CHAPTER

SECURITY AND DATA PRIVACY OF MODERN AUTOMOBILES

6

Juan Deng, Lu Yu, Yu Fu, Oluwakemi Hambolu, and Richard R. Brooks
Clemson University, Clemson, SC, United States

6.1 INTRODUCTION

Surface transportation system has shown improved safety, mobility, and environmental footprints since the introduction of advanced technologies and a new paradigm, known as intelligent transportation system (ITS) has helped to promote technology focused research and development in government and private sectors. In addition, traditionally automobiles have been mechanical devices, but advances in electronics and information and communication technology (ICT) have radically changed the industry. Modern automobiles are heavily computerized and increasingly networked. Electronic Control Units (ECUs) are embedded computer systems that control transmission, engines, brakes, air conditioning, entertainment systems, etc. These ECUs coordinate internal functions over multiple in-vehicle bus networks. Increasingly, automobiles are connected over external wireless networks to other vehicles, roadside units (i.e., ITS infrastructure), mobile devices, and original equipment manufacturer (OEM) service centers.

The evolution from traditional automobiles to connected vehicles has been accepted, in large part, because it reduces manufacturing costs and increases automobile efficiency. However, these emerging technologies also bring real and reasonable concerns about the security and privacy implications of these changes.

Typically, computer and network security requires securing all components in the infrastructure stack at multiple layers. This requires:

- Physical security,
- Communications security, and
- Application security.

Unlike traditional computing systems, where computers and routers are kept in isolated secure facilities, automobiles are left unattended in public places such as parking facilities for most of the day. This means that physical security may not always be possible. At the other end of the stack, automotive applications are usually implemented by a number of small companies for the OEMs. The small companies have small profit margins and the OEMs have multiple vendors to choose from. While this is economically advantageous, the OEMs have limited control over the development process and limited liability for data security mistakes. These issues are representative of the security challenges facing the automobile industry. Other challenges include:

- Each automobile design has to integrate the needs of different stakeholders (including the OEM, component vendors, repair shops, people with leasing agreements, car dealerships, car owners,

Data Analytics for Intelligent Transportation Systems. DOI: http://dx.doi.org/10.1016/B978-0-12-809715-1.00006-7

car fleet operators, the police and environmental regulators, transportation safety regulators, transportation infrastructure operators) with multiple conflicting interests.

- Automobiles integrate a large number of communications networks, such as in-vehicle bus networks (e.g., Control Area Networks (CANs), Local Interconnect Networks (LINs), Media Oriented Systems Transport (MOST), and FlexRay), Wi-Fi, Vehicular Ad Hoc Networks (VANETs), cellular networks, mandated tire pressure monitoring systems (TPMS), Wireless Personal Area Networks (WPANs), entertainment systems, and keyless entry systems.
- As an automobile travels, it moves between multiple networks and network vendors. Handoffs between networks need to maintain both communication connections and security levels.
- Many vehicular applications and services are not designed with security in mind. A single implementation error in one component can be exploited to gain access to the bus networks. From the buses, it is easy to access and control the ECUs. This gives the attacker control over the entire vehicle, including the brakes and steering.
- ECUs can be accessed, apart from directly through the Onboard Diagnostics-II (OBD-II) port, remotely through wireless communication. This provides a much larger attack surface than most traditional systems.
- Multiple ECUs from multiple vendors are integrated into one single platform. The OEMs may, or may not, have access to the source code of vendor software. If two vendors make different assumptions, for example, they use different network packet sizes; this can create an exploitable vulnerability. To be certain that the system is secure; the OEM would have to test all possible combinations of components, which is not commercially attractive.

This chapter surveys connected vehicle security and privacy issues. In Section 6.2 we give an overview of communications networks and the innovative applications in connected vehicles. Section 6.3 identifies stakeholders within the automotive ecosystem and the assets they need to protect. An attack taxonomy that describes attacks on connected vehicles, originally in Ref. [1], is given in Section 6.4. We analyze existing attacks on connected vehicles and map them to the attack taxonomy in Section 6.5. Discussion of security and privacy solutions are presented in Section 6.6. Conclusions and future research directions (i.e., open issues) are presented in Section 6.7.

6.2 CONNECTED VEHICLE NETWORKS AND VEHICULAR APPLICATIONS

6.2.1 IN-VEHICLE NETWORKS

Modern automobiles are controlled by embedded computer systems, called ECUs. The number of ECUs is increasing; high-end vehicles have up to 120 ECUs. ECUs collect sensor data and control a broad range of automobile functions, including the powertrain, entertainment systems, brakes, power steering, and lighting. ECUs communicate over a number of in-vehicle bus systems, CANs, LINs, FlexRay, and MOST networks. CAN and FlexRay buses are for critical ECUs that require fast networks, such as the powertrain. LIN networks are for ECUs that require less transmission speed, such as lights, air conditioning, seats, and doors. MOST networks are mainly for infotainment systems such as audio, video, and voice. Because different bus networks use different physical media and protocol stacks, gateway ECUs are needed to read and write between the different buses and manage protocol conversions. A gateway ECU sends, receives, and translates messages between connected buses.

Wireless technologies are also used for ECU communications. TPMS is mandated on modern automobiles in the United States and European Union. TPMS uses battery powered TPM sensors mounted on the tires of a vehicle to continuously monitor the air pressure of all the tires. The sensors periodically broadcast the pressure, temperature measurements together with their unique identifiers to the in-vehicle TPM ECU. The transmission uses radio frequency technology. The TPM ECU, in turn, analyzes the data, and triggers a TPM warning light and message on the vehicle board if the data suggest underinflated tires. TMPS increases overall road safety by detecting underinflated tires. TPMS also improves fuel economy because proper tire inflation improves traction and tire rolling resistance, and reduces braking distance. Similarly, antitheft systems (e.g., remote keyless entry, engine immobilizer, passive entry) are also common. Radio Frequency Identification (RFID) [2] based antitheft systems have an RFID embedded in a key or keyfob. The RFID communicates directly with a reader device in the car.

In-vehicle WPAN connects personal devices (e.g., cell phone, PDA, headset) via short-range wireless technology, most popularly Bluetooth. WPAN can be interconnected to internal buses via a WPAN gateway ECU. This allows consumers to control lights, windshield wipers, airflow, heat, entertainment units, and many other features using a Bluetooth-enabled PDA or a Bluetooth-enabled headset with voice-activated control [3].

6.2.2 EXTERNAL NETWORKS

Connected vehicles can communicate with each other, or roadside units, by transmitting a basic safety message (BSM) using VANETs. The BSM data transmitted in VANETs include vehicle location, heading, speed, distance measured by Millimeter Radar, and traffic conditions. VANETs can use multiple wireless technologies: Wireless Access in Vehicular Environments (WAVE), Dedicated Short Range Communications (DSRC), Worldwide Interoperability for Microwave Access (WiMAX), Universal Mobile Telecommunications System (UMTS), and Long Term Evolution (LTE) etc.

Connected vehicles also communicate with OEM service centers using cellular networks and traffic management centers through roadside units. Many manufacturers have business to vehicle offerings, such as Ford's Sync [4], GM's OnStar [5], Toyota's Safety Connect [6], Lexus' Enform [7], BMW Connected Drive [8], and Mercedes-Benz's Mbrace [9]. These services provide safety (crash reporting), roadside assistance (remote diagnostics), vehicle monitoring (location tracking, battery monitoring), and antitheft (remote engine stopping and locking) services.

Fig. 6.1 [10,11] shows an example architecture for connected vehicle networks. Internal bus networks communicate with external networks via gateway ECUs. Innovative connected vehicle applications as envisioned in USDOT developed connected vehicle reference implementation architecture (CVRIA) [12] leverage connected vehicle networks.

6.2.3 INNOVATIVE VEHICULAR APPLICATIONS

Over-the-air (OTA) ECU update services connect a vehicle with cellular equipment to the OEM service center to remotely reprogram ECU firmware. Currently ECU updates at a dealership can be time-consuming and inconvenient for vehicle owners, and expensive for OEMs. Some OEMs now provide OTA updates for noncore ECUs. BMW, Audi, and Tesla have recently announced

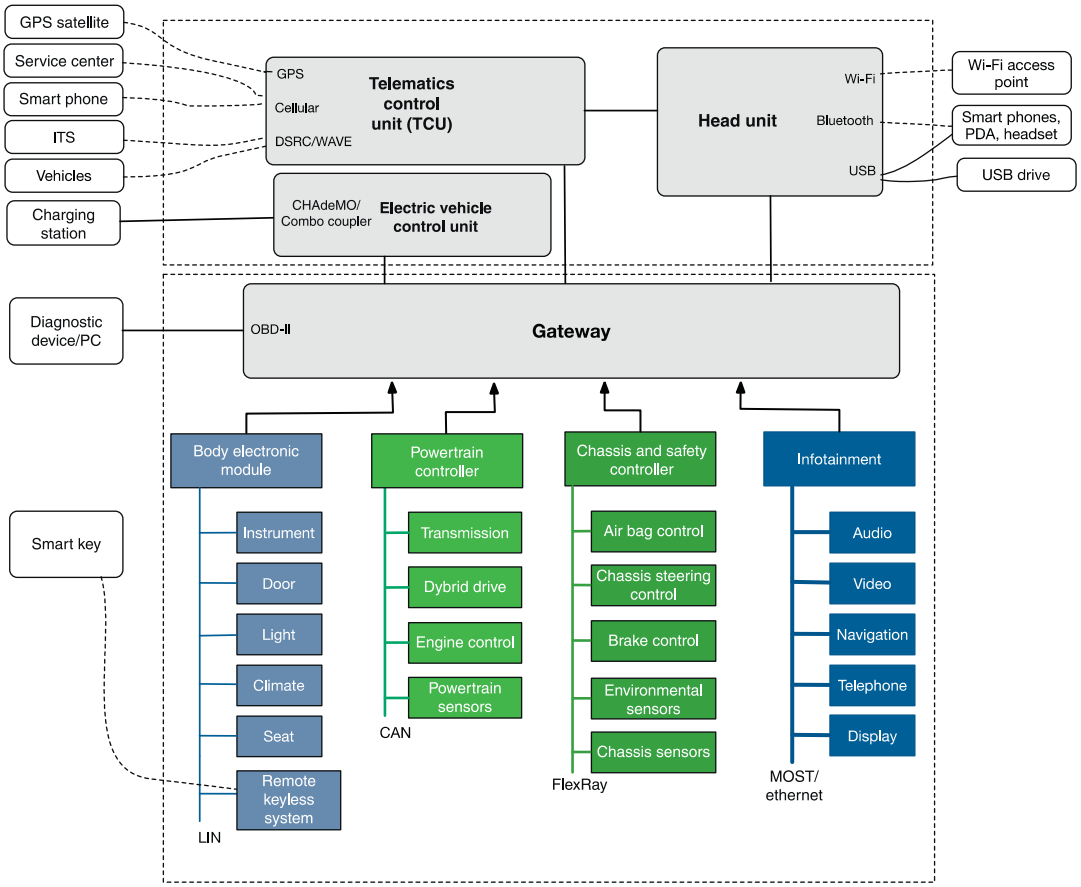

FIGURE 6.1

Architecture of connected vehicle networks, using data from Refs. [10,11].

procedures for remotely updating navigation maps [13]. GM Onstar can remotely update its Telematics Control Units (TCUs) [14]. However, an OTA update for core ECUs is not common. Only Tesla publicly claims to remotely update its core ECUs. Remote updates have security advantages and disadvantages. They let OEMs quickly correct security flaws for their entire fleet. However, if not implemented carefully, attackers can use this access to modify critical systems. Code signing is essential for a remote update to be certain that only authorized code is used. Poorly implemented auto-update systems have been used to infect machines in the past [15].

Smart phone Apps are developed to control connected vehicles. They let customers remotely start/stop the engine, locate vehicles in the parking lot, and lock/unlock doors. Apps can also monitor vehicle speed, mileage, and location. An iPhone App, iDriver, allows customers to steer cars remotely via their iPhones [16]. In Section 6.5.2.1, we discuss problems that have been found in

current security systems. Given our inability to secure simpler systems; it may be reasonable to worry about the potential security challenging of connected vehicles and future automated vehicles. *Vehicle Platooning* applications envision a number of vehicles cooperating to maintain a relatively short distance from each other and improve their fuel efficiency and road capacity. Vehicles use each other's position and velocity data for collaborative control to reduce their fuel consumption by reducing air drag. An *Automated Vehicle* is a self-driving vehicle. It senses its environment and navigates without human operations and will eliminate crashes due to human driver errors and problems such as falling asleep. Vehicle drivers are free from driving tasks and continuous monitoring of the environment. Automated vehicles are anticipated to improve fuel efficiency, increase road capacity/utilization, and reduce pollution. Automated vehicles are attracting the attention of IT companies, academia, and OEMs. Google announced that its prototype automated vehicle has driven hundreds of thousands of miles in self-drive mode under restricted conditions [17]. Recently, Google, Uber, and Tesla have made headlines by developing self-driving taxis for big cities [18].

VANET applications have been proposed to enhance safety (e.g., collision avoidance, lane-changing assistance), increase comfort (e.g., automatic toll/parking payment and fuel payment), and improve road utilization (e.g., congestion notification, route selection). These applications rely on other vehicles to provide reliable information, even though no reliable approach for mutual authentication has been proposed. If such a method were to exist, there would be worrisome privacy concerns.

6.3 STAKEHOLDERS AND ASSETS

As discussed earlier, some major IT companies have joined the automobile ecosystem:

- Google is producing automated vehicles.
- Microsoft has a Windows offering for automobiles.
- Apple announced plans for an electric vehicle by 2019.
- GPS devices, Google Maps, and Apple provide driving directions.
- Communications providers are exploring how to best interface with connected vehicles. The Continuous Air-interface for Long and Medium Range (CALM) [19] is an ISO initiative to define a set of standardized wireless communication protocols and interfaces for ITS services. CALM supports uninterrupted transparent networking and handover between different communications networks (e.g., WiMAX, DSRC, Millimeter Wave, Wi-Fi, etc.) and media providers. This decouples ITS services from the underlying communications technologies and allows services to select networks through a standard interface.

Perfect security does not exist and would probably be prohibitively expensive if it did exist. A reasonable engineering approach considers the value of assets that need to be protected and uses limited resource to secure assets when it makes sense economically. Therefore, we identify the stakeholders involved in connected vehicle ecosystems and their assets to be protected. Fig. 6.2 shows the stakeholders and their assets. In the past, private vehicle owners only needed to protect their vehicles from being stolen. Modern vehicles generate, store, and transmit personal private information. For example, many vehicular applications record vehicle locations, and send the data to

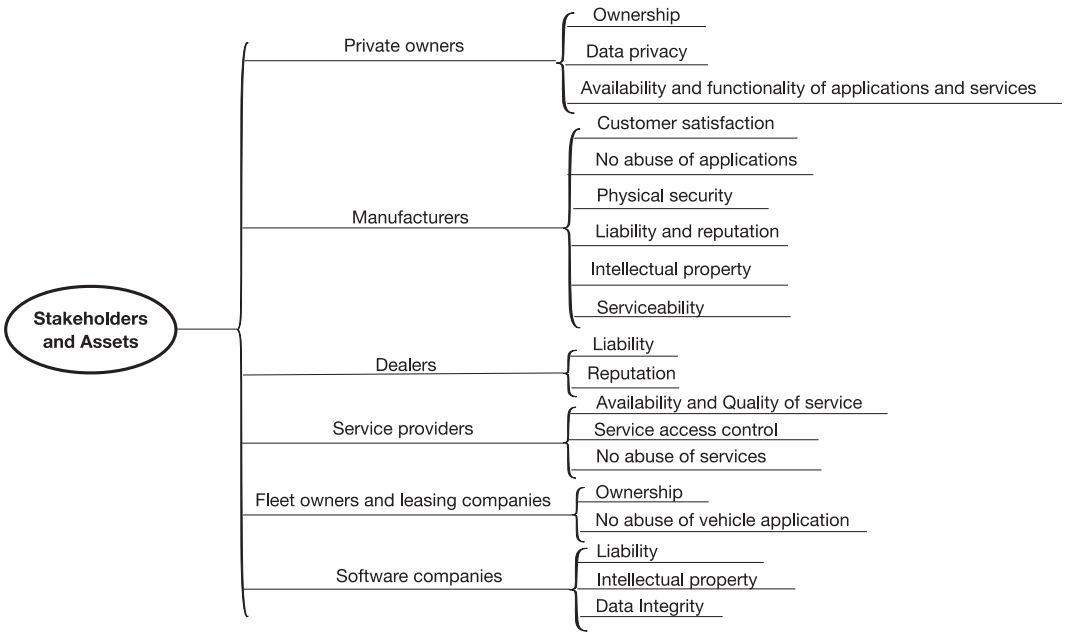

FIGURE 6.2

Stakeholders and their assets to be protected, extended from Ref. [1].

service centers. Internet access in vehicles is used by vehicle owners to access online banking, calendars, email, etc. Sensitive information (e.g., login, itineraries, and billing records) is stored in vehicles. Private vehicle owners should want to protect their data privacy. In contrast, fleet owners view vehicles as a commodity and do not store sensitive information [20]. Thus, conflicts are common. For example, car rental companies track the driving history of their clients. Clients who speed, or leave predefined regions, must pay hefty fines. Needless to say, the clients would prefer for this information to be private.

Vehicle manufacturers have large inventories of automobiles to protect prior to sale. After sale, unauthorized modifications of ECU software can have warranty and liability implications for manufacturers and software suppliers. As automobiles become increasingly computerized, manufacturers make large investments in software development. This intellectual property must be protected as well. Dealers need to protect automobile inventories, but intellectual property issues and unauthorized software modifications do not concern them.

Vehicle manufacturers offer services to their customers through cellular networks; making them service providers. Service providers generate revenues from service provision, so they restrict service access only to paying customers. To keep paying customers satisfied, they must guarantee both availability and quality of service including security and privacy. Software companies that develop software for vehicle manufactures also need to protect intellectual property and prevent unauthorized software modifications.

6.4 ATTACK TAXONOMY

Fig. 6.3 shows the attack taxonomy that describes potential attacks on connected vehicles. It is a modified version of the attack taxonomy developed by Computer Emergency Response Team (CERT) to describe attacks to computer networks (i.e., a computer connected through networks such as the internet or local area network) [21]. We analyze attacks on automotive systems using the taxonomy. Mapping attacks on automobiles to the taxonomy helps find the gaps between attacks and existing security solutions. It also finds common problems shared by known vulnerabilities, like the use of inadequately long cryptographic keys [22,23]. In Fig. 6.3, an incident occurs when an attacker launches a set of attacks to achieve an objective. In a specific attack, a tool exploits the vulnerability of a target to gain unauthorized result. Each attack includes multiple actions to compromise specific target functions.

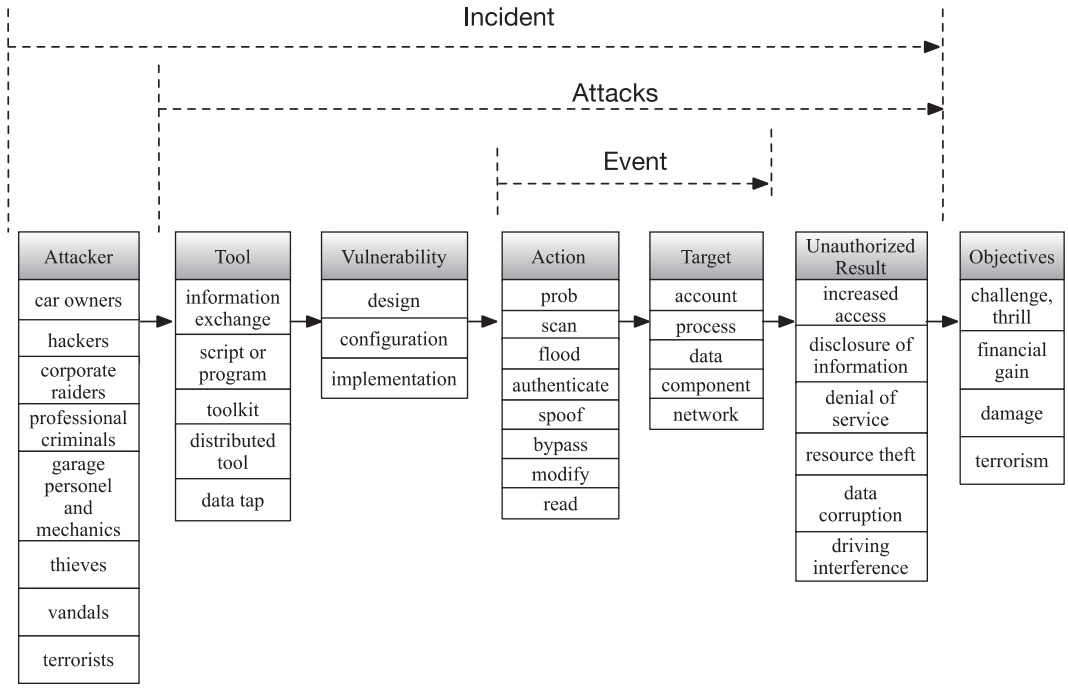

FIGURE 6.3

Attack taxonomy for connected vehicles, extended from the CERT attack taxonomy from Ref. [1].

6.5 SECURITY ANALYSIS

The internal bus networks of automobiles lack necessary security mechanisms. Wireless internal networks (e.g., TPMS and antitheft systems) are also vulnerable. In this section, we analyze the

vulnerabilities of various connected vehicle networks and their protocol stack. Attacks leveraging these vulnerabilities will be enumerated. These attacks are mapped to the CERT attack taxonomy. Inconsistency was found during the mapping. Hence, CERT taxonomy was modified to fit in the connected vehicle context.

6.5.1 NETWORK AND PROTOCOL VULNERABILITY ANALYSIS

In-vehicle bus networks are broadcast and use shared access. No encryption is implemented. Messages on these bus networks are in clear text. No authentication is in place to verify the source of a message. And most of all, the buses are interconnected via gateway ECUs. Even though some gateway ECUs include firewalls, most of them allow diagnostic functions and interfaces that access all the internal bus networks without any restriction. Leveraging these vulnerabilities, a malicious ECU can eavesdrop (i.e., "read" in the language of CERT attack taxonomy), spoof, replay (i.e., "copy" in the language of CERT attack taxonomy) messages, and flood the network. A single compromised ECU on a bus could endanger all ECUs on the connected buses.

CAN Vulnerabilities: A CAN bus includes additional vulnerabilities. CAN messages do not include addresses in the traditional sense; they have identifiers. This identifier determines message type and priority. A CAN ECU decides whether or not to process a message based on the identifier. It is easy to spoof messages and flood CAN bus networks. The CAN protocol uses message priority arbitration to respond to collisions. When two CAN ECUs send messages simultaneously, the message with a lower identifier (i.e., higher priority) gets access to the bus and sends its message, while the other ECU backs off, and waits a predefined period of time before retransmission. A malicious CAN ECU can exploit the priority arbitration and continuously send spoofed messages with the lowest identifier to perform a Denial-of-Service (DoS) attack on other CAN nodes. In addition, because internal buses are universally connected, these DoS attacks can victimize other CAN buses. Carshark is a tool that snoops on CAN communications, reverse-engineers CAN packets, and injects new packets [24]. Attacks exploiting CAN bus vulnerabilities to attack ECUs are discussed in Refs. [24–27]. In particular, the attack described in Ref. [27] caused the electrical window system to malfunction. Attacks described in Ref. [25] successfully disabled the warning light and faked the presence of an air bag that had been removed. A vehicle virus was introduced in Ref. [26] to remotely lock/unlock cars. A comprehensive CAN bus exploit is described in Ref. [24].

LIN Vulnerabilities: LIN uses a single-master multislaves architecture where only the master ECU of a LIN network can initiate a message and it polls a slave ECU to respond to a message. Attacking this single point of failure is promising [28]. In LIN, the master can force a slave to sleep by sending a special message. A malicious LIN ECU can spoof the message to deactivate the entire LIN network. A LIN message contains a SYNC field in the message header. The master ECU sets this field to a predefined value to instruct slave ECUs to synchronize. A malicious LIN ECU can spoof the message and modify the SYNC filed to disrupt the synchronization.

MOST Vulnerabilities: In a MOST network, one MOST device acts as a timing master that periodically sends timing frames that cause MOST slaves to synchronize. A malicious MOST device can fabricate malicious timing frames to interrupt the synchronization. The MOST protocol allows for bandwidth contention. A fixed length communication segment, called the Dynamic Segment, is available periodically so that MOST devices can contend for it. Contention depends on message priority. The device with the highest message priority wins. The winning MOST device can

transmit until it either finishes its transmission or another device with higher message priority joins the contention. A malicious MOST device can jam the segment by spoofing high-priority messages.

WPAN Vulnerabilities: WPAN using Bluetooth is very popular. Security measures including authentication and encryption are used in Bluetooth; however, the security is weak [29]. The keys for encryption and authentication in Bluetooth are based on the Bluetooth device address and a PIN. However, the address of each Bluetooth device, which is a 48-bit unique address assigned by the device manufacturer, is public information. Any Bluetooth device can know the address of any other neighboring Bluetooth device by simply inquiring for it [29]. The PIN is also comprisable. Generally, the PIN is a four-digit, user-entered code like in standard mobile phones. In some worse cases, the PIN is a nonvolatile built-in at the factory. Therefore, Bluetooth security is crackable. WPAN is interconnected to internal buses; compromised WPAN can be the attack vector (i.e., entry point) to ECUs.

TPMS Vulnerabilities: TPMS messages are broadcast over radio. Each TPMS message contains sensitive data: temperature, tire pressure, and a unique identifier. TPMS lacks basic security measures. The message transmissions are not encrypted, and the TPM ECU trusts all received TPMS messages without input validations. Eavesdropping, reverse engineering, and spoofing attacks are possible. TPMS wireless broadcasting also presents a privacy risk, as the unique identifier identifies and tracks a vehicle. The risk is greater since TPMS use is mandatory, and it is hard to deactivate.

Antitheft System Vulnerabilities: The common wireless antitheft systems for modern automobiles include remote keyless entry, passive keyless entry and start, and engine immobilizers. A key communicates with the car over a wireless channel. For security, challenge and response protocols or secret codes usually authenticate the key to the car; and the communications are encrypted. However, inadequate encryption key length and an imperfect cipher structure make it possible to crack these antitheft systems [22,30]. This is often excused by explaining that physical attacks on the car are less expensive than cryptanalysis. It is worth noting that engine immobilizer bypass kits are very inexpensive and sold online.

VANETs Vulnerabilities: Connected vehicles talk to each other or roadside units through VANETs. Vehicle-to-vehicle communications are ad hoc. Self-organized networks, formed voluntarily, are dynamic since vehicles frequently join and leave the network. Message authenticity must be verified. Though some mechanism exists to detect fake messages, an attacker can always forge a large number of messages to drown out authentic messages. This may include a Sybil attack, where one car pretends to be many cars. VANETs data include vehicle location, velocity, distance between vehicles, and traffic conditions. A malicious user can misuse the data to track another vehicle. Without reliable authentication, arbitrary packet spoofing is trivial, which can subvert any VANET application. However, reliable authentication would present a privacy risk.

Vulnerabilities also arise when system implementations either deviate from protocol and standard specifications, or when specifications are vague. Results in Ref. [24] reveal the bus implementation vulnerabilities in a car. One potential vulnerability is bus interconnections through ECU gateways. To mitigate the risk, the standard implicitly defines that high-speed bus networks are more trusted than low-speed buses [24]. High-speed buses connect real-time safety-critical ECUs (e.g., engine, brakes), while low-speed buses connect ECUs that are less critical to safety, such as seat, air conditioner. An ECU connected to a low-speed bus should be unable to send packets to a high-speed bus. However, as shown in Ref. [24] this was not found to be the case in some car models.

In summary, in the attack taxonomy, all classes of vulnerabilities (design, configuration, and implementation) are found.

6.5.2 ATTACKS

Existing attacks on connected vehicle systems target VANETs, antitheft systems, internal buses and ECUs, TPMS, WPANs. An analysis of these attacks is presented and mapped to the CERT attack taxonomy as shown in Tables 6.1 and 6.2.

6.5.2.1 Antitheft system attacks

Automobile antitheft systems prevent unauthorized physical access into automobiles. Potential attackers to break antitheft systems and their objectives [1] are listed in Table 6.1. Successful breaking of antitheft systems not only gives attackers physical access to the automobiles but also various onboard vehicular applications. Thieves usually adopt low-tech attacks to steal cars, such as jimmying the lock, looking for keys left in automobiles, cutting alarm wires, and hot wiring the ignition. High-tech cyber attacks on wireless antitheft systems are increasing, especially targeting high-end cars [31]. Table 6.2 maps existing attacks on antitheft systems to the CERT taxonomy.

Table 6.1 Attackers of Antitheft Systems and their Objectives [1]

Attacker	Objectives
Thieves	Steal cars and costly car components
Vandals	Crack automotive antitheft protection
Hackers	Crack automotive entry system for fun
Professional criminals	Gain access to automobiles

Table 6.2 Attacks on Antitheft Systems

Attack	Tool	Vulnerability	Action	Target	Unauthorized Result
Keeloq attack [30]	Info. exchange	Design (short key; short block size; and similar key schedule)	Read, authenticate	Data (encryption key)	Disclosure of information (encryption key)
DST attack [22]	Info. exchange	Design (short key; cipher function; and structure)	Read, authenticate	Data (cipher function, encryption key)	Disclosure of information (encryption key and cipher function)
Relay attack [32]	Toolkit	Design	Spoof		Resource theft
Bypass kit	Toolkit	Design	Bypass		Resource theft
Jamming	Toolkit	Design	Flood	Network	Denial of service
RollJam	Toolkit	Design	Scan, copy	Data	Resource theft

Keeloq is a 32-bit block cipher used in many remote keyless entries to encrypt the communication between a key fob and a car. Keeloq uses a 64-bit cryptographic key and comprises 528 identical rounds of encryption/decryption cycles. Each cycle of encryption/decryption is equivalent to a non-linear feedback shift register (NLFSR). A key recovery attack [30] revealed the NLFSR and uncovered the encryption key of a Keeloq, exploiting three weaknesses of Keeloq: short key length, short block size, and the existence of an efficient linear approximation of the NLFSR.

The digital signature transponder (DST) is an RFID device that has been used in over 150 million engine immobilizer keys. A DST uses a 40-bit cryptographic key. In its communication with a car, a DST emits a factory-set 24-bit identifier, and then authenticates it with a challenge and response protocol. The car initiates the protocol by transmitting a 40-bit challenge. The DST encrypts this challenge using its 40-bit key, truncates the encrypted challenge to a 24-bit response, and returns it back to the reader. An attack on a DST used in a Ford car uncovered its encryption key after just harvesting two challenge−response pairs [22]. Then the attacker was able to clone the DST and used the cloned DST to unlock the car. The attack first used reverse engineering to uncover the complete functions of the encryption cipher, followed by using brute force attack to obtain the key.

The relay attack [32] on passive keyless entry and start is simple and requires no cryptanalysis expertise. A passive keyless entry and start, unlike a remote keyless entry, does not need human action to unlock cars. A car periodically scans for a passive key. Once a passive key enters in the proximity, the car authenticates the passive key. The car sends a low-powered signal. Passive keyless entry and start only works when the passive key is close to the car (<2 m). The relay attack intercepts the radio signals between a car and a passive key via antennas acting as repeaters, resulting in the passive key activating the car even when it's nowhere near it. The attack has been successfully tested on 10 models from eight manufacturers.

A bypass kit can be an attack vector to antitheft systems. Bypass kits are interface kits used to momentarily bypass the antitheft system. They are produced by OEMs and sold to manufacturers. Sometimes manufacturers need "an additional interface kit to allow an after-market (not factory installed) system to work properly" [33]. With the easy availability of bypass kits [34] and a growing market for stolen luxury cars, this particular crime is likely to be cost-effective in the near future.

Radio jamming is another attack on wireless antitheft systems. A thief can use key fob jammers purchased online to block the radio frequencies emitted from the remote keyless entries to lock the door. More and more radio jamming crimes have been witnessed and reported to police [35,36]. This type of attack can be detected. Normally when a car is locked, it flashes its lights and sounds a beep. When the attack occurs, there is no flashing light or beep.

RollJam is a very small device, available on eBay for less than $50, that attacks remote keyless entries and unlocks cars almost at will [37]. An attacker just needs to put RollJam near a target vehicle and waits for the victim to use the keyfob within the radio range of RollJam. The victim will notice that the keyfob does not work on the first try, but works on the second. Later the attacker can retrieve RollJam, press a button on RollJam to unlock the car. RollJam exploits the design that remote keyless entry uses a set of rolling secret codes. Remote keyless entry changes the secret code every time it uses. A code is rejected by the car if it is used a second time. When a victim uses the keyfob to lock the car for the first time, RollJam jams the signal and records the first code, so the keyfob button press does not work. Naturally the victim tries the keyfob again.

RollJamm jams for the second time, records the second code, and plays the first code at the same time. This time the car will be locked. In this way RollJam has stored a secret code that can be used next time.

6.5.2.2 ECU attacks

Table 6.3 lists major ECU attackers and their objectives. Automotive hobbyists often change their ECUs for enhanced power, or sportive shock calibration. Some dishonest car owners modify mileage when selling their cars. European truck drivers tamper with tachographs to avoid punishment for driving extended hours. Garage personnel steal sensitive customer data that are stored in cars.

An attacker needs to access ECUs to deliver malicious inputs. Checkoway et al. [38] analyzed a full range of I/O channels available in a modern automobile and identified the challenges required to access each channel. Table 6.4 lists the channels that can be used to deliver malicious inputs to ECUs. ECUs can be accessed directly through the OBD-II port, which is federally mandated in the United States and can be found under the hood in virtually all automobiles. The OBD-II port is intended to be used by car owners and garage personnel to access ECUs for diagnostic purposes. A manufacturer-specific tool is plugged directly into the OBD-II port to access the internal buses and retrieve diagnostic information from ECUs. An attacker, by directly plugging in a malicious hardware to the OBD-II port, can gain the control of the vehicle [24]. However, direct access to the OBD-II port is a strong requirement for attackers. The external networks of connected vehicles present a much wider attack surface. Nowadays vehicle diagnostics can be carried out using PCs,

Table 6.3 Attackers of ECUs and their Objectives [1]

Attacker	Objectives
Private owners	Change ECU software to gain more shock calibration, enhanced power, improved brake behavior, or change digital tachometers
Garage personnel	Sensitive information
Corporate raiders	Obtain proprietary information
Hackers	Hacking for fun

Table 6.4 Channels for Attacking ECUs [38]

Channel	Exploitation
OBD-II port	Plug a malicious hardware directly into the OBD-port
CD player	Automotive media systems are connected to internal buses. A compromised CD can attack other ECUs
PassThru	An attacker can either gain control of the PC running the diagnostic software or the connection between the PC and the PassThru device
Bluetooth	Buffer overflow with paired Android phone and Trajan app, or brute force the PIN of Bluetooth network
Cellular	Reverse engineer the software that a car's telematics unit uses to establish connections between the car and a remote center and authenticate the car

instead of dedicated tools. A PassThru device (typically a USB or Wi-Fi device) is plugged into the OBD-II port, and a PC running manufacturer diagnostic software connects to internal buses via the PassThru device. An attacker can either gain control of the PC running the diagnostic software or the connection between the PC and the PassThru device. The Bluetooth WPAN can also be leveraged to deliver malicious inputs to ECUs through a compromised personal device that is connected to the WPAN. The long-range cellular networks offer many advantages for attackers. Cellular networks are generally used to connect a vehicle to the OEM service center. Checkoway et al. [38] reverse engineered the software that a car's telematics unit uses to establish connections between the car and a remote center. They were able to interpose the connections and send arbitrary packets on the connections.

Table 6.5 lists existing attacks in the literature on internal buses and ECUs. Koscher et al. [24] conducted intensive exploits of CAN buses. To begin, they developed CarShark, a CAN sniffer to observe the traffic on the CAN buses. Together with a combination of replay and informed probing, they unveiled how ECUs communicate with each other and the valid packets to control various ECUs including radio, body control module, etc. Koscher et al. also conducted fuzzing attacks and reverse engineering to understand how certain hardware features were controlled. They demonstrated that through CarShark eavesdropping and probing, fuzzing attack and reverse engineering, they were able to take full control of a wide range of individual ECUs including radio, body controller, engine, brakes, and HVAC. Koscher et al. also implemented composite attacks that exploit multiple ECUs. For example, they manipulated the speedometer to display an arbitrary offset of the current speed, such as 10 mph less than the actual speed. This attack intercepts actual speed update packets on the low-speed CAN bus and transmits maliciously-crafted speed packets with the falsified speed to the display.

Another significant attack described in Ref. [24] targets the interconnections of internal bus networks. Each vehicle includes multiple buses, each of which hosts a subset of the ECUs. For functionality reasons, some buses must be interconnected, thus a small number of ECUs are physically connected to more than one bus and act as logical bridges. Perfect and safe network segmentation will not allow ECUs on the low-speed network to access the high-speed network. However, it is

Table 6.5 Attacks on Internal Buses and ECUs

Attack	Tool	Vulnerability	Action	Target	Unauthorized Result
CarShark attack [24]	Script or program	Design	Read, spoof, probe	Data	Disclosure of information (e.g., valid CAN messages)
Fuzzing attack [24]	Script or program	Design	Spoof	Data	Disclosure of information (CAN functionality)
Reverse engineering [24]	Toolkit (CAN ReadMemory, IDA pro)	Design	Read	Data	Disclosure of information (CAN functionality)
Bridging internal CAN Bus networks [24]	Script or program	Design	Modify, spoof	Network	Increased access

not the case in real implementation. It was found that the telematics unit on a car connected to both low-speed and high-speed networks was being exploited. By reprogramming the telematics unit, the ECUs on the low-speed bus were able to disrupt the function of critical ECUs on the high-speed bus. This increased access to critical ECUs can lead to disastrous outcomes.

Two security researchers wirelessly hacked a running Jeep, taking over dashboard functions, steering, transmission, and brakes control [39]. This attack exploits the software vulnerability in Chrysler's Uconnect dashboard computers. Shortly after the hack, Chrysler announced a formal recall for 1.4 million vehicles to patch the software vulnerability.

A light-weight side-channel analysis over the CAN bus is presented in Ref. [40]. Other attacks on ECUs are presented in Refs. [25,27]. However, these attacks, compared to the attacks described in Ref. [24], are weaker and can be achieved using the techniques presented in Ref. [24] as well.

6.5.2.3 TPMS attacks

In a TPMS, battery powered TPM sensors mounted on the wheels of an automobile transmits packets periodically (every 60−90 seconds required by National Highway Traffic Safety Administration (NHTSA)) to in-vehicle TPM ECU. The transmission power of TPM sensors is relatively small in order to prolong sensor battery life. Despite the low data rate, low transmission power, and high travel speed of automobiles, eavesdropping TPMS communications is feasible. Rouf et al. in Ref. [41] demonstrated that with inexpensive hardware the communications can be easily overheard from the distance of over 40 m away from a passing automobile. Reverse engineering TPMS communications to obtain the unique identifier contained in every TPMS packet are also feasible, given that the communications are unencrypted. The identifier can be used to track an automobile. Rouf et al. in Ref. [41] demonstrated the feasibility of tracking an automobile traveling at 60 km/h. Message spoofing is another attack on TPMS due to the lack of authentication, input validation, and proper filtering. It is shown in Ref. [41] that the in-vehicle TPM ECU of an automobile accepted forged packets at an increased rate of 40 packets per second, while the expected packet rate is much smaller. It is also shown in Ref. [41] that an attacker vehicle was able to fool a victim car traveling at the speed of 110 km/h to turn on the low-pressure warning light using spoofed packets, which potentially can drain the vehicle battery. Table 6.6 summarizes these attacks.

Table 6.6 Attacks on TPMS

Attack	Tool	Vulnerability	Action	Target	Unauthorized Result
Eavesdropping	Toolkit (frequency mixer, USRP)	Design	Read	Data	Disclosure of information
Identity exposure	Toolkit (TPMS trigger tool, low-noise amplifier, USRP)	Design	Read	Data (identity)	Disclosure of information
Packet spoofing	Toolkit (frequency mixer, TPMS trigger tool)	Design	Spoof	Data	Denial of service

Table 6.7 Attackers of VANETs and their Objectives [1]

Attacker	Objectives
Terrorists	Can cause harm or hysteria
Greedy drivers	Can clear their route/path by redirecting other traffic
Vandals or hackers	Can access anything

6.5.2.4 VANETs attacks

The attackers that are likely to compromise VANET communications and their objectives are listed in Table 6.7. Terrorists could misuse VANETs in the hope of creating traffic havoc. Greedy drivers that want to clear traffic along their path could fool other vehicles into choosing other paths [42].

VANETs Attacks can be classified into five categories [43]:

- Network monitoring: an attacker monitors the whole network and listens to the communications.
- Social attack: an attacker disturbs the victim vehicles with insulting messages and indirectly causes problems in the victims' driving behaviors.
- Timing attack: an attacker maliciously delays the message and messes up the time-critical safety applications.
- Application attack: an attacker tampers the contents of the messages and causes accidents by sending the fake safety messages.
- DoS attacks: an attacker consumes network bandwidth by message flooding and ID spoofing.

A complete list of attacks on a VANET scan be found in Refs. [44,45] and is mapped to the attack taxonomy in Table 6.8. In a Sybil attack, one vehicle may spoof hundreds of other vehicles to send false road congestion information to fool the nodes/vehicles in the VANETs. DoS attacks are possible, where a large number of spoofed packets absorb all available bandwidth to make the system unavailable for legitimate users. If the attacker launches attacks in a distributed manner from different locations, it becomes Distributed Denial-of-Service (DDoS), which will amplify the power of DoS. Attackers can also send spoofed information to fool the victim vehicle, causing it to halt abruptly to create traffic accidents that may lead to a chain reaction of multivehicle rear-end collisions. In location tracking, an attacker may use data mining technology to track the locations of a vehicle and send spoofed location information for their own benefit. Malicious code/malware/spam attacks can hamper normal network operations and cause serious disruptions in VANETs. A replay attack uses previously generated frames in new connections, which are used by malicious or unauthorized users to impersonate legitimate users. In an illusion attack, the attacker deceives the sensors on his car to produce wrong sensor readings and incorrect traffic information, and send them to neighboring vehicles in order to change their driving behaviors. It will lead to traffic accidents or traffic jams [46]. In a black hole attack, the attacker node claims to have the shortest path to the destination node, hoping to fool other nodes to route messages for the destination node to the attacker. Then the attacker can choose either to drop or forward packets. Gray hole and wormhole attacks are variations of black hole attacks.

Table 6.8 Attacks on VANETs

Attacks	Tool	Vulnerability	Action	Target	Unauthorized Results
Sybil attacks	Script or program	Design (crypto or protocol)	Spoof, authenticate	Identity	Denial of service
Bogus information	Script or program	Design (crypto or protocol)	Spoof, modify	Data	Data corruption
Denial-of-service	Distributed tools	Design (crypto or protocol)	Flood	Resource	Denial of service
Man-in-the-middle attack	-	Design (crypto or protocol)	Modify	Data, identity	Data corruption
Location tracking	Data mining	Design (crypto or protocol)	Read	Location	Disclosure of information
Malicious code	Script or program	-	Modify	-	Denial of service
Replay attack	-	Design (crypto or protocol)	Authenticate	Identity	Disclosure of information, increased access
Illusion attack	Script or program	Design (sensor)	Deceive	Data	Data corruption
Black hole attack	-	Design (protocol)	Spoof, modify	Data	Denial of service

6.6 SECURITY AND PRIVACY SOLUTIONS

A connected vehicle ecosystem includes computers and networks. IT security plays an important role in securing connected vehicles, however, connected vehicle security goes far beyond.

- Vehicles are more physically exposed than computers, as vehicles are operated or parked in the open environment most of the time.
- A connected vehicle has multiple I/O interfaces (e.g., OBD-II access, Wi-Fi, radio, GPS, LTE, Telematics, Bluetooth) whereas computers generally use Wi-Fi and Ethernet.
- A connected vehicle implements multiple protocols in addition to TCP/IP (e.g., CAN protocol, LIN protocol), while a computer connected to the Internet exclusively implements TCP/IP protocols.
- A connected vehicle on the road may go through various networks; handoffs should maintain not only uninterrupted communication connections, but also security levels.
- Multiple external wireless networks have access to internal critical buses through gateway ECUs.
- ECUs are constrained by limited resources (processing power and memory). Security means must respect these constraints.

Data consumed or generated by connected vehicles are valuable assets, and need to be protected. The increasing demand for connectivity collides with data security and privacy on some levels. Potential data breaches pose considerable challenges to the development of connected vehicles. Various types of connectivity equipped in modern cars may enable unauthorized access to

private data collected by the vehicle, such as location data, driver identity, and payment card information used for dashboard shopping. The automobile industry has a strong commitment to consumer privacy protection. The Alliance of Automobile Manufacturers, the Association of Global Automakers and their members (23 global major automakers) developed a voluntary set of data privacy principles in 2014 [47]. The principles include:

- Transparency: Participating Members commit to providing Owners and Registered Users with ready access to clear, meaningful notices about the Participating Member's collection, use, and sharing of Covered Information.
- Choice: Participating Members commit to offering Owners and Registered Users with certain choices regarding the collection, use, and sharing of Covered Information.
- Respect for Context: Participating Members commit to using and sharing Covered Information in ways that are consistent with the context in which the Covered Information was collected, taking account of the likely impact on Owners and Registered Users.
- Data Security: Participating Members commit to implementing reasonable measures to protect Covered Information against loss and unauthorized access or use.
- Integrity and Access: Participating Members commit to implementing reasonable measures to maintain the accuracy of Covered Information and commit to giving Owners and Registered Users reasonable means to review and correct Personal Subscription Information.
- Data Minimization, De-Identification, & Retention: Participating Members commit to collecting Covered Information only as needed for legitimate business purposes. Participating Members commit to retaining Covered Information no longer than they determine necessary for legitimate business purposes.
- Accountability: Participating Members commit to taking reasonable steps to ensure that they and other entities that receive Covered Information adhere to the Principles.

The objective is to address increasing concerns about privacy issues raised by new connected vehicle technologies. In what follows, a set of security and privacy solutions in the literature to secure connected vehicles is described.

6.6.1 CRYPTOGRAPHY BASICS

Security and privacy rely heavily on cryptography. Asymmetric cryptography, symmetric cryptography, and hash are widely used to provide authentication, confidentiality, and integrity.

Asymmetric cryptography is primarily used to authenticate the communication nodes. A public key and secret key pair is used for encryption/decryption in asymmetric cryptography. Encryption using a public key (or secret key) can only be decrypted using the paired secret key (or public key). Each host holds a pair of public key and secret key. The public key is published to other hosts, while the secret key is kept secret. If host A wants to authenticate itself to host B, host A encrypts some predefined value using its secret key and sends it to B. B decrypts it using A's public key and retrieves the value. Then A authenticates itself to B by showing that it owns the secret key. Asymmetric cryptography can also be used for confidentiality. Host A encrypts its messages using the recipient's public key. Then only the recipient can decrypt the messages using its private key.

Symmetric cryptography is primarily used to provide confidentiality. The encryption and decryption use the same key, which is shared only between the communication ends. Compared to asymmetric cryptography, symmetric cryptography is less computational intensive; therefore, it is a general practice to use asymmetric cryptography for authentication and symmetric cryptography for confidentiality.

A hash function maps data of arbitrary size to a bit string with a fixed size, which is called a digest. Hash function is one-way function, that is, infeasible to invert. Hash is used for detecting communication tampering. When host A sends a message to host B, it first applies the hash function that is previously agreed between the two hosts to produce a message digest, and it sends to B both the message and the digest. Upon receiving them, B applies the same hash function on the received message to produce a digest, and compares it with the received digest. If the two digests are the same, then the received message is not tampered.

6.6.2 SECURITY SOLUTIONS FOR BUS COMMUNICATIONS

A significant vulnerability of bus communications is that messages are broadcast in clear text with no authentication. Many attacks (e.g., Carshark sniffer, fuzzing, reverse-engineering [24]) exploit these vulnerabilities. Security techniques to protect internal bus networks include code obfuscation, rootkit traps, cryptography, intrusion detection systems (IDSs), and honeypots [28,48–51].

6.6.2.1 Code obfuscation

An ECU obfuscates messages before sending them to the connected buses [48]. This makes it difficult for attackers to reverse-engineer the ECU firmware and harvest valid messages to control vehicle hardware. Obfuscation is cost-effective. There are quite a few obfuscators out there [52–55].

6.6.2.2 Authentication, confidentiality, and integrity

6.6.2.2.1 Authentication

Weimerskirch et al. [28] used asymmetric cryptography to authenticate ECUs. Each accredited ECU OEM is assigned with a pair of public key PK_{OEM} and a secret key SK_{OEM}. PK_{OEM} is publicly published. Each ECU stores a copy of PK_{OEM}, while SK_{OEM} is a secret and only accessible to the OEM. Each ECU is assigned a unique identification ID, a pair of public key PK_{ID} and secret key SK_{ID}, and a digital certificate

$$\{ID,\ PK_{ID}, Auth_{ID}\}\{SK_{\text{OEM}}\}$$

which consists of the ID of the ECU, its public key PK_{ID} and authorizations $Auth_{ID}$, signed by the secret key SK_{OEM} of the OEM which manufactures the ECU. The SK_{ID} is kept secret. In what follows, we use $\{content\}key$ to denote encrypted $content$ using the key.

When joining a local bus, a new ECU sends out its digital certificate to the gateway ECU of the local bus to authenticate itself. The gateway ECU verifies the new ECU by decrypting the certificate using the OEM's PK_{OEM}. There is a trust chain. The gateway ECU trusts accredited OEMs, so it trusts the ECUs that are signed by the OEMs. After authentication, the gateway ECU stores a copy of the new ECU's public key, and its authorizations, which define the access rights of the new ECU's to other buses connected via the gateway. The idea of ECU authorizations can

potentially solve the security problems introduced by bus interconnections. If an ECU fails to authenticate itself to the gateway ECU, an error code may be generated by the gateway ECU and displayed on the dashboard screen to warn the car owner.

The gateway ECU also authenticates itself by sending its digital certificate. ECUs on the connected bus store a copy of the gateway ECU's public key.

6.6.2.2.2 Confidentiality

To prevent bus sniffers from eavesdropping ECU communications, Weimerskirch et al. [28] used symmetric encryption. The gateway ECU periodically generates a random group key for a local bus and shares the group key with all authenticated ECUs on the local bus. To distribute the group key to an authenticated ECU, the gateway concatenates the group key (denoted as GK) and the time stamp (denoted as TS), encrypts the concatenation using the ECU's public key (denoted as PK_{ID}), and sends out the encrypted concatenation, $\{GK, TS\}\{PK_{ID}\}$. Then only the target ECU possessing the paired secret key SK_{ID} can decrypt and obtain the group key. This protects the secrecy of the group key. Adding the time stamp prevents replay attacks. Each authenticated ECU will apply symmetric encryption to encrypt its outgoing messages using the group key. Only authenticated ECUs with the group key can decrypt, thus the communication confidentiality is guaranteed.

Given that symmetric encryption is lighter and faster than asymmetric encryption, asymmetric encryption is used only for authentication and distribution of group keys, which involve only a few message exchanges.

When selecting symmetric encryption algorithms, we must note that canonical symmetric encryption algorithms, like AES, are unsuited for encrypting CAN messages. AES handles 128-byte data blocks, while the maximum allowable data field size in CAN protocol is 8 bytes. Traditional automakers use a proprietary message format unknown to the public as a means of security [56]. Several celebrated hacking incidents in the past few years show that this form of "security through obscurity" has not been effective.

Trillium, a Japanese startup, developed a CAN bus encryption technology called SecureCAN [57] in 2015 that supports payloads of 8 bytes or less. Three operations (substitution, transposition, and time-multiplexing) are adopted in the algorithm. Trillium claims that SecureCAN can encrypt, transmit, and decrypt within 1 millisecond, which meets the requirement for real-time CAN bus applications. The key management system is another innovation of SecureCAN. A new shared master key is generated every time the car's ignition is turned on, which can be changed at random intervals using the frequency-hopping feature.

Another way is to replace the CAN bus with CAN FD [58] to increase the bandwidth of in-vehicle network. The data field of CAN FA is now increased up to 64 bytes and data transmission speed can be over 1 Mbps. To automakers, the replacement means an increase in manufacturing cost, which impedes the promotion and application of CAN FD. Ethernet is still the most promising solution in the long run.

6.6.2.2.3 Integrity

Even with authentication and encryption, an attacker could still intercept messages, change some bits, and retransmit. Weimerskirch et al. [28] use Message Authentication Codes (MACs) for data integrity. The gateway ECU periodically generates an authentication key for a local bus and distributes it to all authenticated ECUs on the bus the same way as it distributes the group key. When

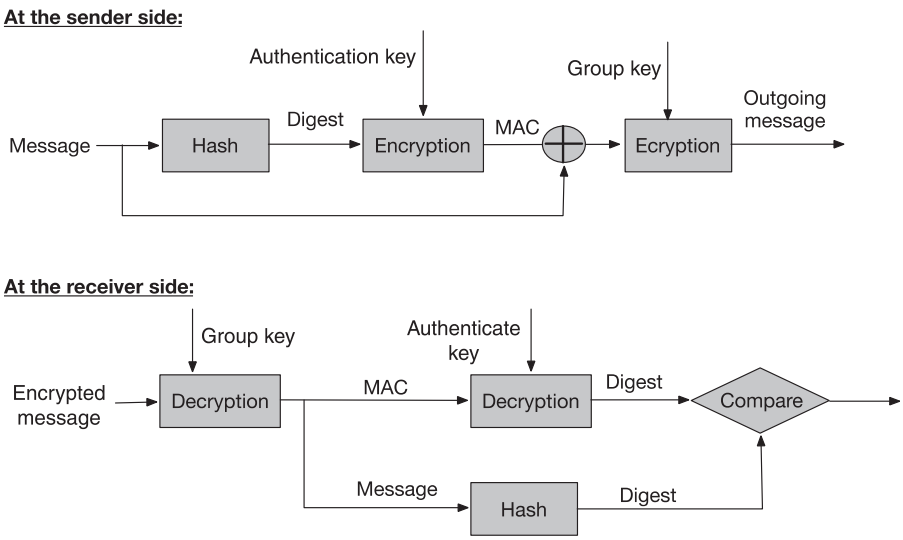

FIGURE 6.4

The use of MAC to ensure data integrity.

sending a message, an ECU first hashes the message to produce a digest. The digest is encrypted using the authentication key, producing a MAC. Then the ECU concatenates the message and the MAC, encrypts them using the group key, as shown in Fig. 6.4. At the receiver end, it first decrypts the encrypted message using the group key and obtains the message in clear-text and the MAC. Then it decrypts the MAC using the authenticate key and obtains a digest. Next it applies the hash function on the received message to produce a digest, and compares it with the received digest. If they are the same, then the message is not tampered, otherwise, the receiver drops the tampered message and reports the tampering.

The above security means rely heavily on gateway ECUs to perform authentication, generate and distribute group keys and authentication keys, and store the public keys of authenticated local ECUs. This requires that gateway ECUs be granted more computation resource and a secure memory to store the keys. The use of a digital certificate relies on a Public Key Infrastructure (PKI) to distribute public keys. Refer to Ref. [59] for PKI details.

6.6.2.3 Rootkit traps

Obfuscation and cryptographic means form the very first security barrier preventing attackers from attacking an ECU. However, neither is obfuscation unrecoverable, nor encryption uncrackable. To further strengthen the ECU security, Yu et al. [48] used a second layer of defense, which is to deploy known rootkit vulnerabilities in the ECU to trap attackers.

A rootkit is usually used by hackers to conceal their traces on a compromised system and leaves a backdoor to allow later returns without being detected [60]. For example, a loadable kernel module (LKM) rootkit can be utilized to monitor and report activities on the ECU, after the

attacker gets inside an ECU [61]. An LKM is a complied kernel code, which is not built into the kernel but can be loaded when required. It is illustrated in Ref. [61] that a kernel rootkit can deceive most rootkit detectors, such as Tripwire and AIDE. This shows that a deliberately modified LKM rootkit can be used to monitor and track all activities of an intruder while being virtually invisible to the intruder.

Metasploit and the rootkit reference work [60,62] are used to find exploits for most vulnerabilities, such as privilege escalation. Rootkits using known exploits easily attract attackers' attention, and thus are more likely to be "taken advantage of." When an embedded rootkit vulnerability is exploited, we can

- Determine if it is a malicious attack or just a system fault;
- Isolate the attack from the rest of the system if it is identified as an attack;
- Identify the type of attack;
- Study the attacker exploits especially when it is an emerging attack;
- Trace back to the attacker if possible.

This design adds one more layer of security by siphoning off attackers using rootkit vulnerability traps. It also enables the system to switch from defense to proactive aggression. Moreover, it helps improve the accuracy of intrusion detection by extracting signatures of emerging attacks.

6.6.2.4 Intrusion detection system

Larson et al. [49] proposed and evaluated specification-based IDS for the CAN 2.0 and CANOpen 3.01 protocols. The system places one detector at each ECU. The detector investigates all incoming and outgoing traffic against the specifications of the protocols. An intrusion is deemed to occur when the traffic does not agree with the specifications. Hoppe et al. [69] demonstrated an anomaly-based IDS for the CAN protocol. The system is attached to a CAN bus and listens to traffic on the bus. It records the rates of specific messages on the bus and compares them to what are considered to be normal.

6.6.2.5 Gateway firewall

Another significant vulnerability of internal buses is that they are interconnected via gateway ECUs, riskily enabling less critical ECUs (e.g., light, seat) that are connected to low-speed buses to access high-speed buses where critical ECUs (e.g., brake, transmission) are attached. An attack that exploits this vulnerability is presented in Ref. [24]. Therefore, Weimerskirch et al. [28] proposed to implement a firewall at a gateway ECU. Recall in Section 6.6.1, a gateway ECU also stores a copy of each authenticated local ECU's authorizations $Auth_{ID}$, which define the ECU's access rights to interconnected buses. When a gateway ECU receives a message from a local authenticated ECU, the firewall on the gateway ECU checks the authorizations of the local ECU. If it is authorized to access an interconnected bus, then the gateway ECU relays the message. Otherwise, it drops the message and generates an error code. In this way, a logical segmentation of internal buses is achieved. We must note that these firewalls must offer special interfaces that allow diagnostic data or ECU firmware update to pass. These interfaces must be prevented from misuse.

6.6.3 WPAN SECURITY AND PRIVACY

The in-vehicle WPAN must be secure, otherwise attackers may be able to access private information on personal devices connected to the WPAN, and gain increased access to internal CAN bus to interfere with the functionality of various ECUs [38].

6.6.3.1 Bluetooth security checklist

Bluetooth is the most widely used wireless technology for WPAN. The National Institute of Standards and Technology (NIST) and the U.S. Department of Commerce published "Wireless Network Security 802.11, Bluetooth and Handheld Device" [63]. Various recommendations are suggested in the publication for securing wireless communications and handheld wireless devices [3]. A Bluetooth security checklist containing 37 items is recommended. Out of the 37 items, 17 items are most relevant to Bluetooth WPAN including [3]:

- Ensure that handheld or small Bluetooth devices are protected from theft.
- Ensure that Bluetooth devices are turned off when not used.
- Bookkeep all Bluetooth-enabled devices.
- Change the default settings of Bluetooth devices to reflect the security policies.
- Set Bluetooth devices to the lowest necessary and sufficient power level so that transmissions remain within the secure perimeter of the agency.
- Ensure that the environment in which Bluetooth devices are bonding is secure from eavesdroppers.
- Choose PIN codes that are sufficiently random and avoid all weak PINs.
- Choose PIN codes that are sufficiently long.
- Ensure no Bluetooth device is defaulting to the zero PIN.
- At the application layer, use an alternative secure protocol for exchanging of PIN codes, for example, the Diffie–Hellman Key Exchange or Certificated-based key exchange methods.
- Ensure that combinations keys are used instead of unit keys.
- Use link encryption for all Bluetooth connections.
- Ensure device mutual authentication for all accesses.
- Ensure encryption for all broadcast for all accesses.
- Configure encryption key sizes to the maximum allowable.
- Establish a "minimum key size" for any key negotiation process.
- Ensure that portable devices with Bluetooth interfaces are configured with a password to prevent unauthorized access if lost or stolen.

6.6.3.2 Secure WPAN

WPAN is interconnected to internal buses via a WPAN gateway ECU. Maintaining secure communications between a Bluetooth device connected to a WPAN and the gateway is very crucial for normal and safe operation of the vehicle. To address this issue, Mahmud and Shanker [3] proposed to build Secure WPAN (SWPAN), in which

- Each Bluetooth device to be used is registered to the gateway, so that the gateway knows which devices are allowed to communicate with it.

- The gateway allows removal of Bluetooth devices from the list of registered devices, as devices may be lost or stolen.
- Each device has its own link keys to encrypt the communications with the gateway, to prevent other devices from eavesdropping.
- The link keys are changed frequently so that uncovering these keys are infeasible.
- The gateway generates the link keys for devices and distributes these link keys to each device in a secure way such that these keys are not compromised due to man-in-the-middle attacks.

6.6.3.3 Enabling data privacy in WPAN

Bluetooth-enabled devices can be used to track people [64]. Each Bluetooth device is assigned a unique 48-bit address at the factory. The address of a Bluetooth device can be easily obtained by simply initiating the inquiry process.

Manufacturers employ a security feature called Bluetooth low energy (BLE) or Bluetooth smart, which was introduced as part of the Bluetooth 4.0 core specification [65]. BLE disguises the MAC address while advertising packets with a random number that periodically changes. A trusted device uses an Identity Resolution Key (IRK) created during pairing to decrypt these random addresses to real MAC address. The problem with BLE is that it is poorly implemented or sometimes completely ignored. As shown in Ref. [66], these random addresses of many devices are found to be fixed. For those that do change their addresses, many of them are easy to identify as they have a counter that increments the last few bytes of the address, and often send out constant identifying information.

The most up-to-date Bluetooth version 4.2 was released in 2014, with new security features added. The new spec provides link layer security with controller-based address resolution. The MAC address of Bluetooth devices can be masked unless connecting to a trusted device.

6.6.4 SECURE VANETs

The IEEE 1609.2 standard [67] specifies four security requirements for VANET communications: confidentiality, authentication, integrity, and anonymity. For confidentiality, the standard recommends using the Elliptic Curve Integrated Encryption Scheme algorithm to encrypt messages. For authentication and integrity, the standard recommends using the Elliptic Curve Digital Signature Algorithm to sign messages. The standard also encourages the use of long cryptographic keys. The minimum recommended size of encryption keys is 256 bits, of signature keys is 224, and of public/secret keys is 256 bits. The standard also defines the format and processing of messages and the digital certificate format. The European Telecommunications Standards Institute is currently working on standards for protecting data exchanges in VANETs [68].

Privacy protection is one of the main security requirements for VANETs security [69,70] since data in VANETs is transmitted in an open access environment. Sensitive data transmitted over VANETs includes, but is not limited to, vehicle location, driver identity, driving behavior, location of the vehicle, internal car sensor data.

Many research efforts have considered VANETs privacy. Most efforts focus on communication schemes. The adoption of pseudonyms (PNs) instead of using the identities of vehicle makes the VANET communications anonymous and improves privacy [71,72]. Each vehicle, V generates a set of public/secret key pairs, $\left(PK_V^1, SK_V^1\right), \left(PK_V^2, SK_V^2\right), \cdots \left(PK_V^n, SK_V^n\right)$, and sends over a secure

channel the public keys (i.e., $PK_V^1, PK_V^2, \cdots PK_V^n$) to a Certificate Authority (CA). All vehicles and roadside units trust the CA and store a copy of the public key of the CA. The CA generates a set of PNs for the vehicle V (i.e., $PN_V^1, PN_V^2, \cdots PN_V^n$). PN_V^icontains $ID_{CA,}$ the identifier of the CA, $T,$ the lifetime of PN_V^i, and PK_V^i, the public keyof vehicle V, signed by the CA:

$$\{ID_{CA},\ T,\ PK_V^i\}\{SK_{CA}\}$$

CA sends over the same secure channel the set of PNs back to vehicle V. When communicating with other vehicles or roadside units, vehicle V can authenticate itself by using the PNs instead of revealing its true identity.

An alternative to PNs is to use anonymous keys [73]. Each vehicle is preinstalled with a set of one-time anonymous keys certified by a CA. Anonymous keys can be updated in a yearly checkup. A privacy preserving protocol called Efficient Conditional Privacy Preservation Protocol (ECPP) for anonymous VANETs communication is presented in Ref. [74], where an anonymous key is valid for a short time period after generation. The scheme introduced in Ref. [75], uses a set of short-time PNs for message encryption. Each PN is associated with a key pair and a certificate for message encryption. The receiver of a message turns to a certificate revocation list (CRL) to validate the attached certificate. Messages are signed on behalf of a group of signing keys so the vehicles' identify will not be divulged. Grouping vehicles traveling at the same speed and in the same direction was proposed in Ref. [76]. Members of the group could anonymously issue and sign messages with a group signature on behalf of the group.

A decentralized group-authentication protocol is proposed in Ref. [77] as an alternative to a CA. Vehicles in the range of the same roadside unit or service centers are considered in the same group and managed by each roadside unit. Vehicles in the same group can verify each other's messages using a secret member key obtained from the roadside unit. The viability of the protocol is based on a dense spread of roadside units. The scheme proposed in Ref. [78] uses k-anonymity, where k vehicles in a region are assigned the same PN for communicating with roadside units or service centers. Using this scheme, an attacker can only detect a group of cars receiving the message but cannot determine which one in particular.

Most privacy preserving technologies rely heavily on time-consuming cryptographic operations and generate a large volume of cryptographic data. For example, in DSRC, a vehicle broadcasts messages to all nearby vehicles every few milliseconds. On the other end of the communication, a vehicle may receive hundreds of messages within a short time period, which need to be verified in real-time. This may cause an unacceptable delay. To tackle this, Zhang et al. proposed a privacy preserving protocol called APPA built on one-time identity-based aggregate signature [79]. A one-time signature is generated using a secret key obtained from the trusted authority. The secret key is associated with a one-time PN, which guarantees the anonymity of the vehicles. Since an aggregate signature algorithm is employed, the signatures on different messages from different vehicles can be aggregated into one signature, which can be verified as a single signature. This feature greatly curtails the time for verification, as well as the storage space for cryptographic data.

Given the above, we can see that most privacy solutions in VANETs involve use of PNs and require the presence of CAs for key management. Generated cryptographic data adds excessive overhead to practical applications. Privacy-preserving techniques for VANETs still call for effective and efficient solutions.

6.6.5 SECURE OTA ECU FIRMWARE UPDATE

Fig. 6.5 shows an overview of OTA ECU firmware update. The update process is initiated by the backend server, which remotely sends an update command to the TCU of an on-board network. Before actual update, the target ECU to be updated needs to send its specifications (e.g., ECU types, firmware version, etc.) to the server to ensure the correct firmware will be used. Though OTA update is rare now, its security has been studied. It is a good practice to embed security at the beginning during the development of an application, rather than distribute security add-ons after being attacked.

To secure the OTA update process, all the components and communication channels involved in the process must be secured. End-to-end security must be provided. The security requirements are identified in Ref. [51] as:

- *Code Origin Authenticity*: An ECU can verify that the firmware to be installed is from the OEM. Any faulty firmware must be denied.
- *Code Integrity*: An ECU can detect any unauthorized modification of the firmware since it leaves the backend servers. Faulty or modified firmware must be denied.
- *Code Confidentiality*: The content of the firmware should remain confidential during the transmission and installation.
- *Update Metadata Confidentiality:* This requirement ensures that an attacker should not gain the information out of the update process about the specifications of the target ECU (e.g., ECU types, version of current firmware) and the firmware version to be used.
- *Availability:* This requirement ensures that the TCU, target ECU, and buses are available throughout the update process.
- *Command Freshness:* This requirement prevents the replay attack that an attacker sends an old update command to deceit the target ECU.
- *Message Source Authenticity.* This requirement ensures that during the process, the target ECU must verify that the received messages are from the backend server. Man-in-the-middle attack can occur if this requirement is not satisfied.

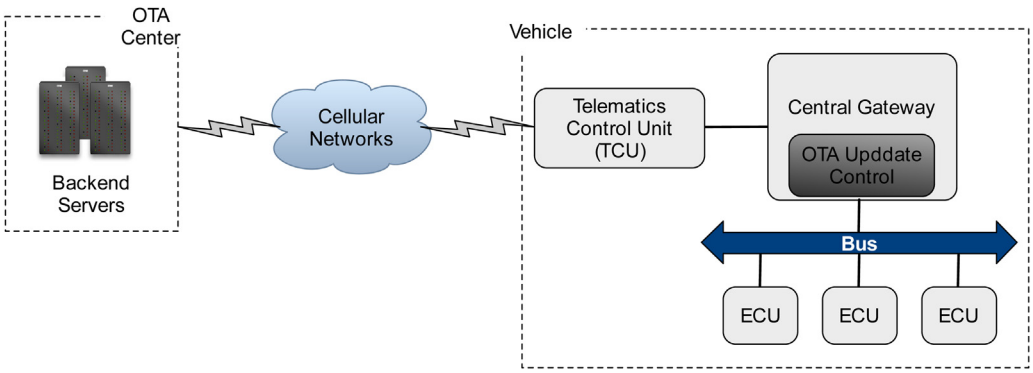

FIGURE 6.5

An overview of OTA ECU firmware update.

A secure protocol for OTA firmware update is proposed in Ref. [80]. The message exchanged defined by the protocol is depicted in Fig. 6.6. The protocol relies on Hardware Security Module (HSM) to provide security features. HSM is responsible for performing all the cryptographic operations including symmetric/asymmetric encryption/decryption, integrity checking, digital signature creation/verification, and random number generation. Each ECU includes a HSM. The protocol satisfies all the security requirements above. In Fig. 6.6, each of the three components (backend server, TCU, and target ECU) has a pair of public key and secret key, and the public keys of the other two components. The backend server also has *SSK*, which is the key for encrypting/decrypting firmware. The process is divided into four phases: Remote Diagnosis, ECU Reprogramming Mode, *SSK* Exchange, and Firmware Download.

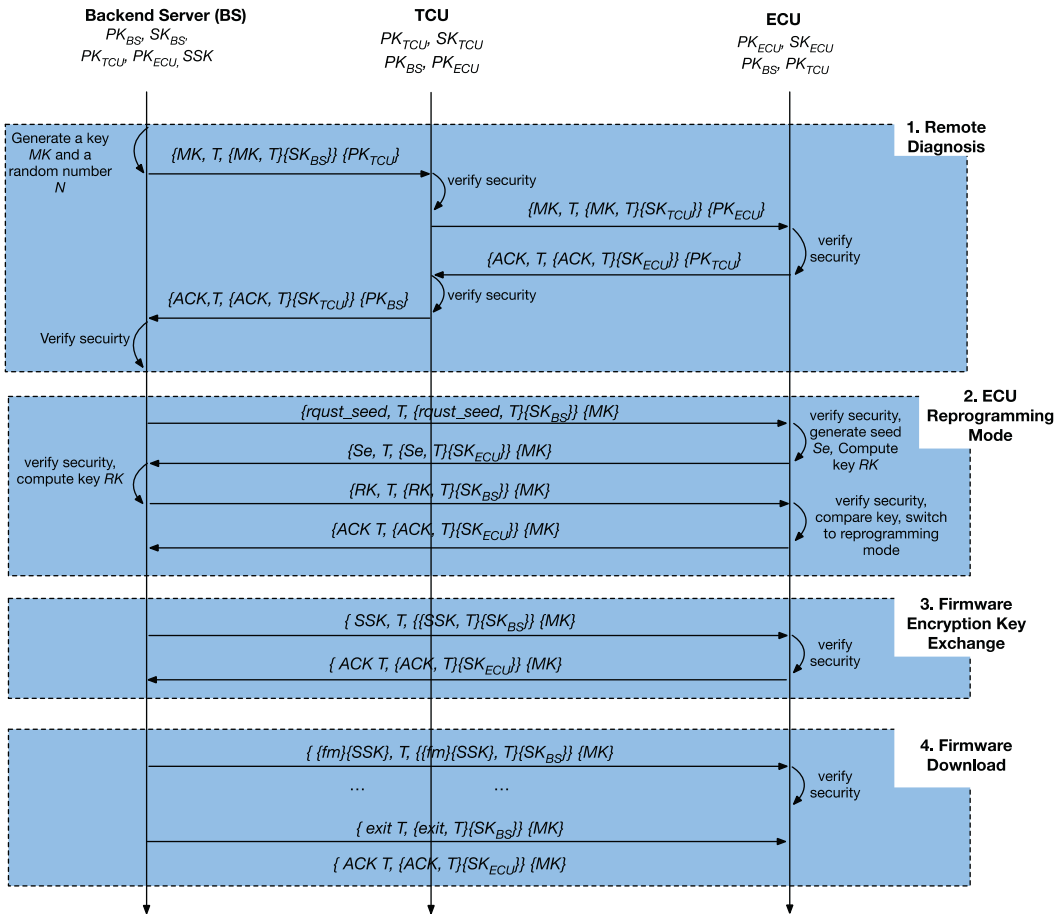

FIGURE 6.6

Secure protocol for OTA ECU firmware update.

The Remote Diagnosis phase authenticates the backend server and the ECU to each other and establishes a session key (MK) for later message encryption/decryption:

- The backend server initiates the update process by requesting the ECU specifications. To do so, it generates MK, concatenates it with time stamp (T), signs the concatenation with its secret key (SK_{BS}) to produce a MAC, concatenates the MAC with MK and T, encrypts with the public key of TCU, and sends to TCU the encrypted message

$$\{M, T, MAC\}\{PK_{TCU}\}$$

  Where, $MAC = \{MK, T\}SK_{BS}$. This message can only be decrypted by TCU. Confidentiality is guaranteed.
- The TCU decrypts with its secret key SK_{TCU} to get MK, T, and the MAC. Then, it decrypts the MAC using the backend server's public key PK_{BS}, and compares the MK and T with the previously obtained values to detect message tampering. The message authenticity is also verified as the MAC can only be signed (encrypted) by the backend server, who owns SK_{BS}. The T is used to check message freshness to prevent replay attacks. After verifications, TCU sends to ECU the similar message

$$\{M, T, \{M, T\}\{SK_{TCU}\}\}\{PK_{ECU}\}$$

- The ECU performs the same verification, and sends back an acknowledgment message.

In this way, the backend server can successfully authenticate itself to the ECU, and distribute MK to the ECU. A secure communication channel between the two can be established. From now on, all the communications will be encrypted using MK. The ECU will send its specifications, encrypted using MK, to the backend server.

After completing the first phase, the backend server will force the ECU to switch to the reprogramming mode. In phase three, the backend server distributes the SSK key to the ECU, which will be used in phase 4 to decrypt firmware. In phase 4, the backend server sends the firmware to the ECU. When it finishes, it sends an *exit* message to the ECU. The ECU returns an acknowledgment message.

The protocol has satisfied all the requirements identified. Other security solutions can be found in Refs. [81–82].

6.6.6 PRIVACY MEASUREMENT OF SENSOR DATA

The internals of a connected vehicle are a swarm of sensors. Although sensor data may not contain Personal Identification information (PII), traffic analysis technologies can be adopted to infer sensitive information from side channels (timing, message size, communication frequency, etc.). Standard privacy preserving techniques like Privacy Preserving Data Mining (PPDM) [83] use noise addition and information suppression. Research has gone into evaluating privacy in Internet of Things (IoT) systems like connected vehicles.

Ukil et al. [84] propose a risk estimation scheme that allows users of IoT systems such as connected vehicles to estimate the risking of sharing private data. In their work, sensitive or private data is defined as *unpredictable anomalous events that may arouse curiosity or undue interest*. Anomalies in sensor data make them distinguishable and thus pose a serious threat to data privacy.

The proposed scheme consists of two steps: sensitivity (anomaly) detection and measurement of privacy/sensitivity. The detection algorithm discovers the anomaly points in a given sensor dataset while optimizing the masking and swamping effects. The detection method shows superior detection performance when compared with other outlier detection algorithms [85,86] in terms of larger KullbackLeibler (KL) distance. According to Sanov's theorem [87], a larger KL distance indicates better detection capability. Given a dataset S, the privacy metric ρ_M is defined as mutual information $I(S, v)$, where v is the sensitive/anomalous part of S. To improve the accuracy of ρ_M as privacy metric, a statistical compensation ρ_S is computed using the Kolmogorov−Smirnov (KS) test of S and v. The rule is ρ_S, if the null hypothesis is rejected; otherwise, $\rho_S = W_{S,v}$ where $W_{S,v}$ is the $L1$-Wasserstein metric between S and v and quantifies the distance between distributions S and v. The privacy is defined as $\rho_Q = \rho_S \times \rho_M$, where $\rho_Q \in [0, 1]$ is in proportion to the privacy risk of S. If ρ_Q exceeds a predefined threshold, the privacy preserving sensor data S' computed using standard PPDM is shared with the third party.

6.6.7 SECURE HANDOVER

As the vehicle roams, it may pass through heterogeneous networks. Current academic and industrial efforts focus on seamless handovers with the least interruption on communication sessions. IEEE 802.21 (Media independent Handover) mainly defines an architecture to enable low-latency handover across multiple technology access networks [88]. Software Defined Networking (SDN) is also proposed to handle handovers to provide session continuity [89].

When a handover occurs, the roaming vehicle needs to authenticate itself to the new network (base station or access point) and other connected vehicles in the new network. This problem is known as AAA (Authenticate and Authenticate Again). AAA can seriously degrade user quality of service (QoS). This is likely to be an especially problematic issue for vehicles traveling at high speed that wish to maintain connectivity with minimal user distraction. A recent survey of AAA optimization techniques (e.g. AAA Context Transfer methodology) can be found in [90].

A vehicle may travel to a less secure network. To protect ongoing communication sessions, we suggest using the Transport Layer Security (TLS) for communication sessions requiring protection. TLS is a cryptographic protocol that provides authentication and communication confidentiality. TLS works at the presentation layer (layer 6) of the OSI stack. Current 802.21 plans work at both layer 2 (data link) and layer 3 (network). TLS should normally be able to coexist with 802.21.

6.7 FUTURE RESEARCH DIRECTIONS

Increasing the security of automotive systems will be difficult. Many of the basic security problems are baked into the current bus standards. No individual manufacturer or supplier would be able to make the necessary changes and remain competitive in a low-margin business. An industry wide change would be needed, but that would leave a large number of legacy automobiles. Numerous new approaches could be made to monitor and filter information on the automotive bus systems. Technologies also *exist* to help secure individual ECUs. We present some here. Other ideas could

leverage recent advances in trusted computing that add a hardware root of trust to make infecting the devices more difficult. All of these research ideas could be helpful, but in many ways the key problem is constrained by the economics of the automotive industry.

6.8 SUMMARY AND CONCLUSIONS

This chapter presents a security profile for connected vehicle systems. Multiple vulnerabilities are analyzed and existing attacks are surveyed. To analyze the attacks, we map them to the attack taxonomy that describes attacks on connected vehicle systems. This mapping helps us find the problem space and locate common vulnerabilities. Various security solutions to the security and privacy issues are presented as well. Cryptographic measures are mainly used. However, we must be aware that these measures rely on PKI to distribute keys. First of all, PKI has known security flaws [91]. Second, no real PKI implementation exists for many of these domains. These issues need to be addressed.

6.9 EXERCISES

Exercise 1. List all the in-vehicle networks and study their security features, if any.
Exercise 2. Explain the vulnerabilities of in-vehicle networks.
Exercise 3. Understand the challenges in securing ECU communications.
Exercise 4. Try design security policies for a ECU gateway that connects two different in-vehicle networks.
Exercise 5. Understand the attack surface enabled by external vehicle networks.
Exercise 6. Study the privacy issues of VANET and the solutions to address them.

REFERENCES

[1] R.R. Brooks, S. Sander, J. Deng, J. Taiber, Automobile security concerns, IEEE Vehic. Technol. 4 (2) (2009) 52–64.
[2] S.A. Weis, S.E. Sarma, R.L. Rivest, D.W. Engels, Security and privacy aspects of low-cost radio frequency identification System, Proceeding of the 1st International Conference on Security in Pervasive Computing, Springer, 2004, pp. 201–212.
[3] S. Mahmud, S. Shanker, In-vehicle secure wireless personal area network (SWPAN), IEEE Trans. Veh. Technol. 55 (3)) (2006) 1051–1061.
[4] http://www.ford.com/technology/sync/, accessed (9.10.16).
[5] https://www.onstar.com/us/en/home.html, (accessed 9.10.16).
[6] http://www.toyota.com/owners/parts-service/safety-connect, (accessed 9.10.16).
[7] http://www.lexus.com/enform, (accessed 9.10.16).
[8] http://www.bmw.com/com/en/insights/technology/connecteddrive/2013/, (accessed 9.10.16).
[9] https://www.mbusa.com/mercedes/mbrace, (accessed 8.10.16).

[10] https://www.linkedin.com/pulse/information-security-connected-vehicle-shashank-dhaneshwar, (accessed 24.05.16).
[11] H. Kitayama, S. Munetoh, K. Ohnishi, N. Uramoto, Y. Watanabe, Advanced security and privacy in connected vehicles, IBM Res. Dev. 58 (1) (2014).
[12] http://www.iteris.com/cvria/html/applications/applications.html, (accessed 9.10.16).
[13] http://www.oesa.org/Publications/OESA-News/August-2015/ver-the-Air-Updates-to-Become-Commonplace-in-Vehicles.html, (accessed 24.05.16).
[14] https://www.onstar.com/us/en/home.html, (accessed 24.05.16).
[15] http://resources.infosecinstitute.com/hacking-autoupdate-evilgrade/, (accessed 10.06.16).
[16] https://www.youtube.com/watch?v=oHDwKT564Kk, (accessed 24.05.16).
[17] J. Muller, No hands no feet: My unnerving ride in Google's driverless car. Available from: <www.forbes.com/sites/joannmuller/2013/03/21/no-hands-no-feetmy-unnerving-ride-in-googles-driverless-car>, (accessed 24.05.16).
[18] http://news.mit.edu/2016/startup-nutonomy-driverless-taxi-service-singapore-0324, (accessed 24.05.16).
[19] https://www.ietf.org/proceedings/63/slides/nemo-4.pdf, (accessed 6.06.16).
[20] R.R. Brooks, S. Sander, J. Deng, J. Taiber, Automotive system security: challenges and state-of-the-art, Proceedings of the 4th annual workshop on Cyber security and information intelligence research: developing strategies to meet the cyber security and information intelligence challenges ahead, ACM, 2008, May, p. 26.
[21] J.D. Howard, T.A. Longstaff, A Common Language for Computer Security Incidents, Sandia Report, SAND98-8867, Sandian National Laboratory, 2007.
[22] S.C. Bono, M. Green, A. Stubblefield, Security analysis of a cryptographically-enabled FRID device, Proceeding of 14th conference on Usenix Security Symposium, vol. 14, 2005.
[23] A.I. Alrabady, S.M. Mahmud, Analysis of attacks against the security of keyless-entry systems for vehicles and suggestions for improved designs, IEEE Trans. Vehic. Techonol. 54 (1)) (2005) 41−50.
[24] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham and S. Savage, Experimental security analysis of a modern automobile, IEEE Symposium on Security and Privacy, 2010.
[25] T. Hoppe, S. Kiltz, J. Dittmann, Security threats to automotive CAN networks − practical examples and selected short-term countermeasures, Proceeding of the 27th International Conference on Computer Safety, Reliability, and Security, Newcastle upon Tyne, Springer-Verlag, UK, 2008, pp. 235−248.
[26] D.K. Nillson, U.E. Larson, Simulated attacks on can buses: Vehicle virus, Proceeding of the 5th IASTED International Conference on Communication Systems and Networks, ACTA Press, 2008, pp. 66−72.
[27] S. Misra, I. Woungang, S.C. Misra, Guide to Wireless ad hoc Networks, Springer Science & Business Media, 2009.
[28] A. Stampoulis, Z. Chai, A survey of security in vehicular networks, Project CPSC 534 (2007).
[29] T.C. Niem, Bluetooth and its inherent security issues, Global Information Assurance Certification Security Essentials Certification, Research Project, Version 1.4b, Nov. 4, 2002. [Online] https://www.sans.org/reading-room/whitepapers/wireless/bluetooth-inherent-security-issues-945.
[30] S. Indesteege, N. Keller, O. Dunkelman, E. Biham, B. Preneel, A practical attack on Keeloq, in: N. Smart (Ed.), Eurocrypt'08,volume 4965 of LNCS, Springer-Verlag, 2008, pp. 1−18.
[31] http://www.bbc.com/news/technology-29786320 (accessed 25.05.16).
[32] A. Francillon, B. Danev, S. Capkun, Relay Attacks on Passive Keyless Entry and Start Systems in Modern Carsin: A. Perrig (Ed.), NDSS, 2011.
[33] http://www.autoalarmpro.com/bypass_kits, (accessed 25.05.16).

[34] https://www.directechs.com/default.aspx, (accessed 25.05.16).
[35] http://www.clickorlando.com/news/local/orlando/thieves-use-device-to-jam-keyless-entry-systems, (accessed 25.05.16).
[36] http://articles.sun-sentinel.com/2012-12-28/news/fl-pirate-radio-hollywood-20121229_1_pirate-radio-entry-systems-keyless-entry, (accessed 25.05.16).
[37] http://thehackernews.com/2015/08/rolljam-unlock-car-garage.html, (accessed 26.05.2016).
[38] S. Checkoway, Damon McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno, Comprehensive experimental analysis of automotive attack surfaces, Proceeding of USENIX security, 2016, pp. 1–16.
[39] Last accessed on June 21, 2016.
[40] H.M. Song, H.R. Kim, H.K. Kim, Intrusion detection system based on the analysis of time intervals of can messages for in-vehicle network, Proceeding of 2016 International Conference on Information Networking (ICOIN), IEEE, 2016, pp. 63–68.
[41] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, et al., in: I. Goldberg (Ed.), Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study, USENIX Security, 2010, pp. 323–328.
[42] Y. Lindell, B. Pinkas, Privacy Preserving Data Mining, Advances in CryptologyCRYPTO 2000, Springer, 2000, pp. 36–54.
[43] A. Ukil, S. Bandyopadhyay, A. Pal, Iot-privacy: To be private or not to be private, Computer Communications Workshops (IN- FOCOM WKSHPS), 2014 IEEE Conference on, IEEE, 2014 pp. 123–124.
[44] R. Rao, S. Akella, G. Guley, Power line carrier (plc) signal analysis of smart meters for outlier detection, 2011 IEEE International Conference on Smart Grid Communications (SmartGridComm), IEEE, 2011, pp. 291–296.
[45] R. M. d. Nascimento, A.P. Oening, D.C. Marcilio, A.R. Aoki, E. de Paula Rocha, J.M. Schiochet, Outliers' detection and filling algorithms for smart metering centers, Transmission and Distribution Conference and Exposition (T&D), 2012 IEEE PES, IEEE, 2012, pp. 1–6.
[46] I. Sanov, On the Probability of Large Deviations of Random Variables, United States Air Force, Office of Scientific Research, 1958.
[47] Letter to the FTC. [Online] <http://www.autoalliance.org/auto-issues/automotive-privacy/letter-to-the-ftc>, (accessed 9.10.16).
[48] L. Yu, J. Deng, R.R. Brooks, SeokBae Yun, Automotive ECU design to avoid software tampering, Proceeding of Cyber Information Security Research Conference (CISR'15), Oak Ridge, TN, 2015.
[49] U.E. Larson, D.K. Nillson, E. Jonsson, An approach to specification-based attack detection for in-vehicle networks, Proceeding of the IEEE Intelligent Vehicles Symposium, 2008, pp. 220–225.
[50] V. Verendel, D.K. Nilsson, U.E. Larson, E. Jonsson, An approach to use honeypots in in-vehicle networks, Proceeding of the 68th IEEE Vehicular Technology Conference, 2008, pp. 163–172.
[51] M.S. Idrees, Y. Roudier, Computer aided design of a firmware flashing protocol for vehicle on-board networks, Research Report RR-09-235, 2009.
[52] https://jscrambler.com/en/, (accessed 10.06.16).
[53] http://stunnix.com/prod/cxxo/. (accessed 20.06.16).
[54] https://javascriptobfuscator.com/ (accessed 20.06.16).
[55] http://www.semdesigns.com/Products/Obfuscators/, (accessed 20.06.16).
[56] R. Currie, Developments in car hacking, Technical report, 2015.
[57] J. Yoshida, Can bus can be encrypted, says trillium. <http://www.eetimes.com/document.asp?doc id=1328081>, 2015.
[58] F. Hartwich, Can with flexible data-rate, Citeseer.

[59] https://en.wikipedia.org/wiki/Public_key_infrastructure, (accessed 3.06.06).
[60] G. Hoglund, J. Butler, Rootkits: Subverting the Windows Kernel, Addison-Wesley Professional, 2006.
[61] J. Rose, Turning the Tables: Loadable Kernel Module Root Kits,Deployed in a Honeypot Environment, SANS Institute InfoSec Reading Room, 2003.
[62] Windows rootkit overview. Symantec, 2006.
[63] T. Karygiannis and L. Owens, Wireless network security 802.11, Bluetooth and handheld devices, National Inst. Standards Tech., Technol. Admin., U.S. Dept. Commerce. NIST Special Publication 800−848.
[64] http://electronics.howstuffworks.com/bluetooth-surveillance2.htm, (accessed 16.06.16).
[65] Bluetooth, Adopted specifications. <https://www.bluetooth.com/specifications/adopted-specifications>.
[66] S. Lester, The emergence of bluetooth low energy. <http://www.contextis.com/resources/blog/emergence-bluetooth-low-energy/>.
[67] IEEE Trial-Use Standard for Wireless Access in Vehicular Environments−Security Services for Applications and management Messages, IEEE Std., July 2006.
[68] Benhaddou Driss, Ala Al-Fuqaha (Eds.), Wireless Sensor and Mobile Ad-Hoc Networks: Vehicular and Space Applications, Springer, 2015.
[69] T. Hoppe and J. Dittmann, Sniffing/Replay attacks on CAN buses: a simulated attack on the electric window lift classified using an adapted CERT taxonomy, Proceeding of the 2nd Workshop on Embedded Systems Security, Salzburg, Australia, 2007.
[70] M. Wolf, A. Weimerskirch, C. Paar, in: C. Paar (Ed.), Secure In-Vehicle Communication, ESCAR, 2004.
[71] P. Papadimitratos, L. Buttyan, J.P. Hubaux, F. Kargl, A. Kung, M. Raya, Architecture for secure and private vehicular communications, Proceeding of 7th International Conference on ITS, IEEE, 2007, pp. 1−6.
[72] F. Dötzer, Privacy issues in vehicular ad hoc networks, Privacy enhancing technologies, Springer, 2005, pp. 197−209.
[73] M. Raya, P. Papadimitratos, J.P. Hubaux, Securing vehicular communications, IEEE Wireless Communications Magazine, Special Issue on Inter-Vehicular Communications, 13(LCA-ARTICLE-2006-015) (2006) 8−15.
[74] R. Lu, X. Lin, H. Zhu, P.H. Ho, X. Shen, ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications, INFOCOM 2008, The 27th Conference on Computer Communications, IEEE, 2008.
[75] G. Calandriello, P. Papadimitratos, J.P. Hubaux, A. Lioy, Efficient and robust pseudonymous authentication in vanet, Proceedings of the fourth ACM International Workshop on Vehicular ad hoc Networks, ACM, 2007, pp. 19−28.
[76] K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, K. Sezaki, Caravan: Providing location privacy for vanet, Technical report, DTIC Document, 2005.
[77] L. Zhang, Q. Wu, A. Solanas, J. Domingo-Ferrer, A scalable robust authentication protocol for secure vehicular communications, IEEE Trans. Vehic. Technol. 59 (4) (2010) 1606−1617.
[78] C. Zhang, X. Lin, R. Lu, P.H. Ho, X. Shen, An efficient message authentication scheme for vehicular communications, IEEE Trans. Vehic. Technol. 57 (6) (2008) 3357−3368.
[79] L. Zhang, Q. Wu, B. Qin, J. Domingo-Ferrer, APPA: Aggregate Privacy-Preserving Authentication in Vehicular ad hoc Networks, Information Security, Springer, 2011, pp. 293−308.
[80] M.S. Idrees, H. Schweppe, Y. Roudier, M. Wolf, D. Scheuermann, O. Henniger, Secure automotive on-board protocols: A case of over-the-air firmware updates, Proceeding of 3rd International Workshop on Nets4Cars/Nets4Trains, Oberpfaffenhofen, Germany, 2011.
[81] D. Nilsson and U. Larson, Secure firmware updates over the air in intelligent vehicles, Proceeding of IEEE International Conference on Communications workshops, 2008, pp. 380−384.

[82] S. Mahmud, S. Shanker, I. Hossain, Secure software upload in an intelligent vehicle via wireless communication links, Proceeding of IEEE Intelligent Vehicle Symposium, 2005, pp. 588–593.
[83] B. Parno, A. Perrig, Challenges in securing vehicular networks, Proceeding of the 4th Workshop Hot Topics in Networks (HotNet-IV), 2005.
[84] I.A. Sumra, I. Ahmad, H. Hasbullah, J.L.B.A. Manan, Classes of attacks in VANET. In Electronics, Communications and Photonics Conference (SIECPC), 2011 Saudi International, IEEE, pp. 1–5.
[85] V.H. La, A. Cavalli, Security attacks and solutions in vehicular ad hoc networks: A survey, Int. J. AdHoc Networking Syst. (IJANS) 4 (2) (2014) 1–20.
[86] S.K. Das, K. Kant, N. Zhang, Handbook on Securing Cyber-Physical Critical Infrastructure, Elsevier, 2012.
[87] A.S.K. Pathan (Ed.), Security of Self-Organizing Networks: MANET, WSN, WMN, VANET, CRC Press, 2016.
[88] http://www.ieee802.org/21/, (accessed 1.06.16).
[89] groups.geni.net/geni/raw-attachment/wiki/GEC21Agenda/.../GEC21poster-V3.pdf, (accessed 1.06.16).
[90] G. Karopoulos, G. Kambourakis, S. Gritzalis, Survey of secure handoff optimization schemes for multimedia services over all-IP wireless heterogeneous networks, IEEE Commun. Surveys 9 (3) (2007) 18–28 3rdQuarter.
[91] R.R. Brooks, Introduction to Computer and Network Security: Navigating Shades of Gray, CRC Press, Boca Raton, FL, 2014.