Connected Cars: Automotive Cybersecurity and Privacy for Smart Cities

Habeeb Olufowobi, Howard University, USA
Gedare Bloom, Howard University, USA
Email: {habeeb.olufowobi, gedare.bloom}@howard.edu

Abstract

This chapter examines the cybersecurity and privacy of the twin notions of smart transportation and intelligent transportation systems with a focus on the role of personal automobiles. Smart transportation encompasses the individual and joint capabilities of connected cars, or more generally vehicles, and so comprises the internal workings of autonomous vehicles and the complex interdependencies introduced by vehicle-to-vehicle (V2V) communications. An intelligent transportation system introduces smart technology to civil transportation infrastructure, and the connected car further creates the opportunity for vehicle-to-infrastructure (V2I) communications. We identify threats and attacks enabled by smart transportation and intelligent transportation systems, and survey methods for providing security and privacy.

Keywords: cybersecurity, V2V, V2I, smart transportation, connected cars, intelligent transportation system.

1 Introduction

This section introduces the role of automobiles in the smart city ecosystem. The terminology and the layout of the chapter is described to orient the reader with a roadmap for the sections of this chapter. Here we also explain how the chapter is organized in two parts: smart transportation and intelligent transportation systems.

Notable attention focuses on the Internet of Things (IoT) by the academic and industrial communities in the past years. Increasingly, applications based on IoT have been deployed in use cases that are significant in the smart city ecosystem. A fundamental application of IoT is in smart transportation. Smart transportation describes an application of modern technologies and strategic management to transportation systems. These technologies include low-level sensors and actuators, data gathering and analysis, and wireless network communication. Taken together, these technologies can dynamically adjust traffic behavior through signal manipulation, better inform users of the status of transportation networks, increase efficiency of transportation services, and improve traffic management operations.

The benefits and effectiveness of smart transportation in smart city ecosystem cannot be overemphasized. Also, in-vehicle systems and global positioning system (GPS) based services have inspired some of the innovations. Intelligent transportation has become an essential part of the general IoT landscape when it comes to developing an empowered society. Integrating technology into transportation infrastructure can decrease the associated cost of traffic congestion, increase the safety of users and also facilitates the development of smarter infrastructure to meet future demands. Furthermore, connecting the car to other smart cars and the transportation infrastructure of the smart city ecosystem will enable new possibilities for our societies, such as self-monitoring roads that can predict traffic and send information to on-the-road users. Intelligent

transportation systems (ITS) have made all these transportation technologies possible. However, these possibilities come with anticipated security and privacy risks.

The modern automobile is a cyber-physical system (CPS) comprising tens to hundreds of computers that control the vehicle's electrical-mechanical components operated by hundreds of millions of software lines of code. Vehicle components are controlled by various electrical control units (ECUs) that are connected together through an internal network, also called an in-vehicle network, which may even be connected to the Internet. Each in-vehicle network typically connects multiple communication networks and protocols, including the industry standard Controller Area Network (CAN), Local Interconnect Network (LIN), FlexRay, Media Oriented Systems Transport (MOST) and Radio Frequency (RF) communication. An in-vehicle network consists of nodes, gateways, and buses. Data is transferred from one network to another through a gateway, and all messages are broadcast on the bus. The vehicle network is a medium that facilitates data exchange in the automobile. These networks can be accessed through the standard on-board diagnostics (OBD)—a vehicle self-diagnostics and reporting port—or via wireless communication interfaces such as Bluetooth, WiFi, and cellular telephone networks.

From the communication bus perspective, modern vehicles contain multiple interfaces that expose the vehicular systems to cyber-attacks through physical and wireless access. These interfaces require varying levels of security in order to effectively thwart cybercriminals from gaining access to them. Physical access means that the attacker has a direct connection to the OBD port of the vehicle that is connected to the CAN bus and all ECUs. This port can be accessed easily by an adversary with the right equipment and a window of opportunity. The attacker can plug a small dongle into the OBD port to gather information or inject messages directly into the vehicle. Also, an attacker can plug a device into the port and access it remotely [10]. Alternatively, an attacker may gain access to the network through the use of the USB port. Using these methods, multiple teams have demonstrated overriding security controls to reflash ECUs [48, 59], providing the opportunity to inject or monitor CAN traffic without leaving any physical traces.

Remote and wireless attack surfaces are more worrying because the attacker does not need to physically connect any dongle to the vehicle. These attack surfaces include in-vehicle Bluetooth and the telematics unit that are common in vehicles for wireless and cellular connectivity. Bluetooth attacks have been demonstrated by Checkoway, et al. [10] using various methods of connecting to the communication bus through Bluetooth with malware installed on an already-paired Android phone, and with a method, they developed for unauthorized pairing. Miller and Valasek [58] demonstrated unauthorized CAN bus access to 2015 Jeep Cherokee through its WiFi network that exploits the weakness in its password generation protocol.

The apparent motivations for adversaries to launch cyber attacks against vehicles are shared across the autonomous vehicle, vehicular ad-hoc networks (VANETs), vehicle-to-vehicle, vehicle-to-infrastructure, connected car, intelligent transportation system, and even traditional (non-connected) automobiles. These motivations, or goals, include:

- *desire* for infamy, vengeance, or twisted pleasure [35];
- *profit* [81];
- *control traffic* [71], so as to create open or congested routes;
- *disrupt traffic* [63] to create congestion or even panic;

Table 1: Threats and attacks against vehicles grouped by targeted security objective.

Availability	**Confidentiality**	**Integrity**	**Authentication**
Denial of service (DOS)	Traffic Analysis	(GPS) Signal Spoofing	Sybil
Distributed DOS (DDOS)	Eavesdropping	Replay	Impersonation
Jamming	Tunneling	Wormhole	Masquerade
Black Hole	Cryptanalysis	False data injection	Tampering
Spamming	Man-in-the-middle (MitM)		
Malware			

- *conduct intelligence, surveillance, and reconnaissance (ISR)* [40], whether targeted or en masse;
- *vehicle theft* [15], usually targeted;
- *remote hijack* [9, 84], to take control of an operating vehicle;
- infecting with *vehicle malware* [89];
- creating a *vehicular botnet* [27].

The kinds of attacks that an adversary may launch to achieve their goals are summarized in Table 1. These attacks are many and varied, but they are basically based on compromising the traditional information security objectives of confidentiality, integrity, availability (CIA), and disrupting the security system's implementation of one of Lampson's "gold standard" of authentication, authorization, and audit. Confidentiality may be lost when an adversary can eavesdrop on the information sent through networks or unauthorized users have access to the information shared within the network, while the integrity of transmitted messages can be compromised by message tampering, injection, replay, masquerading, and deletion. Service availability may be compromised by denying access to use the service, which is typically accomplished by a denial-of-service (DOS) attack or the related distributed denial of service (DDOS) attack. In the following list, we briefly describe each kind of attack:

- Denial of service (DOS). DOS attacks occur when an adversary takes overall control of the network resources or flood the communication channels to deny inflow and outflow of information, making the whole network not usable for all connected nodes. The overall goal is to prevent the legitimate nodes from using the network resources [39]. This attack compromises the availability of the network, which is an essential requirement of normal vehicle operations in the smart city. This action places the driver and passengers in danger if they solely depend on the information provided by the network.
- Node Impersonation. An adversarial node broadcasts a message and claim the message is from another node by changing his identity to prevent being detected. The node may assume the identity of an authorized node to utilize network resources or to disrupt the normal operations of the network.

- Sybil Attack. An adversary creates multiple identities of itself to transmit messages to different nodes on the network. Thus, other nodes believe that there are many nodes on the network at the same time and are forced to use alternate routes.Also, the adversarial node has the potential to inject false information into the networks through the fictional nodes contrived on the network. Sybil attacks have been considered as a severe security threat to sensor networks and VANETs, and they can compromise the data integrity, security, and resource utilization of the vehicular networks [19].

- Global Positioning System (GPS) Spoofing. The adversarial node overrides the signal from a GPS satellite to provide false location and time information to targeted nodes. An adversary makes use of GPS satellite simulator to generate signals more effective than the original GPS satellite [68] to deceive vehicles to think they are in different locations.

- Masquerade. A malicious node simulates an identity to pretend to be another node. This simulation can be accomplished by message fabrication, replay, and alterations.

- Black hole. The adversarial node will not participate in the operation of the routing information when the information is received. This disrupts the routing table and causes packet loss because the network traffic will be redirected.

- Traffic Analysis. An adversary intercepts and analyzes communication patterns of nodes in order to extract useful information. This attack can be performed even when the messages are encrypted and cannot be decrypted.

- Malware. Malicious software is designed to run on a system without the user's consent with the intent of harming the system. Malware is injected into a network to cause disruptions in normal operations which can lead to serious consequence.

- Man-in-the-Middle (MitM). An adversary eavesdrops and possibly modifies the communication between two nodes who think they have a direct communication with one another. MitM violates trust between nodes in the network.

- Timing attacks. The adversary intentionally creates a delay to prevent messages from reaching the destination node in time.

- Eavesdropping. As a passive attacker, an adversary intercepts (listens) to messages sent on the network. Detecting this kind of attack can be difficult, while launching the attack can be easy, both depending on the communication media.

Some of these attacks rely on physical access, e.g., GPS spoofing can only be done in (relatively) close proximity to the target, while other attacks can be conducted remotely using only a network connection. In general, any goal that can be achieved through remote attacks is achievable through physical attacks, since with physical access the adversary can control and observe the same data used to launch an attack with remote access. Although physical access may be harder to achieve for an adversary, attacks that rely on physical access tend to be less complex to conduct than those with remote access. Often, physical access may be used to facilitate remote access, for example by using physical access to install a wireless or radio device that enables future remote access.

1.1 Chapter Layout

This chapter is organized in two parts. Part I consists of Sections 2–6, and addresses the security and privacy of autonomous vehicles and vehicle-to-vehicle communication as the underlying technologies for smart transportation. Sections 7–11 compose Part II, which explores the impact on security and privacy caused by the integration of vehicles with the transportation infrastructure via the vehicle-to-infrastructure and infrastructure-to-vehicle communications. We conclude in Section 12.

Part I: Smart Transportation

Section 2 describes the current state-of-the-art capabilities in autonomous vehicles and vehicle-to-vehicle communication, and discusses some of the expected developments in these capabilities. Primarily, the goal of this section is to give the reader sufficient background and terminology for the remainder of Part I.

Section 3 identifies the range of realistic threat models that should be considered against autonomous vehicles. Motivations for attacks will be described along with the attack capabilities of adversaries in the smart city ecosystem. The impacts of attacks will also be discussed. We will address threats against both the automotive systems, *e.g.*, the controller area network (CAN) bus, and the autonomous software, *i.e.*, the machine learning and computer vision algorithms. Section 4 surveys the solutions for assuring security and protecting privacy against the threats and attacks on autonomous vehicles. Gaps in the literature, *i.e.*, threats that are inadequately defended against by known approaches, will also be identified here.

Section 5 describes how the introduction of communication between vehicles causes new threat models to be relevant; new motivation and attack capabilities will be identified. We will briefly discuss vehicular ad hoc networks here together with direct communications between cars. Section 6 discusses solutions for security and privacy despite the threats and attacks against vehicle-to-vehicle communications.

Part II: Vehicle-Infrastructure Integration

Section 7 describes the current state-of-the-art capabilities in communications between vehicles and the transportation infrastructure, and discusses expected evolution in these capabilities. This section provides background and terminology to understand the remainder of Part II.

Section 8 identifies the threats and attacks against connected cars that arise due to the introduction of vehicle-infrastructure communications. Section 9 surveys approaches for providing security and protecting privacy against the threats and attacks targeting vehicles that are introduced by communications between vehicles and transportation infrastructure. We will not discuss in any detail solutions pertaining to known problems with vehicular or infrastructure security that existed prior to such communication capabilities.

Section 10 surveys attacks against transportation infrastructure that are enabled by communication between the infrastructure and vehicles. Section 11 identifies solutions for assuring security and privacy against the threats and attacks targeting civil infrastructure that are introduced by such vehicle-infrastructure communication.

2 Autonomous Vehicles (AVs) and Vehicle-to-Vehicle (V2V) Communication

With the growing numbers of vehicles on the road, driver error often results in car crashes, which sometimes include loss of human lives or bodily injury. Autonomous vehicles (AVs) and vehicle-

to-vehicle (V2V) communication aim to reduce driver error while simultaneously bringing potential to reduce congestion on our roadways by using sensors and in-vehicle technologies to shape how people move around, work, and live in a smart city ecosystem. Highly automated vehicles are able to navigate using artificial intelligence, sensors, and inter-connected computer systems working together to control the vehicle to reach its destination without human operation. In-vehicle sensors generate data that are analyzed by computer software for the vehicle decision-making algorithms that control vehicle operations such as acceleration, braking, and steering in real-time. The sensors are connected to other devices or services within and outside the vehicle using internal and external networks for data communication. Internal connections rely on the existing in-vehicle network structures of modern vehicles. External communications may include V2V or even communicate with the transportation infrastructure (V2I) and the Internet. Together, the communication capabilities provide traffic information and alerts to help ensure the safety of the vehicle, its passengers, and its surrounding environment.

2.1 Overview of Autonomous Vehicles

Increasingly, AVs are expected to form a significant part of the automotive industry. The industry and other stakeholders continue to harness advances in technology to develop capabilities that will ease congestion on our roads and provide social welfare benefits to users. Some of the benefits include increased mobility for the disabled, elderly and the young, improved fuel or energy consumption, and reduced fuel emissions. Traffic flow could be more efficient, because the AVs will obey traffic laws and travel times more diligently than human operators, and vehicles can be used to engage in activities even without a human driver, thereby reducing travel costs. However, important challenges in achieving these benefits is the cybersecurity and privacy protection of this vehicle and its passengers. As the vehicles become more network-connected, they also become more attractive targets for cyberattack. The risk associated with an attacked AV may greatly outweigh its benefit as the impacts can affect human safety.

2.2 Overview of V2V

V2V facilitates wireless information exchange between vehicles about potential collisions on the road. V2V aims to provide drivers with significant information and warn them about any imminent hazard in real-time. Using dedicated short-range radio communication (DSRC) technology [46], cars will communicate with each other, automatically broadcast data such as current GPS location, the speed of the vehicle, direction, path history, and vehicle control information—brake status, transmission state, steering wheel angle. By integrating V2V communication services into the vehicle, the technology is expected to enhance the safety and efficiency of the drivers and our roads. The idea is to prevent vehicle collisions before they occur.

DSRC protocols [12] is based on IEEE 802.11 Wi-Fi standard and can accommodate device communication of up to 300 meters in range. With this protocol, vehicles will have a 360-degree view of the road and will be able to share safety messages in their closed proximity that can help drivers responds quickly to prevent crashes and save lives. DSRC works in the 5.9 GHz band with a bandwidth of 75 MHz that is assigned separately only for vehicular communication. with a broadcast update of up to 10 times per second, connected vehicles can share basic safety messages that can better pinpoint dangers and warn the drivers about a potential collision. DSRC protocol has a low communication latency (less than 100ms) and high data transfer rates(up to 27 Mbps for services and 6 Mbps for safety) [72]. It can also support multi-hop network for extended range communications. Devices using this protocol can communicate not only with themselves but also the road infrastructure.

According to the United States Department of Transportation and the National Highway Traffic Safety Administration (NHTSA), V2V address the following three different safety applications scenarios for which current vehicle sensors such as cameras or LIDAR cannot be utilized [38]:

1. Intersection Movement Assist: This technology alerts the driver when it is unsafe to enter an intersection due to a possible collision with other vehicles at the intersection. Such alerts could help at signalized intersections and those with stop and yield signs to avoid potentially dangerous accidents.

2. Emergency Electric Brake Light: This technology alerts the driver to apply the brake when a similar V2V-equipped vehicle decelerates quickly. The decelerating vehicle may not be directly in front of the warning vehicle. The warning will be quite helpful in circumstances where the driver's line of sight is obstructed by other vehicles or extreme weather conditions.

3. Left Turn Assist: This technology alerts the driver not to turn left in front of another vehicle traveling in the opposing direction when entering an intersection. When turning across opposite lanes, this warning can help prevent accidents with an approaching vehicle.

Other technologies enabled by V2V include:

1. Forward Collision Warning: This technology is designed to limit and decrease rear-end crashes and to also assist in keeping a reasonably safe distance between vehicles. The warning alerts drivers when an impending frontal collision is about to occur.

2. Blind Spot: This technology alerts the drivers of the presence of other vehicles in the areas they are unable to see. The system identifies the nearness of another vehicle traveling diagonally behind the driver's vehicle and signals its presence with an indicator.

3. Lane Departure or Keep Warning: This technology alerts the drivers whenever the vehicle is veering from the lane by monitoring the lane markings on the roadway. The lane keep warning is able to take corrective actions by keeping the vehicle from drifting, unlike the lane departure warning that just alerts the driver about lane changes.

4. Do Not Pass Warning: This technology alerts the driver that it is unsafe to overtake a slower moving vehicle when using a passing zone which is occupied by another vehicle traveling in the opposite direction. This warning alerts the driver to avoid a head-on collision with the oncoming vehicle.

The future of our roads and cars depends on V2V communication technology. Connectivity presents incredible possibilities for growth by decreasing congestion and increasing the efficiency of traffic flow. These technologies can be harnessed to enhance the safety and usage of our roadway infrastructure. However, V2V can also create potential security threats. Adversarial vehicles can use this technology for sending fraudulent messages for their own gain or use it to disrupt the flow of the traffic system. The severity of a potential tampering could have disastrous consequences and even result in loss of human life. Hence, it is essential to design the V2V system with robust security to ensure seamless communication and trusted data sharing.

3 Threats against Autonomous Vehicles

Although vehicle connectivity is a new sensation among several auto industries and the government, the thought of using these technologies continues to develop rapidly. However, any new technology comes with new risks and challenges along with the benefits. Modern vehicles contain multiple interfaces that expose the vehicular systems to cyber-attacks. We will consider these cyber attacks in two different perspectives.

From AV perspective, an adversary may breach the network that facilitates the communications between the control systems of the vehicle, such as the sensors, cameras, GPS, radar, and odometry to have full control that can threaten human lives. The key control systems could be deactivated remotely to direct or drive the vehicle to an undisclosed destination. Also, the connected technologies including the laser range finders, LIDAR, cameras, and sensors acting as the vehicle's eyes and ears are attractive targets for cyber attackers, because they contains complex software that may have some bugs which are sometimes vulnerable to a security breach.

Another key area of software attack is on the machine learning and the computer vision algorithms used for the AVs. The machine learning models are vulnerable to adversarial example attacks which are inputs designed to intentionally confuse the model into producing an incorrect output such as miscategorizing an object for another [42, 49, 55, 66]. This type of attack causes an inherent security threat for practical machine learning applications, and an adversary can perform misclassification attacks on a machine learning system—such as an AV—without access to the underlying machine learning model [65, 66]. In this kind of attack, an adversary may alter the images (traffic signs) used internally by the vehicle by transforming the physical sign to something else and then use the modified image to mislead the navigation system of the autonomous vehicle or cause the vehicle to behave dangerously. Furthermore, AVs connected technologies generate and collect a vast amount of data through sensing and learning about the vehicle's surrounding environment during operation. Misuse of such data is a threat to the privacy of the drivers, passengers, other vehicles, and other users of the roadways including pedestrians and cyclists.

Worthy of note are the privacy-related issues of the AVs. Presently, AVs are still in testing phases, and while there are no definite answers to the type of data the vehicles will be collecting and sharing with other AVs and the infrastructure, AVs currently are logging and sharing location related information about the vehicle itself. This type of information has the potential to be used in tracking and determining the places visited by the vehicle owner, which is privacy invasive. Other privacy-related issues that can be considered in using AVs includes owners and passengers information, location tracking, sensor data collection by auto companies and travel data stored for route planning, point of interest and location features. Travel and location data leveraged with supplementary information of the owner and passenger of the vehicle could produce such benefits like traffic planning, increased safety and reducing traffic. But, this kind of combined dataset can be privacy invasive as it exposes sensitive information about the users of the service, especially if the data is persistently maintained. If an adversary has access to such information, individuals and society at large may be at risk of information misuse.

The advancement in technology for AVs is generating waves across the automotive and information technology industries, and also excitement among technology enthusiasts, hobbyists, and consumers. However, the risks associated with the use of AVs, as well as cybersecurity threats directed towards them, need to be fully examined and understood before AVs start operating on our roadways.

4 Security and Privacy for Autonomous Vehicles

Auto manufacturers have been struggling to address security and privacy issues in AVs because the attack surface continues to grow as new functionality for safety and comfort are added to the vehicle. Software related security solutions are deemed sufficient in some cases, while in other cases, tamper-proof security solutions are required. Security solutions such as message encryption and authentication [5,24,80,83], digital signatures [70], intrusion detection systems [41, 50, 61, 75, 87], and over the air firmware security updates can provide comprehensive system protection [67]. In the case of privacy, it remains to be seen what kind of personal information the AVs can collect at the moment because they are still in testing phase. At the minimum, the vehicles will be using the GPS location data—route information, destination information, speed, total trip time—to track its own location retaining this data in memory for navigation purposes. This type of data needs to be kept secure to protect the privacy and safety of drivers and passengers.

At the component or device level, the amount of power consumed when in operation, the timing information, electromagnetic radiation, and the sound produced by these components can be another source of information that can be exploited to perform an advanced side-channel attack and physical reverse engineering. Physical security may be employed to protect the components against such threats. For devices that can be accessed remotely, adapting software agents used in distributed real-time can facilitate secure and robust status updates for identifying cyber attacks [85].

Addressing privacy concerns in AVs has been a major topic of discussion for both the government and the automotive industry. Several measures may be taken to ensure the safety and privacy of personal information collected and stored for the vehicle operations. This includes legislation guiding the collection and use of data, data anonymization, notice and consent, differential privacy and so on.

5 Threats against V2V

Raya and Hubaux [69] present four different classifications of attackers in VANETs. These are insider vs. outsider, malicious vs. rationale, active vs. passive, and local vs. extended attackers. Insiders are the authenticated users of the network while outsiders are not. With malicious attackers, the intention is to disrupt the functionality of the network with no personal benefits while a rationale attacker seeks to gain some profits from such attack. A passive attacker monitors and eavesdrops the network activities whereas an active attacker is able to generate and send malicious packets on the network. For local attackers, they have a limited reach and can only perform their attacks within this reach while extended attackers have a wider reach scattered across the network.

V2V uses the vehicular ad-hoc network (VANET) mesh structure to communicate so each node in the network can broadcast and receive signals. VANET aimed to enable safe and efficient driving while providing support for infotainment features. Nodes in the network include the vehicles and the roadside infrastructure units. These nodes may physically move freely within the connected network coverage and communicate in single or multi-hop routing patterns. VANET is designed to ensure continuous and secure communication between all the nodes on the network. Security goals of VANET include ensuring that the source of any message is as claimed, thereby enforcing message integrity, and all the nodes should be obscured from one another and cannot be tracked to enforce privacy. Also, the network should ensure that each node is providing accurate information.

However, security concerns and challenges with VANETs can directly affect the vehicle and the infrastructure, while some attacks could also be directed at the applications using the network. These concerns present different levels of threats to the security goals of the network.

Sumra et al. [77] group the threat levels into three categories based on the confidentiality, integrity, and availability (CIA) triad, and the authors consider availability of the network resources to be at the apex and the most significant of the three levels. Attacks against availability include DOS and DDOS attacks. In the next level is the integrity of the information. The attacker's goal here is to modify the messages in the network. This compromises the integrity of the network activities, but the network services are still accessible. At the lower level are passive attacks where the adversary does not interrupt the network services, but analyzes the network activities to gain information, i.e., circumvent any confidentiality of message information. The information analyzed can be used in identifying the communicating nodes, their locations, or other key data about them.

6 Security and Privacy for V2V

A key area to focus on the security and privacy of V2I is the need for a secure public key infrastructure (PKI) [4] and the proposed security credential management scheme (SCMS) for V2V communication [1, 82]. A vehicular PKI allows each vehicle on the network to have a public-private key pair that allows it to sign messages and verify received messages by relying on a trusted certificate authority (CA) [70]. Most important, the deployment of SCMS will have profound and widespread influence not only on the security of V2V, its intended purpose, but also on the privacy of connected vehicles with respect to the SCMS infrastructure and also the security of connected cars in terms of their reliance on the correctness and inviolability of the SCMS and its constituents. An analogy may be seen in the reliance of the Internet on a secure and trustworthy PKI as the first step for establishing secure connections between two parties without using other prior information. If the PKI does not work or is compromised, for example when certificates or signing keys are stolen, then the root of trust is broken and there can be no security. Similarly, a vehicular PKI as envisioned by the SCMS, or any similar scheme used to establish authority and authenticity, is a lynchpin for secure communications in the V2I and V2V realm, including as a method to provide for secure OTA software updates.

Pseudonym-based authentication has been proposed to avoid unauthorized vehicle traceability and location privacy during communications and preserve both confidential information and privacy of the driver. A key challenge with pseudonyms is the need to refresh them to avoid overuse that can lead to linking long-term pseudonyms to true identities. A common approach to solve this challenge is to change pseudonyms frequently using an algorithm that attempts to ensure privacy while balancing the cost of replacing pseudonyms [3, 6, 30, 54]. These algorithms aim to provide location privacy for the vehicles and the users on the network. With pseudonyms, the real identity of the user is obscured, which prevents identity linking.

Another security and location privacy concealing approach makes use of group signatures. A group signature is a cryptographic primitive that allows the constituent users of a group to share the ability to sign a message on behalf of the entire group. Grouping of vehicles traveling at the same speed towards the same direction was proposed by Sampigethaya et al. [74]. The authors identified that combining neighboring vehicles into groups can reduce the number of V2I transmissions. With this approach, the vehicle will be provided with an extended silent period that enhances their anonymity in the network. Furthermore, temporary anonymous certified keys based on group signatures was presented by Studer et al. [76] to fulfill the security and privacy

management of VANETs. Here, the on-board units provide short-lived keys that are certified by the regional authority for communications. During key updates, a regional authority verifies the requesting on-board unit's validity, but do not determine its identity, thus preserving its privacy and allowing it to acquire a certificate for a temporary key. Guo et al. [34] present a group signature based scheme that relies on tamper-resistant devices for preventing adversarial attacks. This scheme allows a group member to sign messages on behalf of the group while the single public key can be used to verify the signature without revealing the identity of the signer. An important feature of group signatures is that they make it impossible to determine if two signatures have been issued by the same group member, which efficiently prevents tracking of users subject to a large enough group (i.e., the anonymity set).

K-anonymity, a scheme proposed by Sweeney [78] is another approach to deal with security and privacy risks in VANETs using the DSRC/WAVE standards. *K*-anonymity requires that an entity must be distinguishable from *k* - 1 other entities, in the results of database queries [13] i.e. a node cannot be individually identified from a group of *k* nodes on the network. Feng et. al [25] proposed a privacy-preserving model called (*k*, R, r)-anonymity that can be implemented on a mobile terminal. The main idea is to replace the physical location of users and the query target by a specific area and a set of location types, respectively. Caballero-Gil et. al [7] also proposed a revocation scheme that detects and eliminates malicious users after a number of complaints have been received while guaranteeing *k*-anonymity.

While works using differential privacy for privacy preservation in VANETs promise privacy of information [11, 37, 86, 90], additional privacy risk needs to be considered at the communication level, as well as the computation that manipulates the data [21].

7 Vehicle-to-Infrastructure (V2I) and Infrastructure-to-Vehicle (I2V) Communication

Conventional ITSs treat vehicles—and their drivers—as external agents that are monitored and measured through sensors embedded in the infrastructure. The ITS influences vehicles through physical actuation of mutable infrastructure components such as traffic lights and gates that especially are prevalent in ramp metering and traffic flow control applications. Indirect moderation of vehicle behavior is achieved by ITS through visual communication with drivers by way of programmable road signs, such as variable speed zones and congestion alerts. These visual cues require drivers to both observe and honor the warning message for effect. The arrival of V2I/I2V brings active, wireless communication links between vehicles and infrastructure that enable direct messages and the ability of an ITS to treat a vehicle as part of the system by eliciting information from it and by sending targeted warnings and messages—possibly even commands—to it. The inclusion of vehicles within the ITS represents a paradigm shift that will radically change the nature of transportation infrastructure because of the addition of V2I/I2V communication [33].

V2I/I2V is an enabler for VANET and ushers in the next generation of ITS: the era of connected vehicles [18]. Advanced applications in connected vehicles integrate live sensing data embedded in transportation infrastructure with V2I communications and Internet data sources to provide novel safety features, more efficient traffic, and delivery of digital services (i.e., infotainment) [64]. Already deployed capabilities in smart infrastructures include red light violation warning, curve speed warning, weather advisories, traffic signal change warning, congestion and detour warning for navigation planning, and more [17]. New capabilities continue to emerge on a regular basis,

and adoption by public communities is encouraged by the possible benefits of ITS [16], which include improved public safety, traffic safety, fuel and travel time efficiency, and job growth due to market expansion.

The role of V2I/I2V in emerging smart cities is to increase the data sources available for ITS by collecting from vehicles directly, provide support for VANET security and Internet-connectivity, and to close the loop by communicating feedback to vehicles and drivers [23]. Prior to the widespread adoption of wireless technology, ITS relies upon indirect collection of vehicle data using sensor measurements embedded in the infrastructure, and generates physical signals to mediate vehicle behavior, for example, metering lights and smart road signs. ITS therefore relied on widespread data collection and analysis, but without direct communication over a computer network with external agents.

Problematic to the expansion of V2I/I2V are the joint concerns of security and privacy. The security concerns of ITS in the past were readily solved by traditional network security solutions using standard cryptographic techniques. Connected car security is necessary to prevent remote exploits of moving vehicles, and infrastructure security requires rethinking in order to ensure resilient operations at all times because of new, ubiquitous communication pathways between external agents and infrastructure components. Privacy has also been a well-known concern of ITS [26], and is recognized as a key challenge since the advent of V2I [44], yet remains a significant issue in practice. Privacy is primarily of concern for vehicle drivers and passengers, but the challenges that impede privacy, and their respective solutions, exist at both ends of the vehicle-infrastructure communication channel.

8 Threats against Connected Cars due to V2I/I2V

Existing work in the area of transportation infrastructure cybersecurity focuses primarily on attacks against the infrastructure with the goal of manipulating traffic signals to indirectly influence vehicle behavior [63, 71]. The rise of V2I/I2V introduces new possibilities for attackers to target cyber attacks directly at vehicles using the infrastructure as an attack vector. This section identifies such new threats that arise due to the introduction of communication pathways between vehicles and intelligent transportation systems. Motivations for attacks and attack capabilities are described, along with the potential impacts of attacks. The focus of this section is how communicating with infrastructure opens new attack surfaces against vehicles, after which we will discuss approaches to provide security and privacy before exploring how V2I enables attacks against the infrastructure coming from the connected vehicles. We do not address here the existing attack surfaces, threats, and security solutions for automobiles that predate V2I/I2V, which, while relevant, are not facilitated by the rise of this new communication paradigm.

By itself, V2I/I2V does not introduce any new motivation for attacks, but it does expose three attack vectors relevant to compromise of the connected car:

- components of the physical *transportation infrastructure*;
- media channels and protocols of the V2I/I2V *network infrastructure*;
- *on-board computers* of the connected car that support V2I/I2V.

Adversaries capable of exploiting vulnerabilities in these attack vectors are varied, but may be broadly categorized according to their level of access, physical or remote, to the respective infrastructure. That is, the ability to access the physical or network infrastructure, or the on-board

computers of individual vehicles, may be physically under adversarial control, or the adversary may be limited to making remote accesses through, for example, manipulation of ingest data as in false data injection attacks, or through passive monitoring or eavesdropping.

Attacks coming through the physical transportation infrastructure leverage the adversaries ability to control that infrastructure. The sophistication of such an attack is therefore quite high, since the adversary must be able to first subvert components of the infrastructure. Once inside the infrastructure, however, the adversary has the advantage that V2I protocols rely on the infrastructure to be correct. Thus, some motivations for attack, namely those that aim to control, disrupt, or monitor traffic, are met without needing to compromise the connected car, and may even be feasible with remote access to the physical infrastructure. For example, ramp metering attacks that target ITS through remote or physical access [71] could accomplish similar outcomes by influencing the physical infrastructure to not just change traffic signals but to even send messages to the connected car that alter its behavior. Another example is the "Zombies ahead!" message that was presented by hacked changeable message signs [63], which may cause confusion or even panic for human drivers, while the impact of customized messages broadcast by the infrastructure to automated or semi-autonomous vehicles could be much worse.

From the adversary's perspective, the network infrastructure is perhaps the most interesting of the three new attack vectors that V2I creates, because the networks are wireless, thus easier to access both physically and remotely in comparison to the other two vectors, and the networks are ubiquitous, with connections not only to connected cars and transportation infrastructure, but also to Internet-connected computer systems, such as the servers used for public key infrastructure, databases to store the vast data collected from the transportation infrastructure, and third party service providers envisioned to support future driver and passenger demands in both the infotainment market segment and the evolution of the smart city [28].

The third attack vector of on-board computer systems is, perhaps, less enticing to attackers than the other two vectors, but must not be ignored. Of special concern for this vector is that, while traditional vehicular control systems can be isolated from remote network connections that provide infotainment and telematics, the expected development of V2I messages includes the transmission of command-and-control messages that influence the vehicle's driving behavior. In the especially concerning case of autonomous vehicles, V2I messages may even translate directly into vehicular control. Thus, the interface between the vehicle and the V2I network is an important element of the cybersecurity of connected cars to defend against external attacks. As such, the ability to provide over-the-air (OTA) updates in a secure yet prompt fashion for cybersecurity purposes will be important in the connected car.

9 Security and Privacy for Connected Cars

Security and privacy solutions proposed for connected cars generically follow traditional information security system architecture design and implementation [2, 60]. The following security mechanisms are particularly being explored in the V2I domain:

- Cryptography [29];
- Intrusion detection systems (IDS);
- Formal methods, modeling, and verification [73, 92];

- Anti-virus software [89];
- Hardware-based trusted computing [20, 45].

Novel security solutions also appear in the V2I/I2V space to counter the issues faced by the automotive domain that are not relevant in the information security space. In particular, countermeasures for vehicular theft exist for which no obvious complements are found in the traditional cybersecurity realm [47]. Similarly, the need to balance safety constraints, economic pressures, and privacy concerns with security needs sufficiently restrict the solution space such that, despite the similarity in problems and solution methods, significant work remains in addressing the challenges of automotive security.

10 Threats against Intelligent Transportation Infrastructure due to V2I/I2V

The inclusion of communication channels between connected vehicles and ITS opens new attack surfaces against the transportation infrastructure and its supporting cyber-physical system components. In this section, we identify the new threat vectors that V2I/I2V create within civil infrastructure. The motivation for attacks against ITS are essentially a subset of those for attacks against connected cars and vehicles in general:

- *infamy*;
- *control traffic* [71];
- *disrupt traffic* [63];
- *collect ISR* [40].

Note that cybersecurity for ITS has long been a concern especially for public sector agencies and the transportation profession. A lengthy yet accessible introduction to the view of cybersecurity through the lens of transportation operations management can be found in a document prepared by the Transportation Research Board [79]. Vulnerabilities in ITS have existed before the introduction of V2I/I2V, but the new communication channels introduce attack vectors through which adversaries may attempt to exploit the ITS and achieve their goals. In particular, the new attack vectors that threaten the transportation infrastructure are

- *vehicles* participating in the V2I/I2V communications;
- *networking* media and protocols of V2I/I2V;
- *added computing* (hardware and software) that supports V2I/I2V.

Perhaps the most obvious attack vector that V2I introduces is the vehicles themselves. As active participants in the ITS, malicious vehicles now can influence and attack the infrastructure itself through directed cyber attacks within the network that connects vehicles and infrastructure. Attacks against the networking layers also have precedent in the ITS prior to including vehicles in the network. For example, loop detectors embedded in the roadway to detect vehicles communicate wirelessly with a roadside unit that controls traffic signals for stoplights at intersections and in ramp metering applications. A demonstrated attack spoofs a sensor (loop detector) signal, which

allows the adversary to trick the roadside unit into altering its behavior with respect to traffic flow control [31, 88]. The inclusion of additional communication—mostly wireless—to roadside units increases their exposure to similar attacks. Even simpler attacks such as jamming are feasible and effective in achieving the disruption of traffic [22]. The inclusion of even more hardware and software within both vehicles and infrastructure to support V2I increases the attack surface of ITS, thus providing more opportunities for adversaries to launch successful cyber attacks against the computer systems themselves. Existing threat characterization for ITS considers these new threat vectors as extensions to those stemming from VANET and V2V, which are usually cast in terms of cryptographic communication security [36, 91]. A comprehensive technical report produced by ETSI identifies a broad set of threats, attacks, and countermeasures in an ITS [43].

11 Security and Privacy for Intelligent Transportation Infrastructure

Generically, the (draft) NIST Cybersecurity Framework for Critical Infrastructure [62] provides a framework to guide organizations for securing their critical infrastructure. The NIST framework adopts a risk management approach consisting of five core functions: identify, protect, detect, respond, and recover. Identify encompasses threat characterization, while protect, detect, and respond address the usual cybersecurity defensive mechanisms and incidence response deployed in (IT) security. Recover is of particular importance in critical infrastructure, because appropriate recovery ensures the resilience of the infrastructure. The NIST framework has been adopted and specialized by multiple ITS domain-specific cybersecurity policies [56].

Much of the prior work in ITS security focuses on V2V and VANET [57], or on threats to the infrastructure that come from other sources besides V2I [8, 32, 51, 53]. Much more work needs to be done in examining the threat landscape that V2I introduces against the transportation infrastructure, and then ensuring that cybersecurity approaches for ITS are resilient to attacks coming from any new attack vectors.

The impact on privacy caused by integration of V2I and ITS also has received quite a bit of attention. Cottrill [14] examines the problem and solution space for privacy concerns with respect to the emerging V2I-ITS integration. Glancy [33] discusses, among other topics, the legal and policy issues caused by V2I/I2V including privacy concerns and security challenges. Privacy is also a repeated theme of concern in the proposed rules for V2V communications especially as they rely on PKI and network infrastructure [1]. Lederman et al. [52] survey privacy protections in ITS and propose solutions for privacy protection in ITS data collection and storage.

12 Conclusions and Future Work

As the boundary line blurs between vehicle, network, and transportation infrastructure, the security and privacy concerns of all the entities involved in modern transportation will continue to grow in importance. In this chapter, we have dissected how advancements made in autonomy, inter-vehicle connectivity, and vehicle-infrastructure integration are impacting the security and privacy of vehicle and transportation infrastructure computing systems. None of the concerns in any of these areas are solved, and much work remains to be done especially in the emerging domains of V2I and autonomous vehicles. Privacy also is under-investigated in the research community, despite being valued by the consumer, and solutions to protect privacy could have high impact on the adoption rate and long-term viability of automotive and transportation technology that enables smart cities. As the standards and regulations for vehicular technology change in response to autonomy

and ubiquitous connectivity, so too must the security and privacy research community continue to identify problems and propose preventive, reactive, and responsive solutions that are amenable to public use and policy-making. Security and privacy of vehicles and transportation critical infrastructure are not just technical problems, but they are also social and international, multi-cultural problems for which the solutions must meet the security and privacy requirements while also being responsive to human socio-economic and cross-cultural needs while satisfying the cyber-physical system safety constraints. The complexity of this problem space ensures that it will remain an active and viable research area for years to come, and that the fundamental problems will persist. Therefore, an important future research direction is on how to evaluate proposed solutions for security and privacy to meet the above constraints and also address the fundamental problems. Another area that merit further investigation is building security into the entire components of the automobile used for communication and determine how to maintain that level of security through the entire lifecycle of the components by remote updates and other security measures.

Acknowledgments

This material is based upon work supported by the National Science Foundation under Grant No. CNS-1646317 and the U.S. Department of Homeland Security under Grant Award Number 2017-ST-062-000003. 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 and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security.

References

[1] 82 FR 3854 - FEDERAL MOTOR VEHICLE SAFETY STANDARDS; V2v COMMUNICATIONS. *Federal Register*, 82(8):3854–4019, January 2017.

[2] Eslam G. AbdAllah, Mohammad Zulkernine, Yuan Xiang Gu, and Clifford Liem. Towards Defending Connected Vehicles Against Attacks. In *Proceedings of the Fifth European Conference on the Engineering of Computer-Based Systems*, ECBS '17, pages 9:1–9:9, New York, NY, USA, 2017. ACM.

[3] Adetundji Adigun, Boucif Amar Bensaber, and Ismail Biskri. Protocol of change pseudonyms for vanets. In *Local Computer Networks Workshops (LCN Workshops), 2013 IEEE 38th Conference on*, pages 162–167. IEEE, 2013.

[4] Nikolaos Alexiou, Marcello Laganà, Stylianos Gisdakis, Mohammad Khodaei, and Panagiotis Papadimitratos. Vespa: Vehicular security and privacy-preserving architecture. In *Proceedings of the 2nd ACM workshop on Hot topics on wireless network security and privacy*, pages 19–24. ACM, 2013.

[5] Jennifer Ann Bruton. Securing CAN bus communication: An analysis of cryptographic approaches. *M. Sc., National University of Ireland, Galway*, 2014.

[6] Levente Buttyán, Tamás Holczer, and István Vajda. On the effectiveness of changing pseudonyms to provide location privacy in vanets. In *European Workshop on Security in Ad-hoc and Sensor Networks*, pages 129–141. Springer, 2007.

[7] Cándido Caballero-Gil, Jezabel Molina-Gil, Juan Hernández-Serrano, Olga León, and Miguel Soriano-Ibanez. Providing k-anonymity and revocation in ubiquitous vanets. *Ad Hoc Networks*, 36:482–494, 2016.

[8] E. S. Canepa and C. G. Claudel. Spoofing cyber attack detection in probe-based traffic monitoring systems using mixed integer linear programming. In *2013 International Conference on Computing, Networking and Communications (ICNC)*, pages 327–333, January 2013.

[9] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. Comprehensive Experimental Analyses of Automotive Attack Surfaces. In *Proceedings of the 20th USENIX Conference on Security*, SEC'11, pages 6–6, Berkeley, CA, USA, 2011. USENIX Association.

[10] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, Tadayoshi Kohno, et al. Comprehensive experimental analyses of automotive attack surfaces. In *USENIX Security Symposium*. San Francisco, 2011.

[11] Chang-Wu Chen, Sang-Yoon Chang, Yih-Chun Hu, and Yen-Wen Chen. Protecting vehicular networks privacy in the presence of a single adversarial authority. In *Communications and Network Security (CNS), 2017 IEEE Conference on*, pages 1–9. IEEE, 2017.

[12] CAMP VSC Consortium et al. Vehicle safety communications project–final report. *NHTSA Publication DOT HS*, 810:591, 2006.

[13] George P Corser, Huirong Fu, and Abdelnasser Banihani. Evaluating location privacy in vehicular communications and applications. *IEEE transactions on intelligent transportation systems*, 17(9):2658–2667, 2016.

[14] Caitlin Cottrill. Approaches to privacy preservation in intelligent transportation systems and vehicle-infrastructure integration initiative. *Transportation Research Record: Journal of the Transportation Research Board*, (2129):9–15, 2009.

[15] Nicolas T. Courtois, Gregory V. Bard, and David Wagner. Algebraic and Slide Attacks on KeeLoq. In *Fast Software Encryption*, Lecture Notes in Computer Science, pages 97–115. Springer, Berlin, Heidelberg, February 2008.

[16] Kashif Dar, Mohamed Bakhouya, Jaafar Gaber, Maxime Wack, and Pascal Lorenz. Wireless communication technologies for its applications [topics in automotive networking]. *IEEE Communications Magazine*, 48(5):156–162, 2010.

[17] US Department of Transportation. Intelligent Transportation Systems - CV Pilot Deployment Program. https://www.its.dot.gov/pilots/cv_pilot_apps.htm.

[18] Kakan Chandra Dey, Anjan Rayamajhi, Mashrur Chowdhury, Parth Bhavsar, and James Martin. Vehicle-to-vehicle (v2v) and vehicle-to-infrastructure (v2i) communication in a heterogeneous wireless network–performance evaluation. *Transportation Research Part C: Emerging Technologies*, 68:168–184, 2016.

[19] Udaya Suriya Raj Kumar Dhamodharan and Rajamani Vayanaperumal. Detecting and preventing sybil attacks in wireless sensor networks using message authentication and passing method. *The Scientific World Journal*, 2015, 2015.

[20] Sastry Duri, Marco Gruteser, Xuan Liu, Paul Moskowitz, Ronald Perez, Moninder Singh, and Jung-Mu Tang. Framework for Security and Privacy in Automotive Telematics. In *Proceedings of the 2Nd International Workshop on Mobile Commerce*, WMC '02, pages 25–32, New York, NY, USA, 2002. ACM.

[21] Cynthia Dwork and George J Pappas. Privacy in information-rich intelligent infrastructure. *arXiv preprint arXiv:1706.01985*, 2017.

[22] Nnanna Ekedebe, Wei Yu, Houbing Song, and Chao Lu. On a simulation study of cyber attacks on vehicle-to-infrastructure communication (V2i) in Intelligent Transportation System (ITS). volume 9497, page 94970B. International Society for Optics and Photonics, May 2015.

[23] Miad Faezipour, Mehrdad Nourani, Adnan Saeed, and Sateesh Addepalli. Progress and challenges in intelligent vehicle area networks. *Communications of the ACM*, 55(2):90–100, 2012.

[24] Wael A Farag. CANTrack: Enhancing automotive CAN bus security using intuitive encryption algorithms. In *Modeling, Simulation, and Applied Optimization (ICMSAO), 2017 7th International Conference on*, pages 1–5. IEEE, 2017.

[25] Yunxia Feng, Xu Li, and Bo Song. (k, r, r)-anonymity: a light-weight and personalized location protection model for lbs query. In *Proceedings of the ACM Turing 50th Celebration Conference-China*, page 29. ACM, 2017.

[26] Simson L. Garfinkel. Why driver privacy must be a part of ITS. In Lewis M. Branscomb and James Keller, editors, *Converging Infrastructures: Intelligent Transportation and the National Information Infrastructure*, pages 324–340. MIT Press, Cambridge, MA, USA, 1996.

[27] Mevlut Turker Garip, Mehmet Emre Gursoy, Peter Reiher, and Mario Gerla. Congestion attacks to autonomous cars using vehicular botnets. In *NDSS Workshop on Security of Emerging Networking Technologies (SENT)*, 2015.

[28] Mario Gerla, Eun-Kyu Lee, Giovanni Pau, and Uichin Lee. Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds. In *Internet of Things (WF-IoT), 2014 IEEE World Forum on*, pages 241–246. IEEE, 2014.

[29] Matthias Gerlach, Andreas Festag, Tim Leinmüller, Gabriele Goldacker, and Charles Harsch. Security architecture for vehicular communication. In *Workshop on Intelligent Transportation*, 2007.

[30] Matthias Gerlach and Felix Guttler. Privacy in vanets using changing pseudonyms-ideal and real. In *Vehicular Technology Conference, 2007. VTC2007-Spring. IEEE 65th*, pages 2521–2525. IEEE, 2007.

[31] A. Ghafouri, W. Abbas, Y. Vorobeychik, and X. Koutsoukos. Vulnerability of fixed-time control of signalized intersections to cyber-tampering. In *2016 Resilience Week (RWS)*, pages 130–135, August 2016.

[32] Branden Ghena, William Beyer, Allen Hillaker, Jonathan Pevarnek, and J. Alex Halderman. Green Lights Forever: Analyzing the Security of Traffic Infrastructure. In *8th USENIX Workshop on Offensive Technologies (WOOT 14)*, San Diego, CA, 2014. USENIX Association.

[33] Dorothy J Glancy. Sharing the road: Smart transportation infrastructure. *Fordham Urb. LJ*, 41:1617, 2013.

[34] Jinhua Guo, John P Baugh, and Shengquan Wang. A group signature based secure and privacy-preserving vehicular communication framework. In *2007 Mobile Networking for Vehicular Environments*, pages 103–108. IEEE, 2007.

[35] Mohammad Hamad, Marcus Nolte, and Vassilis Prevelakis. Towards comprehensive threat modeling for vehicles. In *the 1st Workshop on Security and Dependability of Critical Embedded Real-Time Systems*, page 31, 2016.

[36] Elyes Ben Hamida, Hassan Noura, and Wassim Znaidi. Security of cooperative intelligent transport systems: Standards, threats analysis and cryptographic countermeasures. *Electronics*, 4(3):380–423, 2015.

[37] Meng Han, Zhuojun Duan, and Yingshu Li. Privacy issues for transportation cyber physical systems. In *Secure and Trustworthy Transportation Cyber-Physical Systems*, pages 67–86. Springer, 2017.

[38] John Harding, Gregory Powell, Rebecca Yoon, Joshua Fikentscher, Charlene Doyle, Dana Sade, Mike Lukuc, Jim Simons, and Jing Wang. Vehicle-to-vehicle communications: Readiness of v2v technology for application. Technical report, 2014.

[39] Halabi Hasbullah, Irshad Ahmed Soomro, et al. Denial of service (dos) attack and its possible solutions in vanet. *World Academy of Science, Engineering and Technology, International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering*, 4(5):813–817, 2010.

[40] Kashmir Hill. 'God View': Uber Allegedly Stalked Users For Party-Goers' Viewing Pleasure (Updated).

[41] Tobias Hoppe, Stefan Kiltz, and Jana Dittmann. Security threats to automotive CAN networks-practical examples and selected short-term countermeasures. *Reliability Engineering and System Safety*, 96(1):11 – 25, 2011. Special Issue on Safecomp 2008.

[42] Ling Huang, Anthony D Joseph, Blaine Nelson, Benjamin IP Rubinstein, and JD Tygar. Adversarial machine learning. In *Proceedings of the 4th ACM workshop on Security and artificial intelligence*, pages 43–58. ACM, 2011.

[43] European Telecommunications Standards Institute. Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA). Technical Report ETSI TR 102 893, France, 2010.

[44] Leslie Jacobson. VII Privacy Policies Framework, Version 1.0.2. Technical report, The Institutional Issues Subcommittee of the National VII Coalition, 2007.

[45] F. Kargl, P. Papadimitratos, L. Buttyan, M. Müter, E. Schoch, B. Wiedersheim, T. V. Thong, G. Calandriello, A. Held, A. Kung, and J. P. Hubaux. Secure vehicular communication systems: implementation, performance, and research challenges. *IEEE Communications Magazine*, 46(11):110–118, November 2008.

[46] John B Kenney. Dedicated short-range communications (dsrc) standards in the united states. *Proceedings of the IEEE*, 99(7):1162–1182, 2011.

[47] P. Knapik, E. Schoch, and F. Kargl. Electronic Decal: A Security Function Based on V2x Communication. In *2013 IEEE 77th Vehicular Technology Conference (VTC Spring)*, pages 1–5, June 2013.

[48] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, et al. Experimental security analysis of a modern automobile. In *Security and Privacy (SP), 2010 IEEE Symposium on*, pages 447–462. IEEE, 2010.

[49] Alexey Kurakin, Ian Goodfellow, and Samy Bengio. Adversarial machine learning at scale. *arXiv preprint arXiv:1611.01236*, 2016.

[50] U. E. Larson, D. K. Nilsson, and E. Jonsson. An approach to specification-based attack detection for in-vehicle networks. In *2008 IEEE Intelligent Vehicles Symposium*, pages 220–225, June 2008.

[51] A. Laszka, B. Potteiger, Y. Vorobeychik, S. Amin, and X. Koutsoukos. Vulnerability of Transportation Networks to Traffic-Signal Tampering. In *2016 ACM/IEEE 7th International Conference on Cyber-Physical Systems (ICCPS)*, pages 1–10, April 2016.

[52] Jaimee Lederman, Brian D. Taylor, and Mark Garrett. A private matter: the implications of privacy regulations for intelligent transportation systems. *Transportation Planning and Technology*, 39(2):115–135, February 2016.

[53] Z. Li, D. Jin, C. Hannon, M. Shahidehpour, and J. Wang. Assessing and mitigating cybersecurity risks of traffic light systems in smart cities. *IET Cyber-Physical Systems: Theory Applications*, 1(1):60–69, 2016.

[54] Rongxing Lu, Xiaodong Lin, Tom H Luan, Xiaohui Liang, and Xuemin Shen. Pseudonym changing at social spots: An effective strategy for location privacy in vanets. *IEEE Transactions on Vehicular Technology*, 61(1):86–96, 2012.

[55] Aleksander Madry, Aleksandar Makelov, Ludwig Schmidt, Dimitris Tsipras, and Adrian Vladu. Towards deep learning models resistant to adversarial attacks. *arXiv preprint arXiv:1706.06083*, 2017.

[56] Marisa C. Ramon and Daniel A. Zajac. Cybersecurity Literature Review and Efforts Report. http://onlinepubs.trb.org/onlinepubs/nchrp/docs/NCHRP03-127_Cybersecurity_Literature_Review.pdf, January 2018.

[57] Mohamed Nidhal Mejri, Jalel Ben-Othman, and Mohamed Hamdi. Survey on vanet security challenges and possible cryptographic solutions. *Vehicular Communications*, 1(2):53–66, 2014.

[58] C. Miller and C. Valasek. Remote exploitation of an unaltered passenger vehicle. BlackHat USA, 2015.

[59] Charlie Miller and Chris Valasek. Adventures in automotive networks and control units. *DEF CON*, 21:260–264, 2013.

[60] R. Moalla, B. Lonc, H. Labiod, and N. Simoni. Towards a Cooperative ITS Vehicle Application Oriented Security Framework. In *2014 IEEE Intelligent Vehicles Symposium Proceedings*, pages 1043–1048, June 2014.

[61] Michael Müter and Naim Asaj. Entropy-based anomaly detection for in-vehicle networks. In *Intelligent Vehicles Symposium (IV), 2011 IEEE*, pages 1110–1115. IEEE, 2011.

[62] NIST. Cybersecurity Framework. https://www.nist.gov/cyberframework.

[63] Jennie Olofsson. 'Zombies ahead!' A study of how hacked digital road signs destabilize the physical space of roadways. *Visual Communication*, 13(1):75–93, February 2014.

[64] Panos Papadimitratos, Arnaud De La Fortelle, Knut Evenssen, Roberto Brignolo, and Stefano Cosenza. Vehicular communication systems: Enabling technologies, applications, and future outlook on intelligent transportation. *IEEE Communications Magazine*, 47(11), 2009.

[65] Nicolas Papernot, Patrick McDaniel, Ian Goodfellow, Somesh Jha, Z Berkay Celik, and Ananthram Swami. Practical black-box attacks against deep learning systems using adversarial examples. *arXiv preprint*, 2016.

[66] Nicolas Papernot, Patrick McDaniel, Xi Wu, Somesh Jha, and Ananthram Swami. Distillation as a defense to adversarial perturbations against deep neural networks. In *Security and Privacy (SP), 2016 IEEE Symposium on*, pages 582–597. IEEE, 2016.

[67] Patrick Pype, Gerardo Daalderop, Eva Schulz-Kamm, Eckhard Walters, and Maximilian von Grafenstein. Privacy and security in autonomous vehicles. In *Automated Driving*, pages 17–27. Springer, 2017.

[68] Ajay Rawat, Santosh Sharma, and Rama Sushil. Vanet: Security attacks and its possible solutions. *Journal of Information and Operations Management*, 3(1):301, 2012.

[69] Maxim Raya and Jean-Pierre Hubaux. Securing vehicular ad hoc networks. *Journal of Computer Security*, 15(1):39–68, 2007.

[70] Maxim Raya, Panos Papadimitratos, and Jean-Pierre Hubaux. Securing vehicular communications. *IEEE wireless communications*, 13(5), 2006.

[71] Jack Reilly, Sébastien Martin, Mathias Payer, and Alexandre M. Bayen. Creating complex congestion patterns via multi-objective optimal freeway traffic control with application to cybersecurity. *Transportation Research Part B: Methodological*, 91:366–382, September 2016.

[72] Randy Roebuck. Dsrc technology and the dsrc industry consortium (dic) prototype team. *prepared by SIRIT Technologies for ARINDC/US DOT*, 28, 2005.

[73] F. Sagstetter, M. Lukasiewycz, S. Steinhorst, M. Wolf, A. Bouard, W. R. Harris, S. Jha, T. Peyrin, A. Poschmann, and S. Chakraborty. Security challenges in automotive hardware/software architecture design. In *2013 Design, Automation Test in Europe Conference Exhibition (DATE)*, pages 458–463, March 2013.

[74] Krishna Sampigethaya, Leping Huang, Mingyan Li, Radha Poovendran, Kanta Matsuura, and Kaoru Sezaki. Caravan: Providing location privacy for vanet. Technical report, Washington Univ Seattle Dept Of Electrical Engineering, 2005.

[75] H. M. Song, H. R. Kim, and H. K. Kim. Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network. In *2016 International Conference on Information Networking (ICOIN)*, pages 63–68, Jan 2016.

[76] Ahren Studer, Elaine Shi, Fan Bai, and Adrian Perrig. TACKing together efficient authentication, revocation, and privacy in vanets. In *Sensor, Mesh and Ad Hoc Communications and Networks, 2009. SECON'09. 6th Annual IEEE Communications Society Conference on*, pages 1–9. IEEE, 2009.

[77] Irshad Ahmed Sumra, Halabi Bin Hasbullah, and Jamalul-lail Bin AbManan. Attacks on security goals (confidentiality, integrity, availability) in vanet: a survey. In *Vehicular Ad-Hoc Networks for Smart Cities*, pages 51–61. Springer, 2015.

[78] Latanya Sweeney. k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(05):557–570, 2002.

[79] Transportation Research Board and National Academies of Sciences, Engineering, and Medicine. *Protection of Transportation Infrastructure from Cyber Attacks: A Primer*. The National Academies Press, Washington, DC, 2016. DOI: 10.17226/23520.

[80] Hiroshi Ueda, Ryo Kurachi, Hiroaki Takada, Tomohiro Mizutani, Masayuki Inoue, and Satoshi Horihata. Security authentication system for in-vehicle network. *SEI Technical Review*, (81), 2015.

[81] Cybersecurity Ventures. *Cybercrime Report*, 2017 (accessed January 31, 2018). `https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/`.

[82] W. Whyte, A. Weimerskirch, V. Kumar, and T. Hehn. A security credential management system for V2V communications. In *2013 IEEE Vehicular Networking Conference*, pages 1–8, December 2013.

[83] Marko Wolf, André Weimerskirch, and Christof Paar. Security in automotive bus systems. In *Workshop on Embedded Security in Cars*, 2004.

[84] S. Woo, H. J. Jo, and D. H. Lee. A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN. *IEEE Transactions on Intelligent Transportation Systems*, 16(2):993–1006, April 2015.

[85] Eray Yağdereli, Cemal Gemci, and A Ziya Aktaş. A study on cyber-security of autonomous and unmanned vehicles. *The Journal of Defense Modeling and Simulation*, 12(4):369–381, 2015.

[86] Wei-Dong Yang, Ze-Ming Gao, Ke Wang, and Hong-Yue Liu. A privacy-preserving data aggregation mechanism for vanets. *Journal of High Speed Networks*, 22(3):223–230, 2016.

[87] Clinton Young, Joseph Zambreno, and Gedare Bloom. Towards a fail-operational intrusion detection system for in-vehicle networks. *Proceedings of the Workshop on Security and Dependability of Critical Embedded Real-Time Systems (CERTS)*, Nov 2016.

[88] Kim Zetter. Hackers Can Mess With Traffic Lights to Jam Roads and Reroute Cars, April 2014.

[89] T. Zhang, H. Antunes, and S. Aggarwal. Defending Connected Vehicles Against Malware: Challenges and a Solution Framework. *IEEE Internet of Things Journal*, 1(1):10–21, February 2014.

[90] Tao Zhang and Quanyan Zhu. Distributed privacy-preserving collaborative intrusion detection systems for vanets. *IEEE Transactions on Signal and Information Processing over Networks*, 4(1):148–161, 2018.

[91] Meiyuan Zhao, Jesse Walker, and Chieh-Chih Wang. Security Challenges for the Intelligent Transportation System. In *Proceedings of the First International Conference on Security of Internet of Things*, SecurIT '12, pages 107–115, New York, NY, USA, 2012. ACM.

[92] Bowen Zheng, Wenchao Li, Peng Deng, Léonard Gérard, Qi Zhu, and Natarajan Shankar. Design and Verification for Transportation System Security. In *Proceedings of the 52Nd Annual Design Automation Conference*, DAC '15, pages 96:1–96:6, New York, NY, USA, 2015. ACM.