Chapter 1
Introduction to Automotive Cybersecurity

1.1 Overview

This chapter gives a brief description of the main topics of the book in automotive cybersecurity. The automotive industry, which comprises many companies and organizations, is one of the leading industries in the world as it is more aware of its environment and responds to it. The history of intelligent autonomous vehicles has improved more than two decades before. Ever since, the automotive industry has made a big transformation to ensure efficiency and safety by eliminating traffic accidents for both the drivers and passengers. The technological progress made in sensor and navigation systems, the Internet of Things, and different types of machine learning techniques would promote new, innovative, and accessible mobility that gives rise to intelligent and autonomous vehicles. However, security plays a vital role in intelligent and autonomous vehicles. In this book, we discuss in detail about the different levels of autonomous vehicles from Level 0 to Level 4, different types of cybersecurity issues in autonomous vehicles, and future trends and challenges in autonomous vehicles. Security must be thought as an important aspect during designing and implementation of the autonomous vehicles to prevent from numerous security threats and attacks. The purpose of this chapter is to provide a comprehensive overview of automotive connectivity and to provide a framework for discussion of the several challenges and issues related to automotive connectivity, security from a technical perspective.

We will begin with basic cybersecurity terms, its impact in autonomous vehicles, security goals, threats, and challenges. We show how a ransomware attack can affect the cybersecurity of the vehicle. We then provide a detailed overview of the autonomous and intelligent vehicle communication, i.e., in-vehicle and inter-vehicle communications and the related cybersecurity issues.

S. Kim and R. Shrestha, *Automotive Cyber Security*,
https://doi.org/10.1007/978-981-15-8053-6_1

1.2 Introduction

The term security refers to the protection of critical assets of the system from malicious threats and mitigation of their impact on the system. The assets can be any valuable object or entity or an organization. These assets can have certain vulnerability, which can be exploited by malicious users or attackers for their own benefits. The malicious threats are generated by malicious users or intruders, which exploits the system's vulnerability, and access or modify the critical assets of the system. These malicious users can be an individual person or group of people or software, whose aim is to find a vulnerability or weak points in the system and attack at that point to collapse, harm, or just to gain access to the system. The security assets are the resources of the system that need to be protected against malicious threats and attacks. The security assets with its environment refer to the security context. If the security environment responds friendly, then it adds for security assets and vice versa.

1.2.1 Security and Its Impact

The automotive industry is experiencing massive changes as well as gaining huge opportunities. The automotive industry is dealing with new technologies and autonomous vehicle concepts that have the potential to turn the vehicle itself into the autonomous computerized moving device. There can be various cyber security mechanisms to provide security, and each security mechanism can have single or multiple impacts on the assets to be protected. A security mechanism can level-up the security for various assets or for all assets in the system's environment context. The security mechanism may be powerful for a limited period of time or impact in such a way that there is a trade-off among assets. The cybersecurity ensures safe access to hardware and protects damage to data during network access data injection and code injection. The cybersecurity is growing as the communication level is advancing extending from big computers to very small devices being a part of the Internet of Things (IoT) [1]. Some security mechanism can have no impact on the assets or may be some time negatively affects the system's assets. Some of the terminology used in security fields includes security objective, security mechanism, threats, vulnerabilities and attacks, defense, risk, policy, assurance, resilience, and countermeasure. The security goal is to provide safety measures to achieve the confidentiality, integrity, and availability (CIA) triad for protection of the overall system along with its peripherals. The triad CIA is as follows:

- Confidentiality: The aim of confidentiality is to protect the critical information from unauthorized users. Confidentiality for network security ensures that the critical assets are accessible only to authorize users.
- Integrity: This ensures that unauthorized users do not modify or manipulate the data or information during their network transmission.

- Availability: The availability is the last component of the CIA triad that represents the real availability of our information. Authentication methods, channel access, and systems all have to function efficiently to prevent the data and make sure that it is available when required. In short, the availability aims to ensure that data and network resources are available when requested by the authorized users.

Besides the CIA triad, authentication, authorization, and accountability (AAA) also play an important role for controlling the access to the system resources, policy enforcement, auditing, etc. The AAA is a term for controlling the access to the system resources, auditing usage, enforcing policies, and offering the details need to charge for services.

- Authentication: In general, authentication is about personal identification information. It contains the incoming request validation mechanism against certain identification credentials.
- Authorization: Authorization means that the user has the approval or privilege to perform a specific operation. Typically, the authorization process takes place after the successful authentication.
- Accountability: Accountability is the third component of the AAA framework. It provides administrators the ability to monitor the activities that users have conducted in a given situation. It is a primary way of evaluating what services have been used and how much resources users have consumed. Accountability is generally enforced by conducting audits, as well as setting up systems for making and maintaining audit trails.

- **Vulnerabilities and Attacks**

The wireless networks are more vulnerable and prone to different types of attacks as compared to the wired networks because any attacker can easily connect to an unsecure switch port without establishing any physical connection to the device. Unauthorized access is the most common vulnerability in wired and wireless networks. There is a tremendous amount of vulnerabilities in the network, and the transmission data is enormously vulnerable to attacks. Any network is attacked first by acquiring the communication channel, then obtaining data and then using the data for some malicious purposes. The network security targets for securing not only the end devices, but also the entire network and end-to-end connectivity. Other vulnerabilities that can take place after unauthorized access are as follows:

- Sniffing the data packet during its transfer to capture critical information.
- The network channel is overloaded with unauthentic data in order to subject denial of service to authentic users on a network.
- The MAC addresses of authentic hosts are spoofed to capture data and induce man-in-the-middle attack.

1.3 Cyber Security in Automotive Technology

Every year, there are huge developments of novel automotive applications and services that are leading the production in terms of cost and technology. More than 90% of automotive inventions lead to innovations in vehicle hardware and software. Hardware in the vehicles has control system, which directs the vehicles to perform various tasks on the roads while driving. Some basic tasks are listed below:

- Primary systems of the vehicles, e.g., the engine, driver assistance, driveline, electric system, brake system, dashboard, etc.
- Secondary vehicles systems, e.g., ignition, indicators, window control, wipers, lights
- Infotainment applications, e.g., navigation systems, telematics, rear seat entertainment, music and video entertainment, and GPS-based services.

Modern advancements in electrical and electronics have dramatically changed the automotive industry. These vehicles are no more completely mechanical systems after the intervention of electronics. In addition, these electronic devices have added a set of unimaginable features, improving the overall performance of the vehicles.

Nowadays, vehicles are faster, more sophisticated, new functionalities, and more efficient. These advancements result from dozens of electronic control units (ECUs) and vast communication network interconnecting them and enabling a whole new driving experience: from vehicles that can be remotely locked and unlocked, to vehicles that can be driven without a key in the ignition and can even drive or park themselves. This new driving experience is achieved by using hundreds of megabytes of code contained in the vehicle's ECUs. One can find Google's driverless vehicles driving themselves in Nevada, and they are also allowed in Florida and California. So it is just a matter of time until we will see more autonomous and smart vehicles all around the globe, probably raising driving safety; however, what about the security aspects?

Because of the current advancement in technologies, it is possible to deploy them to create numerous safety devices and protocols for the vehicles such as automatic emergency braking, forward collision warning, vehicle-to-vehicle communications, and soon fully automated vehicles. Considering that these innovations have great potential in them, vehicle manufacturers and transport authorities are attempting to improvise secure tools to protect these technologies from new challenges, relating primarily to cyberattacks.

As the vehicular systems become more advanced, the possibility of cyber attacks on these systems is increasing alongside. There is a need of applying cybersecurity principles at various components of the vehicles to govern safety, security, and protection from any kind of malicious attacks, damage, illegitimate access, or something, from cyber attacks, which may compromise the safety of the vehicle or the driver. The timeline of automotive cybersecurity history is given in Fig. 1.1 [2].

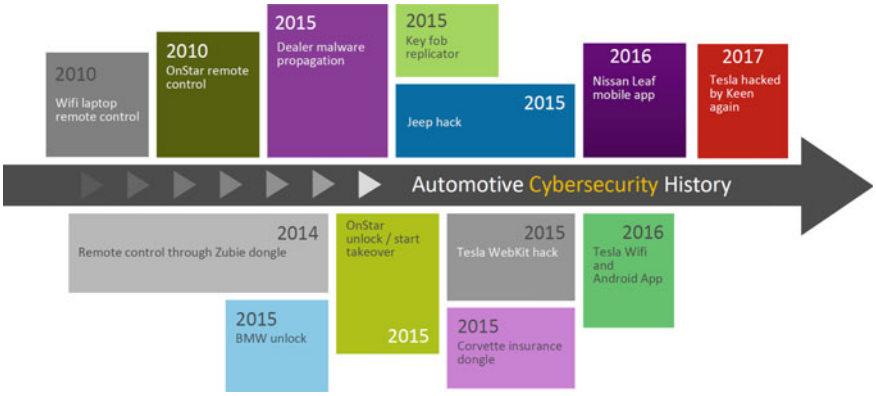

Fig. 1.1 Automotive cybersecurity history timeline

1.3.1 The Rising Threat

As mentioned above, as vehicles are getting more advanced, they use computers to control decisive operations such as brakes, stability control, and airbags functionality. Vehicles become safer on one hand, but on the other hand, the safety mechanisms are controlled by the ECUs, adding more complexity and potential attack vectors to the system. These ECUs are interconnected through a CAN bus in an unsecured way. The notion of merely securing ECUs in individual systems is inadequate in the connected and autonomous vehicle situation. There are several forms of networking such as Ethernet, cellular, Internet, Wi-Fi, Bluetooth, and V2X connected in the vehicle and linking to various networks like controller area network (CAN) bus, Ethernet that are running applications on peripherals (USB, display, sensor, LiDAR, etc.).

CAN bus is an old protocol that was introduced in the 1986, which was not designed according to security guidelines; the messages which are being sent contain an ID, their length, and the payload itself, thus message receiver does not know who the sender is and whether the message is legal. The priorities of the messages are also inferred from the message IDs, thus allowing any component connected to the bus, the ability to send high priority messages, and flooding the bus and other components.

Currently, cybersecurity problems are getting even worse. The vehicles may be remotely hacked or immobilized. Vehicles can be compromised through the wireless sensors in the vehicles, and person can be hurt physically if someone gets hold of the CAN bus and stops the vehicle suddenly through one of the external interfaces of the vehicle. Even luxury vehicles such as the Jaguar suffered from flaws, causing "blue screen of death" immobilizing them.

The weakness in several vehicle assessments is seen as extremely vulnerable security architecture with a significant number of powerful computers with wireless access such as GPS, NFC, Bluetooth, cellular, IR, Wi-Fi, etc. Taking control over

such a wireless system can lead to full control over messages, which are being sent over the bus, thus entirely compromising the vehicle.

A surge of cyber attacks has recently been on the rise and has been targeting the vehicles all over the world. There is no reason to think that these machines are not part of the game because we know that they are the computers we are driving.

One might wonder why anybody would hack a car. The motive may vary, from the theft of vehicles and theft of personal information to extortion, harming the reputation of companies or even homicide or terrorism.

1.4 Vehicular Ransomware Attack

This section describes the procedure for performing a vehicular ransomware attack based on [3].

1.4.1 Vehicle Ransomware Attack Scheme

A representative ransomware attack technique is explained below as shown in Fig. 1.2.

The cyber attacker represented by (3) uses the ransom control software (5, i.e., "bot master"), distributes (c) the ransom malware (2) to their target extortion vehicles (11), behind an anonymous botnet (4), applying TOR technology as an example. The cyber attacker could then attempt (b) to insert the ransomware explicitly (c2) or implicitly (c1) over any wireless (6a) or wired network (6b) that could enter the target vehicles. When the malware enters a potential target vehicle, it utilizes the primary

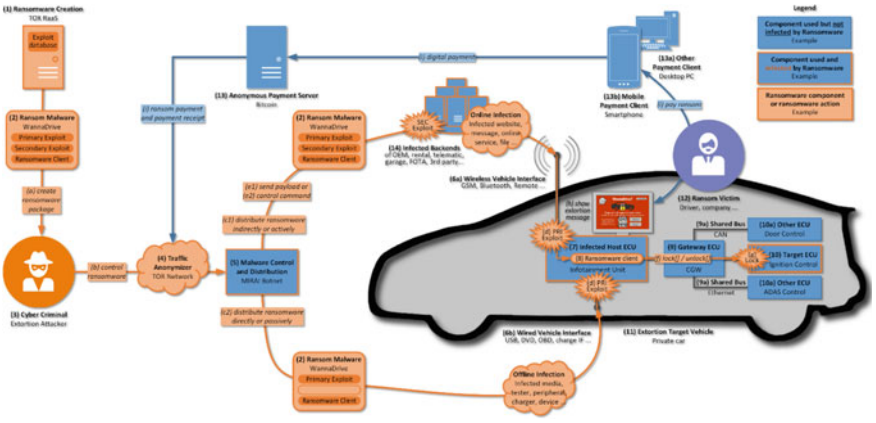

Fig. 1.2 Ransomeware attack scheme in vehicles Adapted from [2]

security exploit (d) of the integrated vehicle to install and deploy the ransomware client (8) on a central, well-connected in-vehicle device (7), like the infotainment unit, misusing it as a host for its further attack. From here, the ransomware client may either initially create an online connectivity back to the attacker to receive additional data ("payload") and/or more commands (e) or directly communicate (f) to a crucial target ECU like ignition control (10) via in-vehicle bus systems (9a) to execute the real onboard locking operation (g) to extortion payment from the ransom victim (12). Then, the ransomware will show the extortion message (h) and demand payment of the associated ransom. When the victim has paid the ransom (i) using an anonymous payment system (13) such as Bitcoin, the attacker would again contact his ransomware using his anonymous botnet (e2) to perform the unlocking command (f) required to free the vehicle (if feasible).

It shows that ransomware for vehicles can be developed and injected, indicating that this ransomware attack on vehicles is real and serious. As the cars are more interconnected and as digital technology begins to provide even more essential vehicle technologies and as vehicle digital technology becomes more standardized, the attack surfaces for ransomware will grow, and the value that ransomware may take hostage will increase. The community that can attack a single type of ransomware will increase.

1.5 Overview of Topics

The number of connected vehicles is growing rapidly with escalating computing and storage resources being provided for vehicles worldwide. The digital transformation of the vehicles combined with various other technologies results in connected, intelligent, and autonomous vehicles also known as self-driving vehicles and automotive cybersecurity. This book provides a comprehensive overview of automotive cyber security and framework for several issues related to connected, intelligent, and autonomous vehicles. The chapters in this book give the reader essential knowledge related to vehicular communication technologies, cyber security, vehicle embedded system securities, standards, challenges, autonomous vehicle use cases, and future trends. The chapters are as follows:

1. Introduction to Automotive Cybersecurity
2. Intelligent and Autonomous Vehicle
3. Cybersecurity and Privacy in Intelligent Autonomous Vehicles
4. In-vehicle Communication and Cyber Security
5. AUTOSAR Embedded Security in Vehicles
6. Inter-vehicle Communication and Cyber Security
7. Internet of Vehicles, Vehicular Social Networks, and Cyber Security
8. V2X Current Security Issues, Standards, Challenges, Use cases, and Future Trends

We will briefly introduce the contents of each chapter hereafter.

1.5.1. In (Chap. 2), the history and evolution of intelligent and autonomous vehicle outlook are provided. It provides a detailed overview of the of intelligent and autonomous vehicle development timeline since 1920s. It provides the classification of autonomous vehicles based on vehicle driving levels, associations between connectivity and autonomy for vehicle performance, and the state-of-the art applications. The intelligent and autonomous vehicle is the next-generation self-driving vehicle equipped with different types of advanced sensors, actuators, controllers incorporated with intelligence (e.g., machine learning techniques), and cooperative driving capability to guarantee autonomy, safety, protection, ease, and energy efficient. In Chap. 2, the in-vehicle technologies in autonomous vehicle are categorized into three different technologies, and they are as follows.

1. Sensor Technologies: The sensor technologies used in autonomous vehicles consist of LiDAR, VLS, ultrasonic ranging sevices (URD), infrared ranging, and millimeter wave radar (MWR), etc. The LiDAR consists of GPS, scanner, and laser technology to generate 3D information about a particular area, providing remote sensing based on pulses of light.
2. Vision Technologies: The vision technologies consist of Stereo Vision System (SVS), HD cameras, Black box, or CCTVs. It helps in forensics and takes necessary actions by recording visual information with high confidentiality, authenticity, and integrity.
3. Positioning Technologies: The positioning technologies include GPS, radar cruise control, and radar-based obstacle detections (RBOD). In autonomous vehicles, the GPS receiver can be used in conjunction with the Doppler radar speedometers, RCC, and RBOD to provide precise vehicle location and active location validation.

   This chapter discusses about different types of vehicular ad hoc network (VANET) technologies based on dedicated short-range communications (DSRC) or 802.11p Protocol and cellular technologies. It provides DSRC standard suites and applications of VANETs such as safety applications, cooperative collision avoidance (CCA), emergency warning messages (EWM), traffic managements, and infotainment applications. In the end, it discusses about the market demand of automotive cybersecurity for current and future environment. It discusses the use of cellular technology to support vehicular communication known as LTE for vehicles (LTE-V) that is being researched and developed. It is an alternative technology for ITS that uses existing cellular base stations making urban transportation more manageable and efficient.

1.5.2. Chapter 3 mostly focuses on cybersecurity and privacy in intelligent and autonomous vehicles. It provides different types of security and encryption schemes that can be used in autonomous vehicles. The cyber security in intelligent and autonomous vehicles can be a combination of physical security, information security, policies, standards, legislation, and risk mitigation

strategies. It also discusses about different security elements used in intelligent and autonomous vehicles. The malicious attackers use different means of attack strategies at different levels, and it severely impacts on the vehicle's physical and cyber security system. The malicious nodes can tamper the vehicle sensors such as onboard systems, in-vehicle sensors and can intercept message exchange between the vehicles in the in-vehicle communication. The malicious nodes can be an insider attacker that may attack both the in-vehicle and inter-vehicle communication. Several attacker models have been demonstrated. It provides some of the security and privacy threats such as fake information attack, message replay attack, integrity, non-repudiation, access control, and privacy attack. The vulnerability is the weak point in the autonomous vehicle system that are misused and easily attacked by the attackers for their own advantages. A detailed autonomous vulnerability taxonomy of the vehicles is given, and solution mechanisms such as preventive, active, and passive defense are also provided. It also deals with the privacy of the autonomous vehicles. Some of the privacy measures discussed are cryptography-based schemes, trust management schemes, and blockchain schemes.

1.5.3. Chapter 4 mainly focuses on the in-vehicle communication systems and cyber security issues. In this, we concentrate on safety, cybersecurity, and privacy of the embedded automotive vehicles within the automotive domain. It discusses about in-vehicle electrical and electronic systems, introduces specialized advanced driver assistance systems (ADAS) in more details, and provides in-depth information regarding vehicle sensors, in-vehicle network types, and in-vehicle architecture and topology. We discuss seven categories of vehicle electrical and electronic (VEE) used in the in-vehicle system. The vehicles use ECUs to communicate with other control units, sharing vital vehicle information via the LAN protocol. Moreover, we discuss about the different types of IVN protocols such as CAN, FlexRay, Automobile Ethernet, LIN, and MOST along with their security threats. We present the IVN network architecture and its challenges on OBD-II ports, threats, and countermeasures. In the end, we discuss the cybersecurity in IVN and present the cybersecurity protection layer for the in-vehicle systems. It provides the functional safety as well as vehicle cybersecurity and discusses its issues and challenges. The safety and security in automotive engineering are closely related with each other, and if there is a worthy interaction between them, then they could get huge benefit from each other.

1.5.4. Chapter 5 focuses on embedded security systems in vehicles such as AUTOSAR. We discussed AUTOSAR and different threat models and risk assessment for automotive vehicles. Within this chapter, we analyze two methods of threat modeling commonly used in the computing industry and determine their eligibility to the connected vehicle. We further suggest improvements to these methods of threat modeling to make them more applicable to the fundamental architecture of applications used in today's vehicles, i.e., AUTOSAR. The first method, TARA, reflects an attacker-centered

approach while the second method, STRIDE, explores the system's information infrastructure and is part of the software-centered approach. The two methods are implemented successfully based on the AUTOSAR norm for the connected car and the underlying software architecture. The TARA method was developed by security experts from Intel Security and is based on three groups of collected data, denoted as libraries, and they are Threat Agent Library (TAL), Methods and Objectives Library (MOL), and Common Exposure Library (CEL). The three libraries developed using the TARA and STRIDE method framework are a strong starting point for all applications in the future. This chapter shows the effectiveness of these approaches, including the real validation of STRIDE tests on real devices. The domain experts will be able to include them in their tool set for future research and analysis.

1.5.5. In Chap. 6, we focus on the inter-vehicle communication system and its cybersecurity issues. We describe in detail the various types of connected vehicle technology and its security issues. The cybersecurity protects the system, or networks from malicious cyberattacks that interrupt the normal communication in the network or thwart the functioning of the system or steal the sensitive information. This section discusses about the cybersecurity of the intelligent and autonomous vehicles against different types of attack vulnerabilities, hacking, associated risks, their preventions, and solutions. We discuss the different types of security and privacy issues and security requirements in connected vehicles. This section especially focuses on security and functional safety related to V2X communication.

We examine recent developments in connected vehicle technology and provide different types of security issues in connected vehicles. The autonomous vehicles based on a limited sensing range cannot be fully trusted. The connected vehicles offer a broader understanding of the surrounding environment and help vehicles make smarter decisions about the messages exchanged between the neighboring vehicles and the RSU. This helps in planning the future travel route in a safe and secure way. The vehicle-to-everything (V2X) is the main communication technology for future VANETs that helps vehicles to obtain a wide range of road information in real time that significantly improves driving safety, traffic efficiency as well as provides infotainment services. In this chapter, we overview the V2X technologies and discussed vehicle-to-infrastructure (V2I), vehicle-to-network (V2N), vehicle-to-vehicle (V2V), and vehicle-to-pedestrian (V2P) communication. This chapter also discusses, in detail, DSRC-based V2X technology to support cooperative awareness applications such as vehicle warning, emergency brake light, and vehicle platooning. However, these applications are suitable only for low density of vehicles with low bandwidth and it is not suitable for high density of vehicles and infotainment applications. So, the third-generation partnership project (3GPP) works toward modifications of radio access suitable for V2X communications known as cellular V2X or C-V2X. In C-V2X, it extends the cellular device-to-device (D2D) communications specification by introducing two more operational modes dedicated to V2V

communications, i.e., Mode 3 and Mode 4. With the advancement in C-V2X technology, the 3GPP enhanced the LTE technologies and released the 5G C-V2X, and recently the 3GPP accelerated the work in new radio technology and introduced and 5G NR C-V2X in Rel. 16, which have backward compatibility features. There are also hybrid technology that combines both the DSRC and cellular technology for vehicular communication. Later in the chapter, it provides the evolution of C-V2X toward 5G technology for autonomous vehicles, as well as its applications and requirements. In the end, we explain the security, privacy, and trust management issues in connected vehicular technologies. We discuss the trust management issues, homomorphic encryption, and blockchain as a security in V2X communication.

1.5.6. In Chap. 7, we discuss about the integration of ITS with the features of IoT, which is called the Internet of Vehicles (IoV). Over time, the IoV has developed from the conventional vehicular networks to advanced infrastructures and other equipment for the ITS and road transport. The IoV is a complex Internet-connected vehicular network where the vehicles are equipped with different types of sensors that collect data from other vehicles and road infrastructures and send them to the cloud. Some of the characteristics of IoV are complex communication, dynamic topology, high scalability, localized communication, and high processing capacity: We present the detailed IoV architecture layer, security attacks, security requirements, and challenges. Some of the applications of IoV can be seen in intelligent transportation system (ITS), business-related applications, and smart city applications. The existing IoV architecture lacks security requirements such as authentication, authorization, and trust-related issues. This chapter discusses the machine learning techniques used in IoV and presents different solution approaches to overcome various attacks based on machine learning.

We also discuss about new emerging paradigm called vehicular social network (VSN), which is the integration of social networks and IoV that builds a social relationship among the vehicles as well as the drivers of the vehicles. In addition to the social relationship, the VSN can combine vehicle communication networks with the human factors that influence vehicle communication between vehicle drivers. In VSN, each vehicle is capable of creating social links with neighboring vehicles, drivers, and smart devices on an autonomous basis. The versatility of vehicles will carry out the features of social networks in which vehicles display similar gestures and habits when driving on the motorway. The VSN architecture consists of three layers, i.e., IoVs, VSNs, and social networks. It also features different applications of VSN and at the end discusses several types of attacks challenging issues.

1.5.7. Chapter 8 provides a detailed information on international cybersecurity regulations, standardizations, and types of organization working in DSRC and C-ITS protocols. The intelligent and autonomous vehicles are at the peak of a major breakthrough in vehicle communication and safety on the road. It is going to be fully implemented soon, which will change the human mobility behavior. Thus, the international technological infrastructure around

autonomous vehicle implementation is already under demand to develop a new set of standards while replacing the existing rules. There are several organizations, consortiums, associations, and authorities working toward the development of new standards, policies, and regulations.
They have been categorized into three regions, viz. Europe, USA, and global standardizations. Several cybersecurity regulations, initiatives, and projects have been carried out under Europe initiatives. Some of them are as follows: In 2006, the SEcure VEhicle COMmunication (SEVECOM) project started to deal with security of vehicular communications and inter-vehicular communications. It provided solutions to the problem that are specific to the road traffic information. In 2008, the E-Safety Vehicle Intrusion protected Application (EVITA) project started, and its goal was to design and verify OBU prototypes and provide e-safety by securing the electronic components of vehicles from tampering. From 2008 to 2012, the SimTD project was carried out in Germany. Its objective was to increase road safety and improve the traffic efficiency based on V2X communication. The result of this project can be applied in the categories like traffic and value-added service. The 7th Framework Program of the EU commission started the Open VEhiculaR SEcurE (OVERSEE) project in 2010 and ended in 2012. OVERSEE provided standard, secure, and generic communication application platform for vehicle and enhanced the efficiency and safety of the road traffic. Similarly, the framework funded another project called Preparing Secure Vehicle-to-X Communication Systems (PRESERVE) in 2011 and ended in 2015. The PRESERVE objective was to design an integrated V2X security architecture (VSA), implement the architecture, and field test the VSA system. The CAR2CAR Communication Consortium (C2C-CC) was established in Europe, which is a consortium of leading European and international vehicle manufacturers, equipment suppliers, engineering firms, road operators, and research institutions. Similarly, the AUTomotive Open System Architecture (AUTOSAR) is very popular in-vehicle software standardization organization for intelligent and autonomous vehicles. The AUTOSAR is a global consortium of automakers, suppliers, service providers, vehicle industry, semiconductors, and Software Company. In the USA, the Society of Automotive Engineers (SAE) and International Organization for Standardization (ISO) jointly worked together to develop the current state-of-the-art cybersecurity standards for vehicles in two areas, i.e., road vehicles and ITS. The SAE and ISO co-chaired and worked as a Joint Working Group (JWG) to introduce ISO/SAE 21434 under a new agreement. The Institute of Electrical and Electronics Engineers Standards Association (IEEE-SA) introduced 802.11p standard to support Wireless Access in Vehicular Environments (WAVE) for ITS applications. As for international initiatives, the International Organization for Standardization (ISO) and SAE work together for the vehicle cybersecurity standards. The ISO introduced ISO 26262, which is an international risk-based standard for functional safety of electronic and electrical systems in vehicles derived from IEC 61508. Similarly, the United Nations

Economic Commission for Europe (UNECE) is preparing a certification for a Cyber Security Management System (CSMS) that mandates the approval of the vehicles according to the requirement of the recent document proposal. It is working toward a global standardization and regulation on cybersecurity of the vehicles focusing on the vulnerability issues like Over the Air (OTA) issues. Likewise, there are several safety and cybersecurity standards and projects in the automotive industry, and the detail information and timeline are given in Sect. 2 of Chap. 8. Similarly, Chap. 8 discusses the V2X technology based on DSRC and cellular network and its adoption. It showcases the 5G V2X test bed and its use cases around the globe. Finally, it presents the future of intelligent and autonomous vehicles, cybersecurity issues, and solutions based on machine learning.

References

1. R. Shrestha, S. Kim, Integration of IoT with blockchain and homomorphic encryption: challenging issues and opportunities, in *Advances in Computers*, vol. 115, eds. by S. Kim, G. C. Deka, and P. Zhang (Elsevier, 2019), pp. 293–331
2. Y. Xiang Gu, The industrial challenges in software security and protection, in *The 9th International Summer School on Information Security and Protection*, (2018), pp. 1–138
3. M. Wolf, T. Enderle, R. Lambert, A. Schmidt-derrick, WannaDrive? Feasible attack paths and effective protection against ransomware in modern vehicles, in *15th ESCAR Europe* (2017), pp. 1–14