall traffic performance. During our fieldwork, we utilized the following tools for signal timing monitoring and management: i) Metropolitan Traffic Control System (MTCS). It is an old intersection controller application running on Microsoft DOS and does not support any modern security features. The monitoring system is not advanced and only detects mismatch between the server's and the local controller's copy of the signal timing and the interface provided to the operators is not very convenient. Hence, any direct/indirect attacks on the RSU may well go unnoticed by the operators for a long duration. ii) Centracs. It is used for both configuration and monitoring of Econolite controllers throughout the network as it interfaces with both devices and an inference system [58]. It is equipped with standard authentication features which is utilized by the operators, unlike on the signal controllers devices. Its connection to the inference system allows operators to access the accumulated logs from all the controllers and MMU devices connected. This comes in handy from an operational security perspective as it can generate alerts on many different types of faults and is also capable of generating reports for further analysis by the operators. It keeps track of any updates made to the signal timing using this application along with the user information. iii) ASC3 tools (kdClient, utility, configurator). These sets of tools are used to connect to older ASC/3 signal controllers. They provide direct connection to a single controller based on IP address for signal timing and the pin assignment manipulations [66]. Surprisingly these tools did not require any authentication to do so. With access to such configuration applications, adversaries can carry out all the attacks discussed in section 5.2.3.

For operation of reversible lanes, we used DYNAC's DynGate application [67]. This application provides interfaces to inference system used for scanning the roadway for vehicles before lane reversal, and control technology that is responsible for operation of lane barriers/gates and the corresponding signs. Adversarial access to such powerful applications can lead to dangerous situations such as lane reversal before the existing traffic within the roadway is cleared.

Other monitoring applications provide operators actionable real-time traffic flow information based on dedicated sensor or crowd-sourced data. BlueTOAD [68] utilizes data collected from traveller's bluetooth-enabled devices at various intersections while Waze Traffic View [69] and Waycare [55] utilize crowd sourced and other open data sources. Even applications only used for visual interface can impact the ecosystem by misleading the end-user/operator that relies on it. Hence, applications, based on the use-case, can have varied impact on the entire transportation ecosystem. Access to such monitoring applications can provide adversaries easier path to misinform operators, compared to attacking sensing (section 5.1.3) and inference systems (section 5.3.3), so as to cause operational decisions leading to unintended results.

5.4.3. Possible Mitigations. Mitigation for the shortcomings of legacy systems such as MTCS is to simply replace it with the latest technology. But in practice, this requires both device replacement and fundamental changes since it requires updating the backbone communication channel from twisted copper pair to fiber optics, and replacing all the cabinets on heavy traffic roads with the latest ones. This is not only cost prohibitive, but also requires coordination between several organizations as it would require construction work on the road, planning from the communication network perspective, and all the while providing smooth traffic flow through the city. This difficulty of upgrading legacy systems poses the primary challenge of securing the transportation ecosystem.

When developing new applications, developers must recognize the potential threats they present to the transportation ecosystem and create application specifications with security in mind. To prevent unauthorized access, eavesdropping, and information leakage, use of proper authentication and secure data exchange mechanisms with use of encryption and proper handling of cryptographic keys are essential. Vendors must utilize secure software development practices aided by the use of available tools for vulnerability discoveries where applicable. Additionally, the security features provided must account for operational requirements so that the operators do not bypass them due to usability concerns.

5.5. Communication Technologies

5.5.1. Types of Communication Technologies Used in the Transportation System. Communication channels facilitate the interoperability between different technologies and components. Latency, bandwidth, and reliability requirements dictate the type of communication channel used. Intra-component communication channels are typically wired using various types of connections and protocols. Inter-component communication, excluding vehicles, are also typically wired with copper-wires or fiber optics but wireless alternatives are necessary for connections to remote locations and to cloud-based services. Fiber optics connections are preferred where possible as they meet high bandwidth, speed, and reliability requirements of modern applications. Communication channels between the infrastructure and vehicles are still under development with approaches based on both 5G and short range point-to-point communication (e.g., Dedicated Short Range Communication (DSRC)) being explored.

5.5.2. Mechanisms of Communication. In vehicles, multiple sensors, ECUs, and other control technologies constantly communicate with varying requirements on timing, bandwidth, and priority. Some of the protocols in use are standardized like the Control Area Network (CAN) protocol while many others utilize proprietary protocols. In RSUs, devices are connected through point-to-point connections, serial communication using SDLC, or local area network (LAN). Communication between infrastructure devices use the National Transportation Communications for Intelligent Transportation System Protocol (NTCIP) standards [70] to support interoperability between vendors. Communication between RSU and intersection tend to be device specific and can be wired or wireless with vendors typically employing proprietary protocols. All the RSUs are then connected to each other and to the central TMC forming the transportation network. Due to the city-wide scale of this network, multiple RSUs are typically connected in a linear chain with no or minimal redundant connections between the different RSU groups. With the introduction of connected and autonomous vehicles (CAVs), vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and infrastructure-to-vehicle(I2V) communications are currently being tested in the field [71], [72]. Vehicle-to-anything (V2X) communications is being standardized as DSRC in the US by IEEE [73] and in europe as ITS-G5 by ETSI [74].

5.5.3. Attack Categories. Communication channels enable many of the attacks discussed. The primary claim to security in the transportation infrastructure is made based on the assumption that the transportation network is isolated/air-gapped from the external network [75]. With the implementation of connected vehicles (CV) technologies, this assumption can no longer hold. During our fieldwork, we found that third-party access to the internal servers is common for maintenance, upgrades, and use of cloud services. This necessitates complete trust in the third party in order to maintain the security assumptions. Workstations with the transportation applications are not supposed to be connected to the internet, but in practice the software is also installed in personal workstations with internet access for ease of use. We also find field devices exposed to the internet through the Shodan search engine [76]. Vendors also tend to claim security of products by use of proprietary protocols. Claims of security through obscurity using proprietary protocols is weak as reverse engineering of protocols is common [77], [78]. With such weak security properties, adversaries can attack the transportation ecosystem through communication channels by: i) attacking weak crypto; and ii) compromising network nodes.

Attacking Weak Crypto. Wireless communication channels that do not use proper encryption and authentication between the communication nodes are susceptible to MITM attacks. As mentioned, many of the vendors choose to develop proprietary protocols and claim it to be secure, but usually fail to implement secure protocols. This has been widely demonstrated in the IoT domain as well [59]. Cerrudo [2] reports that vendors of wireless vehicle detectors deliberately chose not to implement authentication and encryption when designing their protocol, claiming that the proprietary nature of the protocol led to the clients and vendors deciding against additional security. Such poorly implemented protocol allowed the researcher to eavesdrop on the communication from within the range of the IEEE 802.15.4 2.4 GHz transceiver, and reverse engineer the protocol. This resulted in post-acquisition false data injection attacks against the sensing technology. Additionally, the over-the-air update system was found not to be encrypted or signed, potentially allowing firmware update worms against the system. Even with the use of cryptographic measures, flaws in the protocol design can allow adversaries to exploit it through cryptanalysis and replay attacks. Roufa et al. [79] found that the protocol used by the tire pressure management system (TPMS) to send data simply uses a single bit to represent an alert, which means that the attackers only has to flip the bit to trigger an alert. Additionally, the presence of an identifier in the data packets led to the possibility of tracking the vehicles by eavesdropping on the communication. Due to the static nature of the data packet format, the protocol was deemed vulnerable to simple cryptanalysis and replay attacks even with the use of cryptographic measures. Ghena et al. [3] find that proprietary protocols are used for communication between RSUs over the ISM band (5.8 GHz or 900 MHz) and have similar shortcomings of lack of encryption, information leaking data packet formats, and use of simple transmission schemes such as frequency hopping spread spectrum (FHSS).

Compromising Network Nodes. Gaining access to any one of the network nodes gives adversaries access to the transportation network, allowing them to launch attacks. For example, standardized V2X and I2V communications such as DSRC, although not built with security in mind, do have the use of public key infrastructures (PKI) incorporated into the IEEE 1609.2 standards [80], [81], potentially preventing MITM attacks. However, Laurendeau et al. [82] and Kreilein [81] note that, even with cryptographic measures, DSRC can still be an enabler for attacks to the transportation ecosystem through deception attacks, denial of service (DoS) attacks (using false messages for spoofing or jamming), cryptographic attacks (private keys still accessible through OBD-II ports in vehicles), malware exploitation (using DSRC as a transmitter), and V2X exploitation (due to deployment of infrastructure without security architecture). When MITM is not possible, adversaries can still leverage the communication channel for attacks by compromising the communication node. For example, when the communication protocol uses proper authentication and cryptographic measures, adversaries can compromise a communication node to send malicious data through the legitimate communication channel [4].

5.5.4. Possible Mitigations. When using Internet Protocol (IP) suite for communication, TLS/SSL must be enabled and regularly checked for updates. Implementing secure communication protocols is known to be a difficult problem as even the most widely used protocols like TLS/SSL have previously been found to have vulnerabilities [83]. Hence, when appropriate, vendors should opt for well established protocols over custom ones. When custom protocols are created, data packet formats have to be designed to facilitate consistency checks and the use of encryption [79]. Use of cryptographic measures is always suggested but may not be feasible due to the restrictions in bandwidth, data rates and/or compute power. These challenges must also be accounted for when retrofitting existing protocols with security measures so that the solutions are feasible for use [84]. Additionally, applications involved in communication must also be secured. This includes use of up-to-date implementations of cryptographic libraries, and secure storage of cryptographic keys. Some of the legacy applications may also be patched to use updated protocols and enable encryption. Regulations should be introduced where possible so that there is uniform use of secure standards throughout the ecosystem.

6. Discussions

Within the transportation ecosystem, the roadside infrastructure is still in its infancy of technological advancement. This often means that the impact of cyber vulnerabilities is not as high yet. However, we are able to identify a number of weaknesses that portend much graver impacts should the system move quickly into the connected vehicle/autonomous vehicle paradigm, as many contend is happening: i) Over reliance on the isolated nature of the transportation infrastructure for security; ii) Race for rapid development of feature-rich products; iii) Stakeholders leading the development do not have adequate technology background, with many vendors evolving from developing mostly electrical systems to modern computer applications and cloud-based services. iv) Usability trumps security. In an operational environment such as the transportation infrastructure where many operators are not "cybersecurity savvy", operational usability is even more emphasized compared to cybersecurity practices.

As seen from section 5, transportation system is an intricate system where different technologies rely on each other to perform their tasks. Hence, the need for security might not be obvious as identifying attack goals, attack paths, and impacts can be difficult. To answer "why someone would attack a device?" one needs to not only know what the device does, but how it interacts with other devices in the ecosystem. Understanding the interactions between devices also helps identify potential attack paths. This information is not obvious to the developers working only on a single technology in the transportation ecosystem, as evidenced by the vendor's decision to not include authentication and encryption on wireless detectors discussed in section 5.5.3. The impacts of attacks and incentives to achieve them are also not easily observable. The primary impact is congestion and, even with the development of a successful exploit, its impact can only be shown through simulation models, which is not as "eye-catching" as real demonstrations of potential harm as shown by vehicular hacks. But congestion is a real problem. A study conducted by INRIX in 2018 estimates that drivers spent 97 hours in congestion in the U.S. and amounts to an average cost of $1,348 per driver ($87 billion annual cost) based on the FDOT's time loss valuation [48]. Until recently, the impact on safety was thought to be limited as conflict monitors were assumed to protect against conflicting greens by sending the intersection into conflict flash [3]. But flickering green attacks weakened this major safety assumption [42].

Emerging Threats. Transportation ecosystem is a critical infrastructure and is going through a rapid technology-driven overhaul. With increasing involvement of technology in mobility of both vehicles and pedestrians, the impacts of cyber attacks is only rising. Most of the applications being tested in the three CV pilots in U.S. are designated as safety features – 12 of 15 in New York, 9 of 13 in Tampa, and 5 of 5 in Wyoming. Once these are deployed and relied upon, cyber attacks will have even bigger safety implications. As we have seen, mitigating issues after deployment in the transportation system has many barriers – large-scale deployment, difficulty in access, financial restrictions, and involvement of multiple agencies. Hence, future deployments of technologies must first be put through a thorough security evaluation.

Security is considered a niche domain that requires expert knowledge and yet deploying a secure system requires collective effort from everyone involved. From the perspective of a user, it is the responsibility of the vendors to develop adequate security measures in all technologies. But to maintain security, users also need to utilize the available security measures. For the vendors, conducting a thorough security evaluation not only requires technical expertise but also domain knowledge from multiple disciplines to extensively identify attack goals, attack paths, and potential impacts. City-wide deployments of transportation infrastructures utilize technologies from multiple different vendors that have to work in unison. Hence, regulatory bodies also need to step in so that security standards are maintained by all the vendors involved. We believe that our systematization approach helps to breakdown the silos of each discipline and get everyone involved in the security discussion by abstracting away technical details into five core technologies which can then be used to describe any part of the transportation system. This provides the necessary context required to identify attack goals, uncover attack paths, and reason about attack impacts. Security experts can then use this information to flesh out the details in the development phase.

7. Related Work

There have been a number of prior works in vulnerability discovery in transportation infrastructure. Cerrudo [2] studied wireless vehicle detectors and discovered several security flaws allowing adversaries to control detector outputs and potentially deploy malicious firmware update worms. Ghena et al. [3] partnered with a local transportation agency to conduct a thorough vulnerability analysis of the signal controller and associated communication channels. They are the first to conduct such analysis and present important findings such as remote manipulation of signal timing. Ernst et al. [11] present a framework for threat assessment of traffic cabinets with four levels of access and evaluate the potential impact using simulation models. Ning et al. [42] expose the flickering greens attack allowing practically all-way-green state by manipulating control signal latency in CMU/MMU, which is a much stronger attack than previously demonstrated and has tremendous safety implications. Our work is related to these prior efforts in that we also focus on transportation infrastructure security. Our goal is to create a systematization framework for understanding the security issues in a holistic and context-aware manner. This has not been done in the past and is our unique contribution. Our systematization framework is based on insights from fieldwork in a real TMC for a period of six months, where we were embedded and interacted and worked along with the domain experts.

8. Conclusion

We present a systematization framework for understanding and reasoning about cyber security risks in the vehicle transportation ecosystem. The framework views the ecosystem through two dimensions: functional components and enabling technologies. This two-tiered view allows us to discuss security issues that are both common in pattern across multiple components, and intricate and context-specific. This provides a coherent framework through which to communicate security risks to transportation stake holders, and as a useful tool for security evaluations to derive insights into attack goals, attack paths, and potential impacts.

Acknowledgment

This research was supported by the U.S. National Science Foundation under grant no. 1638301. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

References

[1] C. Miller and C. Valasek, "Remote exploitation of an unaltered passenger vehicle," *Black Hat USA*, vol. 2015, p. 91, 2015.

[2] C. Cerrudo, "Hacking us traffic control systems," in *DEFCON 22*, 2014.

[3] 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)*, 2014.

[4] 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 *Network and Distributed Systems Security (NDSS) Symposium*, 2018.

[5] Texas A&M Transportation Institute. Traffic Management Centers. [Online]. Available: https://mobility.tamu.edu/mip/strategies-pdfs/traffic-management/technical-summary/traffic-management-centers-4-pg.pdf

[6] USDOT-FHWA. Transportation Management Centers - Freeway Management Program - FHWA Operations. [Online]. Available: https://ops.fhwa.dot.gov/freewaymgmt/trans_mgmnt.htm

[7] USLegal. Transportation Management Centers [TMC] Law and Legal Definition. [Online]. Available: https://definitions.uslegal.com/t/traffic-management-center-tmc

[8] B. Erskine. (2018) You Just Got Attacked By Fake 1-Star Reviews. Now What? [Online]. Available: https://www.forbes.com/sites/ryanerskine/2018/05/15/you-just-got-attacked-by-fake-1-star-reviews-now-what/#787a499b1071

[9] USDOT-FHA. (2017) Traffic Control Systems Handbook: Chapter 6 Detectors. [Online]. Available: https://ops.fhwa.dot.gov/publications/fhwahop06006/chapter_6.htm

[10] USDOT. (2017) Traffic Signal Timing Manual: Chapter 6. [Online]. Available: https://ops.fhwa.dot.gov/publications/fhwahop08024/chapter6.htm

[11] J. M. Ernst and A. J. Michaels, "Framework for evaluating the severity of cybervulnerability of a traffic cabinet," *Transportation Research Record*, vol. 2619, no. 1, pp. 55–63, 2017.

[12] USDOT. USDOT: Security Credential Management System (SCMS). [Online]. Available: https://www.its.dot.gov/factsheets/pdf/CV_SCMS.pdf

[13] A. J. Kerns, D. P. Shepard, J. A. Bhatti, and T. E. Humphreys, "Unmanned aircraft capture and control via gps spoofing," *Journal of Field Robotics*, vol. 31, no. 4, pp. 617–636, 2014.

[14] M. L. Psiaki and T. E. Humphreys, "Protecting gps from spoofers is critical to the future of navigation," *IEEE spectrum*, vol. 10, 2016. [Online]. Available: https://spectrum.ieee.org/telecom/security/protecting-gps-from-spoofers-is-critical-to-the-future-of-navigation

[15] P. Papadimitratos and A. Jovanovic, "Gnss-based positioning: Attacks and countermeasures," in *MILCOM 2008-2008 IEEE Military Communications Conference*. IEEE, 2008, pp. 1–7.

[16] K. Wang, S. Chen, and A. Pan, "Time and position spoofing with open source projects," *Black Hat Europe*, vol. 148, 2015.

[17] J. Coffed, "The threat of gps jamming: The risk to an information utility," *Report of EXELIS*, pp. 6–10, 2014.

[18] C. Yan, W. Xu, and J. Liu, "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle," *DEF CON*, vol. 24, 2016.

[19] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote attacks on automated vehicles sensors: Experiments on camera and lidar," *Black Hat Europe*, vol. 11, p. 2015, 2015.

[20] S. Networks. (2019) Sensys Networks - Traffic Detection Solution and Wireless Sensors. [Online]. Available: https://sensysnetworks.com/

[21] J. Obermaier and M. Hutle, "Analyzing the security and privacy of cloud-based video surveillance systems," in *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security*. ACM, 2016, pp. 22–28.

[22] K. C. Zeng, S. Liu, Y. Shu, D. Wang, H. Li, Y. Dou, G. Wang, and Y. Yang, "All your {GPS} are belong to us: Towards stealthy manipulation of road navigation systems," in *27th {USENIX} Security Symposium ({USENIX} Security 18)*, 2018, pp. 1527–1544.

[23] W. Xu, C. Yan, W. Jia, X. Ji, and J. Liu, "Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles," *IEEE Internet of Things Journal*, vol. 5, no. 6, pp. 5015–5029, 2018.

[24] B. S. Lim, S. L. Keoh, and V. L. Thing, "Autonomous vehicle ultrasonic sensor vulnerability and impact assessment," in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*. IEEE, 2018, pp. 231–236.

[25] USDOT-FHA. (2017) Traffic Control Systems Handbook: Chapter 7 Local Controllers. [Online]. Available: https://ops.fhwa.dot.gov/publications/fhwahop06006/chapter_7.htm

[26] N. American Association of State Highway and Transportation Officials (AASHTO), Institute of Transportation Engineers (ITE). Advanced Transportation Controller (ATC) Standard Version 06. [Online]. Available: https://www.ite.org/pub/?id=acaf6aca-d1fd-f0ec-86ca-79ad05a7cab6

[27] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham *et al.*, "Experimental security analysis of a modern automobile," in *2010 IEEE Symposium on Security and Privacy*. IEEE, 2010, pp. 447–462.

[28] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno *et al.*, "Comprehensive experimental analyses of automotive attack surfaces." in *USENIX Security Symposium*, vol. 4. San Francisco, 2011, pp. 447–462.

[29] A. Greenberg. (2016) The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse. [Online]. Available: https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks

[30] A. Goodwin. (2015) Tesla hackers explain how they did it at Defcon. [Online]. Available: https://www.cnet.com/roadshow/news/tesla-hackers-explain-how-they-did-it-at-def-con-23/

[31] F. Lambert. (2019) Hackers crack Tesla Model 3 in competition, Tesla gives them the car. [Online]. Available: https://electrek.co/2019/03/23/tesla-model-3-hacker-competition-crack/

[32] Traffic Parts. Traffic Parts. [Online]. Available: https://www.trafficparts.com/590CAB.pdf

[33] B. Stern. (2009) HOW TO - Hack Construction Signs. [Online]. Available: https://makezine.com/2009/01/27/how-to-hack-construction-signs

[34] K. B. Kelarestaghi, K. Heaslip, M. Khalilikhah, A. Fuentes, and V. Fessmann, "Intelligent transportation system security: hacked message signs," *SAE International Journal of Transportation Cybersecurity and Privacy*, vol. 1, no. 11-01-02-0004, pp. 75–90, 2018.

[35] C. Kraft. (2009) Road sign hacking - Hackaday. [Online]. Available: https://hackaday.com/2009/01/24/road-sign-hacking/

[36] B. Wojdyla. (2009) Road sign hacking - Hackaday. [Online]. Available: https://jalopnik.com/how-to-hack-an-electronic-road-sign-5141430

[37] ICS-CERT. (2014) Daktronics Vanguard Default Credentials (Update A). [Online]. Available: https://ics-cert.us-cert.gov/alerts/ICS-ALERT-14-155-01A

[38] B. Krebs. (2014) They Hack Because They Can - Kerbs on Security. [Online]. Available: https://krebsonsecurity.com/2014/06/they-hack-because-they-can/

[39] NEMA. NEMA TS-2 2003 Standard. [Online]. Available: http://www.peektraffic.com/portal/sites/default/files/NEMA%20TS2-2003.pdf

[40] ITS Cabinet Standard. ITS. [Online]. Available: https://www.ite.org/pub/?id=E26A4960-2354-D714-51E1-FCD483B751AA

[41] Z. Zhang, Z. Lv, J. Mo, and S. Niu, "Vulnerabilities analysis and solution of vxworks," in *2nd International Conference on Teaching and Computational Science*. Atlantis Press, 2014.

[42] Z. Ning, F. Zhang, and S. Remias, "Understanding the security of traffic signal infrastructure," in *International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment*. Springer, 2019, pp. 154–174.

[43] S. Peeta, J. L. Ramos, and R. Pasupathy, "Content of variable message signs and on-line driver behavior," *Transportation Research Record*, vol. 1725, no. 1, pp. 102–108, 2000.

[44] C. L. Dudek, *Changeable message sign operation and messaging handbook*. Federal Highway Administration, Operations Office of Travel Management, 2004.

[45] J. Olofsson, "'zombies ahead!'a study of how hacked digital road signs destabilize the physical space of roadways," *Visual communication*, vol. 13, no. 1, pp. 75–93, 2014.

[46] P. SrinivasaSunkari, "The benefits of retiming traffic signals," *ITE journal*, p. 26, 2004.

[47] Boston Transportation Department. The Benefits of Traffic Signal Retiming Report. [Online]. Available: https://www.cityofboston.gov/images_documents/The%20Benefits%20of%20Traffic%20Signal%20Retiming%20Report_tcm3-18554.pdf

[48] T. Reed, "Inrix global traffic scorecard," *INRIX research*, 2018.

[49] Cloudera. Navistar — Customer Success — Cloudera. [Online]. Available: https://www.cloudera.com/about/customers/navistar.html

[50] Y. Zhao, S. Li, S. Hu, L. Su, S. Yao, H. Shao, H. Wang, and T. Abdelzaher, "Greendrive: A smartphone-based intelligent speed adaptation system with real-time traffic signal prediction," in *2017 ACM/IEEE 8th International Conference on Cyber-Physical Systems (ICCPS)*. IEEE, 2017, pp. 229–238.

[51] E. Koukoumidis, L.-S. Peh, and M. R. Martonosi, "Signalguru: leveraging mobile phones for collaborative traffic signal schedule advisory," in *Proceedings of the 9th international conference on Mobile systems, applications, and services*. ACM, 2011, pp. 127–140.

[52] Connected Signals. Connected Signals Enlighten. [Online]. Available: http://connectedsignals.com/products/#enlighten

[53] M. Ginsberg, "Traffic signals and autonomous vehicles: Vision-based or a v2i approach?" *Intelligent Transporation Systems, ITSA-16*, 2016.

[54] M. L. Ginsberg, P. J. Flier, M. C. Drohmann, and T. S. Stirling, "Traffic routing display system with multiple signal lookahead," Feb. 5 2019, uS Patent App. 15/804,630.

[55] Waycare. Waycare AI-driven Mobility Solutions. [Online]. Available: https://waycaretech.com/

[56] A. M. De Souza, C. A. Brennand, R. S. Yokoyama, E. A. Donato, E. R. Madeira, and L. A. Villas, "Traffic management systems: A classification, review, challenges, and future perspectives," *International Journal of Distributed Sensor Networks*, vol. 13, no. 4, p. 1550147716683612, 2017.

[57] Miovision. Traffic Operations - Miovision. [Online]. Available: https://miovision.com/solutions/traffic-operations/

[58] Econolite. Centracs Edaptive Econolite. [Online]. Available: https://www.econolite.com/products/software/centracs-edaptive/

[59] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose, "Sok: Security evaluation of home-based iot deployments," in *Proceedings of the IEEE Symposium on Security and Privacy (S&P). https://doi.org/10.1109/SP*, 2019.

[60] A. Marshall. (2018) Uber's Self-Driving Car Just Killed Somebody. Now What? [Online]. Available: https://www.wired.com/story/uber-self-driving-car-crash-arizona-pedestrian/

[61] A. Greenberg. (2019) Death of Elaine Herzberg - Wikipedia. [Online]. Available: https://en.wikipedia.org/wiki/Death_of_Elaine_Herzberg

[62] R. Dedinsky, M. Khayatian, M. Mehrabian, and A. Shrivastava, "A dependable detection mechanism for intersection management of connected autonomous vehicles," in *1st International Workshop on Autonomous Systems Design*, 2019.

[63] T. Jeske, "Floating car data from smartphones: What google and waze know about you and how hackers can control traffic," *Proc. of the BlackHat Europe*, pp. 1–12, 2013.

[64] M. B. Sinai, N. Partush, S. Yadid, and E. Yahav, "Exploiting social navigation," *arXiv preprint arXiv:1410.0151*, 2014.

[65] N. Tufnell, "Students hack waze, send in army of traffic bots," *Wired*, 2014.

[66] Econolite. ASC/3 Programming Manual. [Online]. Available: http://www.dot.state.oh.us/Divisions/Operations/Traffic/miscellaneous/Signals%20Documents/ASC3_Programming_Manual.pdf

[67] Kapsch TrafficCom. DYNAC Advanced Traffic Management. [Online]. Available: https://www.kapsch.net/us/ktc/downloads/brochures/Kapsch-KTC-BR-ATMS-DYNAC-EN_US-WEB.pdf?lang=en-US

[68] TrafficCast. BlueTOAD by TrafficCast. [Online]. Available: https://makezine.com/2009/01/27/how-to-hack-construction-signs

[69] Waze. Use Traffic View - Waze Partners Help. [Online]. Available: https://support.google.com/waze/partners/answer/7246755?hl=en

[70] NTCIP. NTCIP Published Standards. [Online]. Available: https://www.ite.org/pub/?id=E26A4960-2354-D714-51E1-FCD483B751AA

[71] M. Faezipour, M. Nourani, A. Saeed, and S. Addepalli, "Progress and challenges in intelligent vehicle area networks," *Communications of the ACM*, vol. 55, no. 2, pp. 90–100, 2012.

[72] USDOT. Intelligent Transportation Systems - Connected Vehicle Pilot Deployment Program. [Online]. Available: https://www.its.dot.gov/pilots

[73] J. B. Kenney, "Dedicated short-range communications (dsrc) standards in the united states," *Proceedings of the IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011.

[74] ETSI. ETSI - Our Committee Intelligent Transport System (ITS). [Online]. Available: https://www.etsi.org/committee/1402-its

[75] E. Fok, "Cyber security challenges: Protecting your transportation management center," *Ite Journal*, vol. 85, pp. 32–36, 02 2015.

[76] Shodan. Shodan. [Online]. Available: https://www.shodan.io/

[77] J. Caballero and D. Song, "Automatic protocol reverse-engineering: Message format extraction and field semantics inference," *Computer Networks*, vol. 57, no. 2, pp. 451–474, 2013.

[78] B. D. Sija, Y.-H. Goo, K.-S. Shim, H. Hasanova, and M.-S. Kim, "A survey of automatic protocol reverse engineering approaches, methods, and tools on the inputs and outputs view," *Security and Communication Networks*, vol. 2018, 2018.

[79] R. M. Ishtiaq Roufa, H. Mustafaa, S. O. Travis Taylora, W. Xua, M. Gruteserb, W. Trappeb, and I. Seskarb, "Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study," in *19th USENIX Security Symposium, Washington DC*, 2010, pp. 11–13.

[80] Z. MacHardy, A. Khan, K. Obana, and S. Iwashina, "V2x access technologies: Regulation, research, and remaining challenges," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 3, pp. 1858–1877, 2018.

[81] A. Kreilein, "Security considerations for connected vehicles & dedicated short range communications," *SecureSet*, 2017.

[82] C. Laurendeau and M. Barbeau, "Threats to security in dsrc/wave," in *International Conference on Ad-Hoc Networks and Wireless*. Springer, 2006, pp. 266–279.

[83] C. Meyer and J. Schwenk, "Sok: Lessons learned from ssl/tls attacks," in *International Workshop on Information Security Applications*. Springer, 2013, pp. 189–209.

[84] C.-W. Lin and A. Sangiovanni-Vincentelli, "Cyber-security for the controller area network (can) communication protocol," in *2012 International Conference on Cyber Security*. IEEE, 2012, pp. 1–7.

Appendix

1. Summary on Threat with Each Attack Category

Attacker capabilities. We examine the threat model based on assumptions on attacker capabilities: (1) *Access Required*: A strong threat model requires the adversary to have physical access, while a weaker model may only require proximity or remote access. (2) *Expertise Required*: The knowledge and the skill required to carry out a cyber-attack can range from layman, proficient, to expert.

TABLE 1. Example: Different Threat Models based on Technological View

Technological View	Access Required			Expertise Required		
	Physical	**Proximity**	**Remote**	**Layman**	**Proficient**	**Expert**
Sensing	E.g., Mechanic miscalibrating a sensor during maintenance	Access to objects in the range of the sensor (e.g., tampering road signs); Access to devices that can communicate with the sensing device (e.g., spoofing V2I messages from a controlled device.)	Access to sensor through online configuration tools (E.g., Mobile or web interface)	Basic understanding of what the device does based on openly available resources (E.g., Tampering road signs.)	Understanding of the device mechanism, tools to interact with it. E.g., Replay attacks	Detailed understanding of device implementation. E.g., Reverse engineering protocols, device firmware updates
Control	E.g., Manipulating the physical device using on device controls	Direct connections to the device through open WiFi/Bluetooth; MITM attacks	Access to device through online configuration tools (e.g., Mobile or web interface)	Basic understanding of the device based on openly available resources (E.g., Logging in using default configuration found online.)	Exploiting weak authentication and vulnerable services (E.g., Launching brute-force password cracking, accessing open SSH ports)	E.g., Developing targeted exploits, reverse engineering, updating firmware
Inference	E.g., Adversaries with access to devices/servers running the inference; Insider threats	Indirect attacks (E.g., Proximity attacks on data sources like sensing)	Post-acquisition data injections (E.g., Exploiting server APIs)	Basic understanding of how the system works. (E.g., Logging in to cloud services using default configuration)	Indirect attacks (E.g., Data replay attacks); Exploiting weak authentication and vulnerable services (E.g., SSH, API misuse, data injection)	E.g., Crafting malicious data based on knowledge of the algorithm used, DDoS
Applications	Access to the device running the application (E.g., Access to an operators device)	MITM attacks	Remote connection to the application/device running the application	Basic understanding of application usage. (E.g., Perform allowed changes using the application)	Understanding of the application (E.g., Bypassing authentication, application API misuse, privilege escalation)	E.g., Reverse engineering the application, extracting encryption keys, creating malicious applications
Communication	Access to networking device (E.g. router, switch, or any communicating node)	Access within the range of communication devices. (E.g. WiFi, DSRC)	Internet connected devices	Basic understanding of networking and using commercial tools for eavesdropping	Ability to sniff, capture, delay, modify, transmit communication packets	Ability to infer information by analyzing the captured traffic and craft adversarial packets (E.g., Side-channel attacks, Cryptanalysis)

The threat model can be used to assess the likelihood of attacks. A sample description of the threat model for each technology is given in Table 1.

We apply the systematization approach to identify the target component and the technologies that enable it to provide the context for security analysis. We then perform security analysis within this context to analyze the potential attack methods the adversaries pursue and the mitigations approaches stakeholders employ.

The common attack categories identified are defined as follows:

- **Sensing vulnerability** refers to any means which lead to erroneous information flow into the system.
- **Service vulnerability** refers to vulnerabilities in running services. This category groups together the following: exposes unnecessary services, exposes unauthenticated services, service allows remote code execution, leaks sensitive information, or exposes unauthenticated/unsigned software updates.
- **Weak/No authentication** refers to lack of or weak/guessable credentials. This category groups no authentication, using weak/shared/guessable passwords, and using default/hard-coded passwords.
- **Weak/No encryption** refers to lack of encryption or support of weak encryption protocols. This category also groups issues related to encryption such as hard-coded encryption keys or extractable encryption keys through side-channels.

- **Programming vulnerability** refers to vulnerable implementations of running programs, issues emerging from misusing APIs, or security assumptions made when integrating with other products.

The mitigation approaches to prevent these vulnerabilities are categorized as follows:

- **Patching** refers to upgrading the existing software.
- **Device replacement** refers to upgrading the existing hardware.
- **Fundamental changes** refers to the need for major changes. For software issues, this can mean changing the development process, or deploying new frameworks. For hardware, this can mean upgrading the entire infrastructure, or switching to different class of devices. This approach demands major effort, time, and finances.
- **Regulation** refers to introduction or changes made in rules, or standards. This may include changes to an organizations operational practices, or introduction/modification made by the standardization bodies.