INVITED PAPER *Special Section on Information and Communication System Security*

An Overview of Cyber Security for Connected Vehicles

Junko TAKAHASHI[†a)], ***Member***

SUMMARY The demand for and the scope of connected services have rapidly grown and developed in many industries such as electronic appliances, robotics, and industry automation. In the automotive field, including connected vehicles, different types of connected services have become available and they provide convenience and comfort with users while yielding new business opportunities. With the advent of connected vehicles, the threat of cyber attacks has become a serious issue and protection methods against these attacks are urgently needed to provide safe and secure connected services. From 2017, attack methods have become more sophisticated through different attack surfaces attached to navigation systems and telematics modules, and security requirements to circumvent such attacks have begun to be established. Individual threats have been addressed previously; however, there are few reports that provide an overview of cyber security related to connected vehicles. This paper gives our perspective on cyber security for connected vehicles based on a survey of recent studies related to vehicle security. To introduce these studies, the environment surrounding connected vehicles is classified into three categories: inside the vehicle, communications between the back-end systems and vehicles, and the back-end systems. In each category, this paper introduces recent trends in cyber attacks and the protection requirements that should be developed for connected services. We show that the overall security covering the three categories must be considered because the security of the vehicle is jeopardized even if one item in the categories is not covered. We believe that this paper will further contribute to development of all service systems related to connected vehicles including autonomous vehicles and to the investigation into cyber security against these attacks.

key words: *automotive security, cyber security, connected vehicles, autonomous driving, connected services, in-vehicle protocol*

1. Introduction

The sector of the automotive field known as connected vehicles has rapidly grown. The connected vehicles are generally defined as the vehicles that are equipped with Internet communication functions for improving user convenience. The environment surrounding vehicles is shifting from a closed network to an open network that connects to outside networks. The report by Fuji Keizai Co. predicts that the worldwide market for passenger-type connected vehicles will be 9,900 million units by 2035 and almost all brand-new vehicles will be equipped with connected systems or services by 2035 [1]. With the increase in the number of connected vehicles, new services such as car sharing and dispatch services have proliferated and it is expected that simple and convenient driving will be achieved in an environmentally-friendly and efficient way. From the aspect of comfortable driving, user stress related to driving can be reduced using remote or autonomous functions. For example, we have remote-control door locks and the remote function that flashes the headlights when searching for a vehicle in a crowded parking area [2]. Furthermore, we can verify the battery power of electric vehicles (EVs) [2] regardless of location. Just recently in 2017, remote parking has been actualized in some vehicles such as the Audi A8 [3], Tesla model S [4], and Nissan leaf EV [5]. These systems are achieved through a smartphone application. Some companies try to utilize the vehicle information shared through the networks, referred to as telematics, for their businesses for example a car dealer may use it for vehicle maintenance or an assurance company may use it to calculate insurance rates.

Autonomous driving is also related to connected vehicles. At this time, 2018-model year vehicles have achieved level 3 self-driving [3], although this is mainly achieved through sensors attached to the vehicle itself. However, vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communications for connected vehicles will also be used for autonomous driving. V2V is the data exchange between the vehicles and V2I is the data exchange between the vehicle and the infrastructure such as traffic lights as examples. It is considered that these types of communications avoid traffic congestion by exchanging various types of information such as that regarding road conditions with other vehicles through the Internet [6].

Google autonomous driving, which is a service achieved by integrating the vehicle and telecommunications, is a major autonomous driving system [7]. Google also launched the Android Auto platform, which is an in-vehicle device software based on Android. This platform actualizes an easier way to access information on a smartphone in a vehicle by integrating the smartphone and navigation systems [8]. Some car manufacturers are partnering with Google to bring the Android platform to vehicles. Apple launched the CarPlay platform with cooperation from many car manufactures and this platform actualizes iPhone use in vehicles through the navigation system [9]. Automotive Grade Linux (AGL) [10], which is a collaborative open source project, is also being developed for connected vehicles by many car manufacturers, suppliers, and related technology companies. This project because it is open source would make it easier to develop in-vehicle infotainment (IVI) systems.

Thus, new services and systems for connected vehicles

Manuscript received April 17, 2018.
Manuscript publicized August 22, 2018.

[†]The author is with NTT Secure Platform Laboratories, NTT Corporation, Musashino-shi, 180–8585 Japan.
a) E-mail: junko.takahashi.fc@hco.ntt.co.jp

DOI: 10.1587/transinf.2017ICI0001

have been rapidly developed and have brought us in-vehicle convenience and comfort. However, from the aspect of cyber security, connected vehicles have come under threat because connected systems have interfaces to outside networks that are vulnerable and may affect the vehicle control systems.

Due to this, vehicle security has attracted attention and abnormal behavior has been actually induced in real vehicles. Research results in the field of remote attacks against vehicles shocked vehicle manufactures [11] and this triggered a recall of 1.4 million vehicles. Subsequently, other researchers hacked Tesla vehicles and they showed that they could remotely control the vehicle including critical vehicle controls [12]. An attack that could possibly remotely inject a Controller Area Network (CAN) command through the telematics unit in a Nissan Leaf was reported utilizing well-known attack techniques using an iOS [13]. This study shows that well-known smartphone vulnerabilities are not shared with the automobile industry. Thus, recent studies from 2016 have shown that more and more remote attacks can be performed through vehicle systems connected to outside networks although direct message injection attacks have been the major focus in past years [14]–[16].

With the increase in the sophistication and number of advanced attack techniques, protection methods have been discussed and developed in information technology (IT) security which is used in the personal computers (PC) and server fields. Protection methods for direct attacks have already been installed in modern vehicles. For example, a gateway between the port and the in-vehicle network has already been installed in modern Japanese domestic cars and imported cars based on the type of vehicle in 2017. In the near future, some other protection techniques are to be installed in vehicles such as secure boot systems for the electronic control unit (ECU) [17], message authentication codes (MACs) [18]–[20], and Intrusion Detection Systems [21]–[23]. For connected vehicles, in addition to in-vehicle security, we consider that the security surrounding the vehicles such as back-end systems, communications outside the vehicles, and the smartphone applications is significant because a lack of security in any one of the environments may trigger the serious abnormal control of the vehicles based on prior history.

Most previous studies showed individual attack techniques or protection methods and focused on the novelty of the specific technique. There are only a few reports that give an overview of connected vehicle security and show the relationship between them based on recent hacking and protection technology. Furthermore, to the best of our knowledge, there are no reports that focus on the importance of the overall security surrounding the connected vehicles to ensure vehicle security.

In this paper, we describe our perspective on connected vehicle security based on recent hacking and protection techniques. We classify the environment surrounding connected vehicles into three categories: in-vehicle, communications between the back-end system and vehicles, and the back-end system of the service providers. We introduce recent cyber-attack threats and the requirements based on the three categories. Through an overview of these threats, we show the importance of the overall security surrounding connected vehicles to protect vehicles from cyber attacks. We also show that secure systems would be disrupted even if one of the security items is not covered in the three categories. We believe that this paper is informative in developing and utilizing connected vehicle services and in investigating cyber security of connected vehicles.

In the rest of the paper, Sect. 2 provides background information on the environment surrounding connected vehicles. Section 3 describes recent hacking techniques and their security requirements in the in-vehicle category. In Sects. 4 and 5, we describe the threats and requirements in the communication category between the vehicles and the back-end system and in the back-end system category, respectively. We also describe other significant contents for connected-car security which are not covered in previous sections in Sect. 6. Finally, we conclude the paper in Sect. 7.

2. Environments Surrounding Connected Vehicles

This section introduces a general structure for connected vehicles to describe the importance of the overall security.

Up to now, the vehicle navigation system could establish a link to a passenger smartphone through Bluetooth or USB, and enable smart phone functions through the navigation system. In some modern vehicles, an embedded Subscriber Identity Module (eSIM) card is installed in the telematics module of the vehicle when it is constructed, and this eSIM enables Internet access in order to display contents such as the current weather at the current location and the road directions to the destination on the navigation monitor. Furthermore, the driver can enable remote control functions such as door locking/unlocking and automated parking using the driver's smartphone. In addition, a communications module for V2V or V2I communications will be installed in vehicles.

Based on this, Fig. 1 shows a schematic related to connected vehicles. In the figure, we classify the environment surrounding connected vehicles into three general categories from the above facts. The first category is the in-vehicle category and it contains in-vehicle protocols such as the CAN [24], Local Interconnect Network (LIN) [25], and FlexRay [26]. From 2013, in-vehicle Ethernet has been installed in vehicles for communications related to the navigation systems [27], [28] and will be employed as the backbone of in-vehicle networks. In-vehicle systems such as the immobilizer and keyless entry systems are also in this category.

The second category is the communications network between the back-end system and the vehicles. In this category, the vehicle functions that have an interface to an outside network such as navigation systems and telematics modules are included. Although these systems are physically inside the vehicle, they have functions to connect to

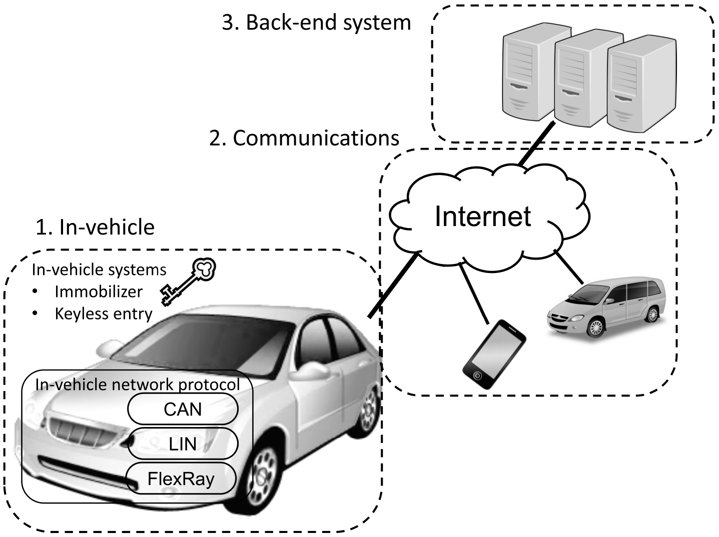


Fig. 1 Environment surrounding connected vehicles is classified into three categories.

an outside server. Therefore, we classify them into the communications category. In this category, remote control applications using smartphones and vehicle-to-everything (V2X) communications are also included. V2X communications have specific types such as V2V communications in which data are exchanged between vehicles and V2I communications that take place between the vehicle and infrastructure such as traffic lights.

The third category is the back-end system, that is, the server cluster which the service providers use. Apart from remote control services, examples of connected services are dynamic map delivery services for automated driving [29], vehicle remote maintenance, or the software update services that provide patches [30], and additional services corresponding to vehicle information such as vehicle insurance and recommended directions [31]. To provide these services, the back-end system plays an important role.

From here, we introduce the possible cyber-attack threats based on these three categories, especially focusing on the in-vehicle and communications categories that are more related to the cyber security of connected cars. We show that the cyber-attacks induce significant accidents when there is a lack of security in one of three categories, and introduce the need for protection technology.

3. In-Vehicle Category

This section describes the recent cyber-attacks and protection methods in the in-vehicle category. Here, we select and introduce the recent studies regarding the in-vehicle protocol, sensors and the in-vehicle devices and systems for physical car access because these are also the most significant for connected vehicles.

3.1 Studies Related to In-Vehicle Protocol

Here, we describe the investigations on the attacks after compromising the in-vehicle system through the navigation systems or the telematics modules that have an interface connected to an outside network. These studies are very significant because we should know how abnormal control of the vehicles is implemented after compromising the in-vehicle network.

In the past, denial of service (DoS) attacks and spoofing attacks were proposed against some in-vehicle protocols such as the CAN [14], [15], [32], [33]; LIN [34], [35]; and FlexRay [36], [37]. Here, we focus on attacks against the CAN and LIN protocols because they have become an active area of research and many papers were published. There are few previous investigations regarding the FlexRay protocol.

3.1.1 Studies Related to CAN

Regarding the attacks against the CAN protocol, many previous reports showed that abnormal behavior could be induced by injecting false CAN messages into a real vehicle. The CAN protocol is a multi-master protocol and employs the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) method [24]. The attack node can send a false command at any time. In spoofing attacks that do not modify the victim ECU, some injection methods were developed to inject a false command with high frequency compared to that for the original command [15] or to inject a false command immediately after the original command [38].

Although there are many attack methods regarding the CAN, we focused on reports regarding security evaluations using real vehicles or real devices related to vehicle services. The pioneering study in 2010 that shows the abnormal behaviors by injecting a CAN message is [14] and this study is referenced by many related papers. Some abnormal behaviors including the driving support controls were first shown in [15] and this study triggers successive vehicle attacks. The study that was the most influential in the automotive

Table 1 Studies related to CAN (Direct access to internal bus)

Kind of Attacks	Vehicle or Devices Used in Experiments	Year Published	Reference
Spoofing	No Mentioned in [14]	2010	[14]
	Ford Escape and Toyota Prius	2013	[15]
DoS	Honda Accord and Hyundai Sonata	2016	[32]
DoS or Spoofing	Bosch Drivelog Connector Dongle	2016	[33]

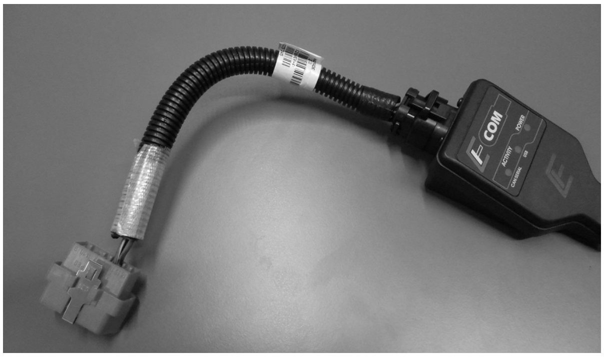
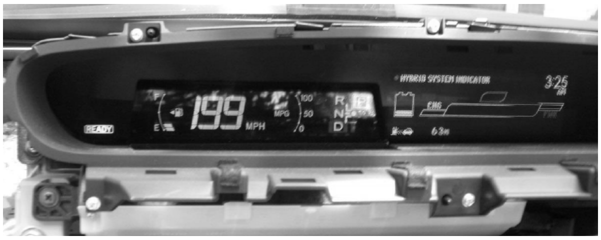


Fig. 2 Example of device for diagnostics in CAN communications. Depicted is a replacement that fits into the OBD-II port.



Taken from Fig. 17 in [15]

Fig. 3 Example of spoofing attacks to change the speedometer display. The speedometer display indicates 199 MPH while the vehicle is stopped.

world is [11] because it was the first to show abnormal behaviors remotely implemented without the connection of the devices to the vehicles. For better understanding, the brief history given in [39] on the attacks using real vehicles is helpful.

Table 1 gives the studies from 2010 regarding the attacks against the CAN protocol and these attacks are performed by directly connecting a commercial device through on-board diagnostics (OBD)-II [40] to access the CAN bus. Basically, such commercial devices are sold for maintenance and diagnosis of vehicles and to capture the driving log. These devices are also used to investigate the CAN traffic to develop related services [41]–[44]. As an example, Fig. 2 shows an ECOM device used for the diagnostics of CAN communications in the particular vehicles. The connector for the device is originally applied to another interface that is not the OBD-II port. It is replaced with the connector to fit the OBD-II port (the details are described in [15]). By injecting false messages in the CAN bus using the device, which is shown in Fig. 2, the speedometer display can be changed as shown in Fig. 3 as an example. (Fig. 17 in [15]).

In Table 2, we show the attacks that could remotely perform abnormal behaviors without direct access to the bus, i.e., no device is inserted into the OBD-II connector or the internal buses. In a connected vehicle that is equipped with an IVI system and applications associated with the IVI system can be easily compromised if they are not protected against attacks.

We note that the remote attacks in 2017 in Table 2 employ previous well-known vulnerabilities in the IT field which is the PC and server fields, to access internal software. This fact indicates that previous vulnerabilities remain in the telematics module or navigation systems installed in the vehicles [12], [13]. As an example, researchers found a previous vulnerability in the iPhone in the telematics module used in the Nissan Leaf [13] (details are described in Sect. 4.2.). They found that they could inject an irregular command over a wireless connection using a stack overflow or buffer overflow to enable them to send an attack command. We consider based on the recent vehicle security evaluations reported in 2017, that it is necessary to examine whether or not vulnerabilities, which are well known in the IT fields, remain in the vehicle systems.

3.1.2 Studies Related to LIN

Regarding the security evaluations of LIN, there are some previous papers [34], [35]. Here, we introduce the security evaluation of its protocol in [34] because this paper described the details of the attacks in the LIN.

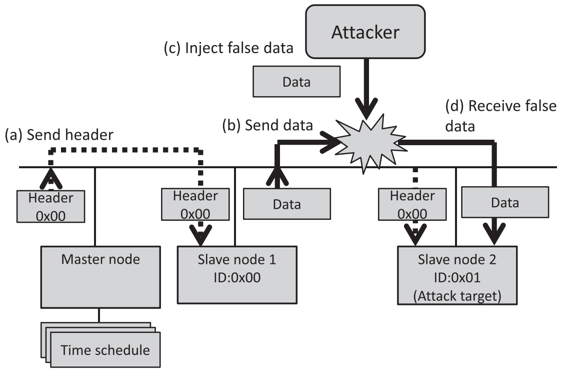
The LIN is usually used in body control of the vehicle such as seats and doors, and used in the steering [47]. Thus, there is the possibility for a significant threat especially while traveling at high speed. The LIN is based on a master-slave method that is different from the CAN. It also uses a time trigger method that employs a priori fixed time schedule, which is the key property of the LIN [25].

The master node transmits a header including the identifier (ID) that denotes the contents of the process, and the slave nodes corresponding to this ID start to transmit and receive data. Since the LIN specification does not define how to proceed after a transmission error has been detected, LIN error-handling mechanisms are application dependent. For example, when the data transmitted by a sender node differ from the data on the bus, the sender node detects an error. Then, it stops data transmission via the error handling mechanism and waits for the next header. Reference [34] focuses on the characteristics of this error handling mechanism and

Table 2 Studies related to CAN (Remote access)

Kind of Attacks	Vehicle Used in Experiments	Year Published	Reference
Spoofing	No Mentioned in [45]	2011	[45]
	Jeep Cherokee	2015	[11]
	Tesla Model S and Model X	2017	[12]
DoS or Spoofing	Tesla Model S	2015	[46]
	Nissan Leaf*	2017	[13]

* They did not actually inject false commands into the vehicles.



Taken from Fig. 3 in [34]

Fig. 4 Attack techniques that induce abnormal behaviors.

the false data are recognized as correct by the slave node (receiver). As a result, the attacker can induce abnormal behavior based on the LIN transmissions.

An example of the attack mechanism is given hereafter. Figure 4 shows the attack techniques that induce the abnormal behavior. First, the attacker monitors the bus to see if the target data are transmitted. The master node sends the header corresponding to the attack target data (Fig. 4 (a)). At the same time that the correct data corresponding to the header are sent by the slave node (Fig. 4 (b)), the attacker injects false data to induce a collision as indicated by Fig. 4 (c). Then, the transmission of the correct data stops because the error-handling mechanism is induced. Since the sender slave node stops transmitting the correct data, the attacker injects false data. This results in false data being recognized as the correct data by the slave node (receiver) (Fig. 4 (d)). As a result, the attacker can induce abnormal behavior without the driver intent.

Since the LIN will continue to be used as the in-vehicle protocol as well as the CAN and CAN with Flexible Data-Rate in the future, we consider that the security evaluation of the LIN using a real vehicle is also important.

3.2 Protection Technology for the Attacks Against In-Vehicle Protocols

This section introduces recent protection technology against the attacks for the in-vehicle protocols because many kinds of technologies have emerged from about 2013.

Since a multi-layer defense is the general security concept in the IT fields, this concept was applied to the in-vehicle systems around 2016 [48], [49]. Figure 5 shows a layer classification based on the vehicle structure. The first defense layer is a secure interface to protect a communications module or interfaces to outside networks, for example, the authentication between the communications module and an outside server. The second layer is a secure gateway between the in-vehicle bus and the interface or communications module. The third layer is a secure network to protect the communications in the in-vehicle network. The fourth layer is secure processing of the ECUs. It includes the secure update of the ECUs over the air (OTA) and secure boot.

Here, we focus on and describe the second and third layers that are related to the in-vehicle protocols and that are particular in the vehicles. Especially, we introduce the protection methods that are beginning to be installed in vehicles.

3.2.1 Installing a Gateway

This section describes the second layer protection.

Installing a gateway in a vehicle is not a brand new technology. However, the function of recent gateways in 2018 is more complex because of the increase in the number of ECUs [50]. The gateway also provides many functions such as linking data and signals from various nodes around the vehicle, converting many automotive communication protocols, and assuming a role as an interface for bus communications.

It also plays a role as a firewall, i.e., it makes it more difficult for attacks to capture and inject false data through the OBD-II port. However, attacks are still possible by accessing the internal bus behind the gateway through direct access to the bus as reported previously in [11]. So implementing a gateway itself is not a sufficient protection method although it is an effective deterrent from the aspect of easily accessing the in-vehicle buses.

In the future, the in-vehicle architecture will shift to set a domain controller between the gateway and each ECU connected to the powertrain, body, or IVI bus [50]. Based on [50], the role of the domain controller such as powertrain, body, and IVI domain is to control the ECUs connected to each bus and to manage the transmissions of the data. Furthermore, the gateway manages all domain controllers through Ethernet. The OBD-II port does not directly connect to the in-vehicle buses and there will be some con-

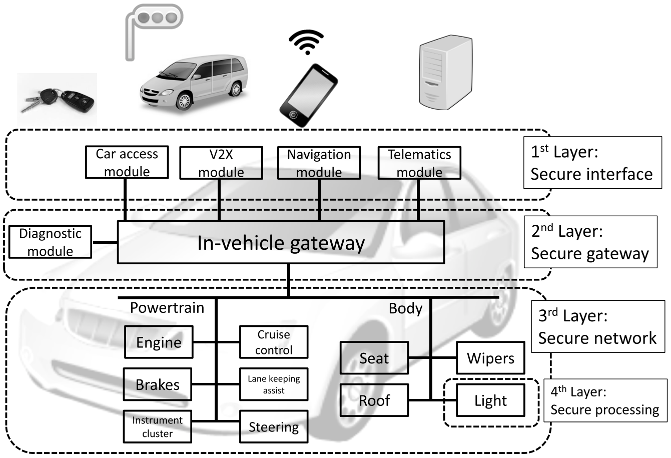


Fig. 5 Multi-layer defense based on the structure of recently produced vehicles.

trollers and gateways between the OBD-II port and buses. Furthermore, each domain such as the powertrain and the IVI system will be separate and the gateway would connect to each domain. It will be more difficult to access the internal bus and the attacker needs to guess and obtain accurate information regarding the relationships between the domain controllers and each target ECU.

3.2.2 Prevention Methods on Unauthorized Messages

This section describes the third layer protection to prevent the unauthorized message transmission such as MACs and the error frame transmission because they are more general methods.

(1) MAC

In 2017, the AUTomotive Open System ARchitecture (AUTOSAR) [51] published the specifications for Secure Onboard Communications (SecOC) 4.3.1 [52]. In the specification, the authentication method based on symmetric cryptography is considered. By installing a MAC, the attacker cannot easily generate a message that is accepted by the receiver node because the attacker must obtain the secret key for authentication in general. Thus, this technology is effective in mitigating the attack; however, there are other problems related to communication cost and secret key storage.

In 2017, the possibility for a practical attack on a MAC implementation was proposed [53]. They implied that the MAC is not effective based on its implementation. For example, some messages change very rarely and the length of the counter is short; therefore, the attacker can reply to the message because the MAC is calculated based on the data and counter, and can be guessed by the attacker. In this case, to prevent the replay attack, the MAC must be calculated from the time stamp of the message transmissions in addition to the data and counter.

Furthermore, in order to implement successful spoofing attacks continuously, a false message must be injected equal to or more often than the correct one. In this case, it is difficult to perform spoofing attacks when the MAC is implemented. Of course, if the attack is successful by injecting a message only a few times, the MAC will be not effective based on its implementation.

(2) Transmission of Error Frame

Another protection method to prevent unauthorized CAN messages was theoretically proposed in [54]. The method intends to prevent the spoofing attacks and replay attacks in which unauthorized messages induce abnormal behaviors.

The basic idea of the method is that when the node detects unauthorized messages that it did not send itself and which have the same ID, the node immediately transmits an error frame to override the unauthorized messages before it is received by the receiver node. If the genuine sender node can send the error frame immediately after the unauthorized messages by monitoring the bus data, the method is effective. To do so, the method must be implemented in the physical layer of the node to achieve a real-time response.

In the subsequent papers [55], [56], the error frame defined in the CAN is used for preventing unauthorized CAN messages, which include the incorrect MAC [55] and which do not match the correct CAN transmission rules [56].

3.2.3 Implementing Anomaly Detection in In-Vehicle Networks

Anomaly detection in the in-vehicle network is related to the third layer. Here, we also describe related techniques.

Anomaly detection is well known in the IT field to detect anomalous packets on the Internet. From around 2015, techniques have been adopted and consideration given to detecting anomalous messages in the CAN [57]–[59]. The basic approach is to investigate frequencies, sequences, and types of messages and to compare them to the messages in the case of normal operations. Thus, when abnormal message behavior is detected, the system will be stopped or only a limited form of the system will remain activated.

In addition to detecting anomalous behavior, methods to identify which malicious ECU sent a false message in the network have been proposed from 2014 [60]–[62]. Using these techniques, which ECU is compromised or which ECU is illegally installed in the network can be identified and the target ECU can immediately be isolated. These techniques need to identify each ECU based on the characteristics of the voltage profiles and they employ very sensitive information compared to general anomaly detection methods.

The technology to identify malicious hardware in the network follows the trend in detection methods in vehicle networks and there is a possibility that it will be installed in vehicles in the near future.

3.3 Studies Related to Sensors for Self-Driving

This section introduces recent interesting studies on attacks that confuse the sensors in vehicles used for driving assist functions and the self-driving by emitting false signals.

Multiple sensors such as Light Detection And Ranging (LiDAR), radar, and local cameras are equipped in recent automated vehicles commercialized around 2017 to handle local awareness of the vehicle surroundings. Because these sensors are important in terms of controlling the vehicle, sensors must be robust against attacks.

Since 2015, attacks on theses sensors have been presented [63]–[66]. In [66], physical layer cyber-security threats to autonomous vehicle systems are described. Previous research found that spoofing attacks on LiDAR were possible and induced a fake status by injecting an attacker light. This may cause the vehicle to sense non-existing objects when using the autonomous driving function. In the spoofing attacks, the sensor may become confused by false road signs or false distance signals from other vehicles, and this may result in changing the course of travel or an abnormal stop even when the distance from the real object is far from the vehicle.

Jamming attacks on the sensors were also presented in [63]–[65]. In these attacks, the attacker injects the same type of signal but at higher intensity to interfere with the real signal that is reflected from an obstacle. This may cause collision with other vehicles and yield false distances to an object. In fact, in [65], for automatic parking of the Tesla vehicle, the experimental results showed that the automated parking system did not correctly work and it collided with obstacles. Whether or not the attack is successful depends on the power of the jamming device, i.e., the distance between the jamming device and the vehicle.

Preventative measures against the spoofing and jamming attacks are to install sensor data authentication, encryption, and sender identification [66]. As specific countermeasures for the attacks on the sensors, redundancy of the different types of wavelengths for the LiDAR against the spoofing attacks and multiple measurement instances for the jamming attacks were presented [63].

3.4 Studies Related to Device or Systems for Physical Car Access

In this section, we focus on physical car access, i.e., more traditional vehicle security such as key systems. Here, we describe the security of the key systems, i.e., the vehicle immobilizer, and keyless entry and start system as examples because the related key system began to be realized using the smartphone (details are described in Sect. 4.3) and such systems may be susceptible to cyber attacks.

3.4.1 Vehicle Immobilizer

Here, we describe the security techniques related to the vehicle immobilizer that have proposed in 2010.

The vehicle immobilizer is a well-known anti-theft system and is widely used in vehicles. It actualizes electronic security to prevent the engine from running unless the corresponding transponder (often referred to as a key fob) is used. For several years, the transponders of the immobilizer system such as Hitag, Digital Signature Transponder, and Megamos were broken one by one because the size of their secret keys were very short [67]–[70].

Then, in 2010, an immobilizer system using the Advanced Encryption Standard (AES), which is the standard cryptographic algorithm, was proposed by a semiconductor manufacturer [71]. Reports regarding the security evaluation of [71] proposed theoretical analysis [72] and implementation attacks [73]. In the theoretical analysis [72], the authors described the possibility of attacks such as relay and replay attacks and then proposed countermeasures.

Even though the cryptographic algorithm used in the immobilizer is theoretically secure, its system could be broken by implementation attacks such as side-channel attacks [74] and invasive attacks [75]. Thus, the security against implementation attacks is an important aspect for the immobilizer. Although there are not so many papers on implementation attacks against the immobilizer, we consider that this aspect of the security is important especially in systems that use cryptography. Here, we briefly introduce the attack mechanism of the implementation attacks against the immobilizer [73].

Reference [73] focused on a fault attack, which is a kind of invasive attacks [75]. In the target immobilizer system [71], it has a characteristic that the key fob, which is the electronic key for the immobilizer, contains three copies of the original secret key used for the authentication between the key fob and the vehicle. These copies are used in sequence so that authentication does not fail in a harsh environment and to increase the system availability.

Using the characteristics of such a key storage method, the paper proposed an attack method that changes the value of the secret key stored in the key fob through sequential fault injections. Figure 6 shows the procedures for the attack in which the faults are injected into the key fob one by one. Using such fault injections, the secret key space is reduced

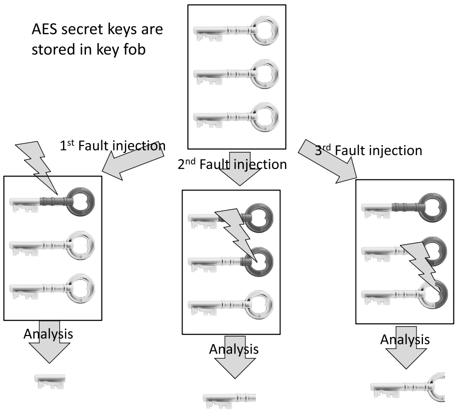


Fig. 6 Technique for evaluating immobilizer authentication protocols.

by the analysis based on the authentication protocol between the key fob and the vehicle. As a result, the attacker can recover some part of the AES key using the fault injections and analysis, and acquire the entire AES key with a brute-force search.

In [71], two kinds of authentication protocols, the unilateral authentication and the bilateral authentication protocols, were proposed. In the unilateral authentication protocol, where the vehicle authenticates the key, it is possible to identify the AES key in a practical amount of time. In the bilateral authentication protocol, where the vehicle and key authenticate each other, successful attacks to recover the secret key depend on factors such as the number of electronic key fobs and the output size of the encrypted data.

Reference [73] also proposed countermeasures to the attacks such as performing a preliminary comparison of the encryption results calculated using each secret key in order to verify whether or not any value in the key fob changed.

In connected vehicles, the immobilizer system will continue to be used, and the number of secure systems using cryptography will increase. Considering this, the practical security aspects of the cryptographic implementations must be considered as well as that for the theoretical aspect.

3.4.2 Passive Keyless Entry and Start System

Passive Keyless Entry (PKE) is an automotive security system that operates automatically to unlock or lock the door without human action on the electronic key. The user can often start the engine when the key is inside the vehicle. We note that these systems are available when the key is close to the vehicle or in the vehicle.

The easiest attack against PKE is a jamming attack to intercept communications between the key and the vehicle [76]. Jamming was easily achieved using a signal output from the attacker jamming device. Figure 7 shows the commercial jamming attack described in [76] (Fig. 1 in [76]). In fact, these kinds of devices can get from the cite of [77]. The experiments showed that keyless entry becomes ineffective when the attacker interferes with the correct signals between the key and the vehicle.

Taken from Fig. 1 in [76]

Fig. 7 A commercial jamming devices.

Another well-known attack against PKE is to perform relay attacks [78]. In the attack, the attacker places an antenna near the key holder and a second antenna close to the vehicle. The communications between the key and the vehicle are relayed and the attacker can finally open the door and start the engine even though the key is physically far from the vehicle. The distance that a signal can be relayed is up to 50 meters. The vulnerabilities of PKE to relay attacks are evident in 10 kinds of vehicle models.

Simple steps to prevent these attacks are to shield the key or to remove the battery from the key although it is somewhat inconvenient for the user [78]. Reference [78] also describes another prevention step in which the user disables temporally the PKE system.

These attacks do not break the cryptography used in the electronic key and the attacker does not need to tamper with the key itself. This is different from the attacks against the immobilizer systems described in Sect. 3.4.1. The protection against these kinds of attacks is also significant because the attacker can remotely perform abnormal actions to cause the doors to lock/unlock and there is a possibility to steal it.

4. Communications Category

This section describes the cyber security related to the communications category as shown in Fig. 1.

Connected vehicles have an Internet connection to achieve remote control of the vehicle, and remote diagnostics services to monitor the current status of the vehicle and to search for desired destinations.

Here, we introduce recent threats and requirements related to the communications between the vehicle and back-end system. First, we describe the security regarding the modules that play important roles in the interface to connect to an outside network. In particular, we focus on the security of the car navigation systems and telematics modules because they are the most attractive attack surface for the attackers. We describe the security regarding applications for remote services using a smartphone or a PC that have come into use in the past several years. We also discuss V2X security related to connected vehicles in this section.

4.1 Communications with Car Navigation Systems

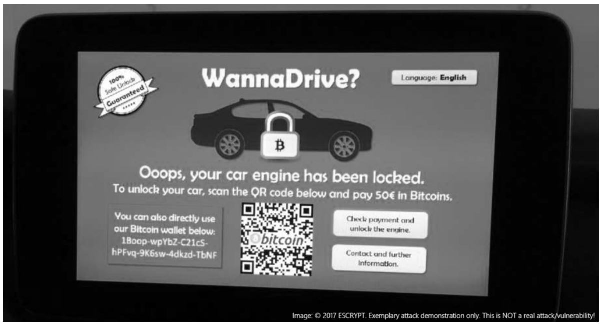
More and more car navigation systems (navigation head units) have functions that are connected through WiFi, Bluetooth, and the USB interface. The navigation system also has a firmware update function and navigation maps. Because the navigation systems have these interfaces connected to outside networks and the systems communicate with in-vehicle modules through the in-vehicle bus, the attacker can easily compromise the in-vehicle systems through the navigation systems. Hereafter, we describe the security for the navigation systems with the remote access and the malware risk in the navigation systems.

4.1.1 Compromising Navigation Systems for Remote Access

Some researchers have tried to compromise navigation systems in order to access remotely in-vehicle systems. The attack in [12] exploits the web browser of the navigation system by utilizing two well-known browser vulnerabilities to achieve arbitrary code execution. In successive processes, they used another Linux vulnerability and were able to perform arbitrary read and write processes to the kernel contents. After bypassing some embedded systems, they finally sent arbitrary CAN commands. This implies that the previous vulnerabilities still exist when the oldest version of the web browser or Linux is used even in recent Tesla models in 2016.

In [13], the researcher introduced a security evaluation of the car navigation system itself. They investigated the navigation system in order to extract the system files for debugging using diagnostic menus and found an unused URL during the debug. They installed a honey pot in the URL and observed the access log that included private information such as the user password and the vehicle identification number (VIN). This shows that the debugging code remains in the file systems of the navigation systems and normally it should be deleted before shipment so that it cannot be used for mischievous purposes.

Related to the in-vehicle platform used for navigation systems, we introduce a report in 2017 in which AGL vulnerabilities were investigated [79]. This study targeted AGL v3.0 and it evaluated attack interfaces such as Wi-Fi, Bluetooth, and USB. They found an exploit for the connection manager, which performs name resolution when the AGL device accesses an outside network, and showed that any command can be remotely injected. Such investigations are performed while the system is under development. These investigations imply that some countermeasures must be developed for AGL. This study may represent a good reference for investigating the vulnerability of the IVI system for connected vehicles.


100% Safe Unlock Guaranteed
WannaDrive?
Language: English
Check payment and unlock the engine.
Contact and further information.
bitcoin

Ooops, your car engine has been locked.
To unlock your car, scan the QR code below and pay 50€ in Bitcoins.

You can also directly use our Bitcoin wallet below: 1Boop-wpYbZ-C21cS-hPFvq-9K6sw-4dkzd-TbNF

Image: © 2017 ESCRYPT. Exemplary attack demonstration only. This is NOT a real attack/vulnerability!

Taken from Fig. 17 in [80]

Fig. 8 A demonstration of the WannaDrive if the navigation system is compromised from the malware. We note that this is not a real attack and vulnerability.

4.1.2 Malware Risk in Navigation Systems

Malware is a well-known computer virus in the IT fields such as PCs and smartphones. In 2017, ransomware called WannaCry, was unleashed on the world. Ransomware is a type of malicious software that locks up the victim data on a PC so that it cannot be accessed unless a ransom is paid.

In 2017, an interesting study concerning the possibility of malware in vehicles was published [80]. Reference [80] introduced the possibility of ransomware threats to the navigation system called WannaDrive. Figure 8 shows the display of the navigation system in a simulation where the vehicle was compromised by WannaDrive. Because of the ransomware the vehicle would not work unless the ransom was paid. The figure is taken from [80]. We note that this is not a real attack and vulnerability.

Because the navigation system connects to outside networks and has a function to update firmware using Wi-Fi or USB as mentioned earlier, the threat level from malware will increase. If an attacker implements an attack where malware is inserted in the vehicle systems, there is a risk that the vehicle may, for example, run at high speed until the ransom is paid [80]. This is a more dangerous situation compared to what may happen in the PC field. In the near future, antivirus software may be needed for navigation systems just as it is already for PCs.

4.2 Communications with Telematics Modules

The telematics module is another attack surface to compromise the in-vehicle system because it incorporates an electronic chip for communications with outside servers. In luxury vehicles, a hotspot can be generated to allow passengers easy access to the Internet for their smart devices through combination with the telematics module.

In fact in 2015, the German researchers analyzed the telematics module (referred to as combox) and found a vulnerability that enabled attackers to perform replay attacks in [81]. They reverse engineered the firmware to find the cryptographic algorithms and keys used in the module. As a result, they were able to perform replay attacks to send text messages and remotely open the door using an emulated cellular network without the driver knowledge. According to the report, there were some issues with the remote services in that the telematics module used the same encryption keys in all vehicles and the communications between the vehicles and back-end system were not encrypted, i.e., they used the Hypertext Transfer Protocol. They also mentioned that these problems were patched before the report was published.

In another example in 2017, the security researchers found that the telematics control module (referred to as Telematics Control Unit (TCU)) included security problems [13]. The units had a 2G modem and a chipset installed in which the communications could easily be analyzed and the vulnerabilities were well known. Using the well-known vulnerabilities in remote code execution, they concluded that any false command could be injected into the CAN bus through the TCU if it connects to a 2G network.

Since the telematics module represents an important interface to the in-vehicle system from an outside network, countermeasures have been taken to install gateways between the telematics module and the in-vehicle networks as described in Sect. 3.2.1.

Furthermore, once a vehicle has been marketed, it will be used for a long time. Therefore, the potential exists that an old module that has an IT vulnerability would remain in a vehicle. Steps should be taken to check whether or not installed modules are secure and a framework for updating the modules should be established such as OTA, to provide patches immediately when a vulnerability is found.

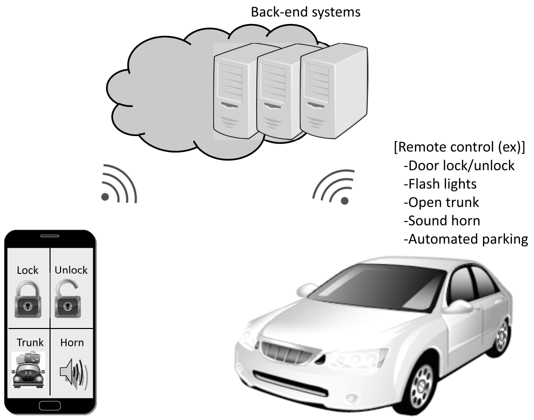


Fig. 9 Image of remote control services.

4.3 Application of Remote Control Services

In around 2017, remote control services such as confirming the vehicle status, door locking/unlocking, and auto parking function were implemented in many kinds of vehicles [2], [82]–[85]. An image of remote services is shown in Fig. 9. Most remote control applications for locking/unlocking the vehicle, flashing the headlights, and locating the vehicle can be accessed using a web service and some of these services have a function to start the engine. Mobile applications communicate with back-end systems through the Internet. As a result, the user can remotely communicate with the vehicle using such a service to monitor the vehicle status or to perform specific vehicle controls.

There is also a strong threat to mobile applications and systems because they can be used to access easily the in-vehicle systems. In the past, security evaluations of remote control services were performed and they highlighted vulnerabilities of the applications. Table 3 gives published security evaluations related to remote control services.

These vulnerabilities were triggered because the implementation of the application code had a security flaw. As a result, a specific remote control function such as opening a door could be performed without the electronic keys or any special device.

As an example, in [86], inadequate usage of the Secure Sockets Layer (SSL) certification of the application induced a man-in-the-middle attack. In fact, an adequate SSL certification check was not implemented in the smartphone application. Then, if the attacker certification is installed in the victim smartphone, the attacker could sniff the communications between the smartphone and the back-end server even when SSL is employed. The authors reported that the same attack method was applicable to the remote systems of BMW, Mercedes-Benz, and Chrysler.

In [88], a vulnerability in a smartphone application was revealed. If the attacker knows the last five digits of the VIN, the attacker can guess possible numbers and try a candidate search until the vehicle is found. As a result, the attacker could turn on the air conditioning even when the target vehicle is on the opposite side of the earth. The application only needs the VIN to identify the vehicle for remote control. So, the attacker can perform the same functions that can be done using the application if the attacker can guess the VIN of the target vehicle. Furthermore, in the report, the

Table 3 Security evaluation of remote control applications

Services Using Evaluations	Year Published	Reference
GM's OnStar (*)	2015	[86]
BMW Connected Drive	2016	[87]
NissanConnect EV	2016	[88]
Mitsubishi Remote Control	2016	[89]
Hyundai Blue Link Application	2017	[90]

attacker was able to obtain the information of the user name, and the times and distances of recent journeys. This shows that vulnerabilities in the application may reveal the private user information as well as enable unwanted control of the vehicles.

Since the above evaluations are mainly related to body control of the vehicle at this point, the safety risk to the driver and passengers is deemed low because they would most likely not be directly exposed to an accident. However, if the control such as unlocking the door is under threat by the attacker, the attacker can break into the car. When the remote control to start the engine is also installed, the attacker could steal the vehicle.

Remote control using a smartphone has begun to spread to critical control of driving. As an example, some expensive types of vehicles have installed remote parking control using the smartphone to park the car automatically in an unoccupied space without driver control. In the near future, more kinds of remote control related to driving will appear and eventually automated driving will be achieved using portable devices. This implies that increased security measures should be considered in mobile or web applications that trigger critical vehicle control. As an example, the best practices of mobile application security for the application developer are published and these reports describe the basic security considerations when developing an application [91]. This type of document is useful when considering the structure of a secure application. Of course, the developers need to examine the details of the code implementation to avoid security risks based on the items in [91] because this document does not describe details on how to implement the application code securely.

4.4 V2X Security

Some car manufacturers have begun to provide vehicles with V2X communications, including V2V and V2I communications [92], [93]. These systems are expected to be used for predicting dangerous situations to alert the driver and automatically preventing an accident through message from other vehicles or roadside units. Sending and receiving of message communications are mainly achieved through dedicated short-range communications.

From the security aspect regarding V2X, a message mutually transmitted between vehicles (or vehicle and infrastructure) must be trustworthy because there are cases in which the vehicle is only controlled by these messages. In the Car 2 Car Communication Consortium [94], the security level of V2X communications and protection methods was discussed for a long time. The Trusted Assurance Level and the security requirements at each level were defined [95]. Level 2 is the minimum level and this level is equal to Evaluation Assurance Level 4 in the Common Criteria used in IT products and information systems. As an example of the protection methods for V2X, the use of public-key cryptography based infrastructure such as the Public Key Infrastructure (PKI) is considered to ensure the trustworthiness of the message because of the ad-hoc communications in the case of V2X communications [96].

In addition, the messages transmitted between vehicles must be anonymous because these include private information such as the driver location and vehicle status. Each vehicle can regularly change its identifier every communication instance to make it harder for an attacker to identify or follow a specific vehicle [97]. In [97], some challenges were reported that remain on the vehicle side to achieve anonymity based on PKI. For example, because many messages are transmitted in a crowded traffic situation, the vehicle can receive hundreds of messages per second and must verify the messages as soon as they are received. The module must verify the signature at high speed. If such a module is not installed, it may be difficult to achieve autonomous control using the V2X systems especially in a situation that requires rapid action to control the vehicle.

5. Back-End System Category

This section describes the cyber security related to the back-end system. At this time, to the best of our knowledge, there have not yet been any published investigation on the security threats to back-end system that are inherent to connected vehicles. The importance of the security problems related to the back-end system for connected vehicles are equal to that in the network services in the IT field because the system is almost the same as those in the IT field. In this section, we briefly describe possible security threats for the back-end system in the automotive field.

5.1 DoS Attacks

In the field of the back-end systems such as back-end servers, DoS attacks are serious and well-known attacks [98]. If back-end servers for connected vehicles are targeted by DoS attacks, the vehicle itself would not work correctly and the attacks may affect the traffic network infrastructure when a real-time map is served to the vehicle from the back-end servers. A DoS mitigation system must be installed against such traditional attacks in the back-end servers.

5.2 Cross Virtual Machine (VM) Side-Channel Analysis

As a kind of server cluster implementation configuration used by service providers, there is a case that a cloud computing system is used. The cloud computing systems have begun to be applied to back-end systems in the automotive field. In this case, the user shares physical memory with another virtual machine user, and therefore, security problems must be considered.

The cross VM side-channel attack is one of the security risks for the cloud computing systems [99]–[101]. In co-existing environments using a VM, there is a risk that secret information can be extracted by such attacks. Figure 10 shows an image of the cross VM side-channel anal-

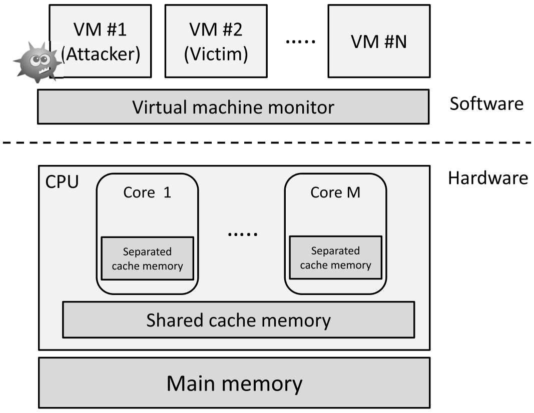


Fig. 10 Image of cross VM side-channel analysis.

ysis. In this situation, the attacker can guess the secret information such as the encrypted key or the user secret data used in the victim environment by monitoring the behavior of shared cache memory and main memory and then performing cache-timing attacks. In the back-end systems of the service providers, critical data related to each user are uploaded and a situation may occur in which some users share the same cloud computing resources even when the applications or the system are separate. Then, we consider that the secure implementation must be performed to mitigate the attacks when the cryptographic algorithm is used in the cloud computing environments [102].

6. Other Significant Contents for Connected Vehicle Security

In this section, we introduce significant contents related to vehicle security such as the concept of functional safety and recent specifications or guidelines released around 2015 for automotive security.

(1) Functional Safety

In the automobile field, functional safety, which is defined in part 1 of ISO 26262 [103], is also significant. This safety measure sometimes mitigate the cyber attacks, so, we briefly mention it here. In functional safety, even when a system failure occurs in a vehicle, the vehicle shifts to and maintains a safe status. The vehicle also operates when the functionality is reduced or limited when a system failure occurs. Such functional safety is installed in vehicles and some kinds of attacks can be thwarted by functional safety [11]. However, functional safety is not sufficient for all kinds of attacks and we must implement other means of security protection. Thus, we must consider a balance of security and safety to develop and install protection methods against cyber attacks.

(2) Guidelines for Automotive Security

Because more and more specifications of guidelines for automotive security have been published over several years, we briefly mention them for reference in designing the automotive systems.

In 2015, Robert Bosch proposed Bosch SEP: Security engineering process for automotive embedded systems [104]. Bosch SEP includes three phases that are needed for the development of vehicle systems. This also describes a security testing scheme such as fuzz testing and invasive testing. In 2016, SAE published SAE J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems and provided the design techniques to mitigate cyber attacks against vehicle systems in the development of its systems [105]. In 2017, car manufactures also presented requirements for the embedded systems [106]. They insisted that the implementation phase of the embedded systems is the most significant for considering security. Thus, automotive security guidelines were specified and published to create a unified method to implement and develop embedded systems.

7. Conclusions

This paper presented our perspective on cyber security for connected vehicles based on a survey of recent studies related to vehicle security. We classified the environments surrounding connected vehicles into three categories and introduced a wide range of security risks and protection requirements in each category. In the in-vehicle category, we presented recent studies on security regarding the in-vehicle protocols based on actual vehicle attacks and the major protection methods based on multi-layer environments surrounding connected vehicles. We also described the security of physical car accessing devices or systems, that are used in the immobilizer and keyless entry systems. In the communications category, we introduced threats and requirements regarding interface systems to outside networks such as the car navigation system and telematics modules. Furthermore, we showed that secure applications for remote control services must be considered because vulnerabilities were previously found and attackers were able to perform some abnormal remote control. Finally, we briefly introduced aspects of V2X security. In the back-end system category, to the best of our knowledge, actual attacks on back-end system have not yet been reported. In light of this, we introduced potential upcoming threats to the servers in the automotive field that are well known in the IT field. For example, we described traditional DoS attacks and cross VM side-channel analysis, and indicated possible protection methods. We emphasized that overall security covering the three categories must be considered because serious accidents can be induced even if one security item in the three categories is not covered as described in each section. We also described the significant contents for the connected-vehicle security such as the functional safety which is originally installed in the vehicles and the specifications or guidelines for vehicle security.

In conclusion, we believe that this paper will contribute to better understanding through this overview of connected vehicle security and help readers when they develop and provide services, communications, and devices including autonomous driving.

References

[1] Fuji Keizai, Marketing reports, "Investigations of the Connected Vehicle Marketing," published in Japanese, https://www.fuji-keizai.co.jp/market/17022.html, accessed Feb. 20, 2018.

[2] BMW, "BMW Connected Drive," 2017, https://www.bmw.com/en/topics/fascination-bmw/connected-drive/overview.html, accessed Feb. 20, 2018.

[3] Audi, "Audi Technology Portal, Audi A8 - Audi AI parking pilot and garage pilot," https://www.audi-technology-portal.de/en/electrics-electronics/driver-assistant-systems/audi-a8-audi-ai-parking-pilot-and-garage-pilot, accessed Feb. 20, 2018.

[4] Tesla, "Summon Your Tesla from Your Phone," https://www.tesla.com/blog/summon-your-tesla-your-phone, accessed Feb. 20, 2018.

[5] Nissan Motor Corporation, "Technology, ProPILOT Park," http://www.nissan-global.com/EN/TECHNOLOGY/OVERVIEW/propilot_park.html, accessed Feb. 20, 2018.

[6] R. Bauza, J. Gozalvez, and J.S.-Soriano, "Road traffic congestion detection through cooperative Vehicle-to-Vehicle communications," Proc. 4th IEEE Workshop On User MObility and VEhicular Networks (On-MOVE), IEEE-CS, pp.606–612, 2010.

[7] Waymo, "On The Road To Fully Self-Driving, Waymo Safety Report," https://waymo.com/safetyreport/, accessed Feb. 20, 2018.

[8] Android Auto, "Get music and messages while driving," https://developer.android.com/auto/index.html, accessed Feb. 20, 2018.

[9] Apple, "CarPlay," https://www.apple.com/jp/ios/carplay/, in Japanese, accessed Feb. 20, 2018.

[10] "Automotive Grade Linux," https://www.automotivelinux.org/, accessed Feb. 20, 2018.

[11] C. Miller and C. Valasek, "Remote Exploitation of an Unaltered Passenger Vehicle," Proc. DEFCON Hacking Conference 23, 2015, http://illmatics.com/Remote%20Car%20Hacking.pdf, accessed Feb. 20, 2018.

[12] S. Nie, L. Liu, and Y. Du, "FREE-FALL: Hacking Tesla From Wireless to CAN Bus," Proc. Black Hat USA, 2017, https://www.blackhat.com/docs/us-17/thursday/us-17-Nie-Free-Fall-Hacking-Tesla-From-Wireless-To-CAN-Bus-wp.pdf, accessed Feb. 20, 2018.

[13] J. Michael, M. Shkatoy, and O. Bazhaniuk, "Driving Down the Rabbit Hole," Proc. DEFCON Hacking Conference 25, 2017.

[14] 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," Proc. IEEE Symposium on Security and Privacy (SP), IEEE-CS, pp.447–462, 2010.

[15] C. Valasek and C. Miller, "Adventures in Automotive Networks and Control Units," Proc. DEFCON Hacking Conference 21, 2013, https://ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf, accessed Feb. 20, 2018.

[16] C. Miller and C. Valasek, "CAN Message Injection," OG Dynamite Edition, 2016, http://illmatics.com/canmessageinjection.pdf, accessed Feb. 20, 2018.

[17] F. Stumpf, C. Meves, B. Weyl, and M. Wolf, "A Security Architecture for Multipurpose ECUs in Vehicles," 2009 https://www.evita-project.org/Publications/SMWW09.pdf, accessed April 9, 2018.

[18] B. Groza, S. Murvay, A.V. Herrewege, and I. Verbauwhede, "LiBrA-CAN: a Lightweight Broadcast Authentication protocol for Controller Area Networks," ACM Transactions on Embedded Computing Systems (TECS) - Special Issue on Embedded Computing for IoT, Special Issue on Big Data, vol.16, Issue 3, Article No.90, pp.1–28, 2017.

[19] D.K. Nilsson, U.E. Larson, and E. Jonsson, "Efficient In-Vehicle Delayed Data Authentication Based on Compound Message Authentication Codes," Proc. IEEE 68th Vehicle Technology Conference (VTC), IEEE-CS, pp.1–5, 2008.

[20] C. Szilagyi and P. Koopman, "Low Cost Multicast Authentication via Validity Voting in Time-Triggered Embedded Control Networks," Proc. 5th Workshop on Embedded Systems Security (WESS), ACM, 2010, https://dl.acm.org/citation.cfm?id=1873558, accessed Feb. 20, 2018.

[21] L.A. Maglaras, "A Novel Distributed Intrusion Detection System for Vehicular Ad Hoc Networks," Proc. International Journal of Advanced Computer Science and Applications, vol.6, no.4, pp.101–106, 2015.

[22] J. Li, "CANsee - An Automobile Intrusion Detection System," Presentation slides on Hack In The Box Security Conference (HITBSecConf), 2016. https://conference.hitb.org/hitbsecconf2016ams/sessions/cansee-an-automobile-intrusion-detection-system/, accessed Feb. 20, 2018.

[23] H.M. Song, H.R. Kim, and H.K. Kim, "Intrusion Detection System Based on the Analysis of Time Intervals of CAN Messages for In-Vehicle Network," Proc. International Conference on Information Networking (ICOIN), IEEE-CS, pp.63–68, 2016.

[24] ISO 11898-1:2015 Road vehicles – Controller area network (CAN) – Part 1: Data link layer and physical signalling.

[25] LIN Specification Package Revision 2.2A, pp.1–194, Dec. 2010.

[26] FlexRay Communications System Protocol Specification Version 3.0.1, pp.1–341, Oct. 2010.

[27] P. Hank, S. Muller, O. Vermesan, and J.V.D. Keybus, "Automotive Ethernet In-vehicle networking and smart mobility," Proc. Design, Automation & Test in Europe Conference & Exhibition (DATE), IEEE-CS, pp.1–5, 2013.

[28] IXIA, "Automotive Ethernet: An Overview, WHITE PAPER 915-3510-01 Rev.A," 2014, https://support.ixiacom.com/sites/default/files/resources/whitepaper/ixia-automotive-ethernet-primer-whitepaper_1.pdf, accessed Feb. 20, 2018.

[29] Dynamic map planning Co. Ltd., "Dynamic Map Planning (DMP)," 2016, http://www.aisantec.co.jp/ir/library/aboutDMP2016.pdf, accessed Feb. 20, 2018.

[30] G. de Boer, P. Engel, and W. Praefcke, "Generic Remote Software Update for Vehicle ECUs Using a Telematics Device as a Gateway," Proc. Advanced Microsystems for Automotive Applications, Springer, pp.371–380, 2005.

[31] J. Peng, N. Liu, H. Zhao, and M. Yu, "Usage-Based Insurance System Based on Carrier-Cloud-Client," Proc. 10th International Conference on Communications and Networking in China (ChinaCom), IEEE-CS, pp.1–6, 2015.

[32] K.-T. Cho and K.G. Shin, "Error Handling of In-vehicle Networks Makes Them Vulnerable," Proc. ACM SIGSAC Conference on Computer and Communications Security (CCS 16), pp.1044–1055, 2016.

[33] Argus Cyber Security, "A Remote Attack on the Bosch Drivelog Connector Dongle," https://argus-sec.com/remote-attack-bosch-drivelog-connector-dongle/, accessed Feb. 20, 2018.

[34] J. Takahashi, Y. Aragane, T. Miyazawa, H. Fuji, H. Yamashita, K. Hayakawa, S. Ukai, and H. Hayakawa, "Automotive Attacks and Countermeasures on LIN-Bus," Journal of Information Processing, vol.25, pp.220–228, 2017.

[35] M. Wolf, A. Weimerskirch, and C. Paar, "Secure In-Vehicle Communication," Part II in Book of Embedded Security in Cars, K. Lemke, C. Paar, and M. Wolf (eds.), Springer-Verlag Berlin Heidelberg, pp.95–109, 2006, ISBN-10 3-540-28384-6 (Print)

[36] D.K. Nilsson, U.E. Larson, F. Picasso, and E. Jonsson, "A First Simulation of Attacks in the Automotive Network Communications Protocol FlexRay," Proc. International Workshop on Computational Intelligence in Security for Information Systems (CISIS), ASC 53, pp.84–91, 2009.

[37] M. Wolf, A. Weimerskirch, and C. Paar, "Security in automotive bus systems," Proc. Workshop on Embedded Security in Cars (escar) Europe, 2004.

[38] K.-T. Cho and K.G. Shin, "Fingerprinting Electronic Control Units for Vehicle Intrusion Detection," Proc. 25th USENIX Security

Symposium, pp.1–18, 2016, https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_cho.pdf, accessed April 9, 2018.

[39] G+D Mobile Security, "A Brief History of Car Hacking 2010 to the Present," https://smart.gi-de.com/2017/08/brief-history-car-hacking-2010-present/, accessed Feb. 20, 2018.

[40] SAE J1962: Diagnosis Connector Equivalent to ISO-DIS 15031: Dec. 2001.

[41] CAN capture, "Standard ECOM Device - Controller Area Network (CAN) to USB hardware interface," https://www.cancapture.com/ecom, accessed Feb. 20, 2018.

[42] Vector Informatik, "CANoe," https://vector.com/vi_versionhistory_detail_en,,,1653990,detail.html, accessed Feb. 20, 2018.

[43] ZMP, "Automotive CAN data cloud system construction service," http://www.zmp.co.jp/products/obd2?lang=en, accessed Feb. 20, 2018.

[44] E. Evenchick, "CANtact -The Open Source Car Tool-," http://linklayer.github.io/cantact/, accessed Feb. 20, 2018.

[45] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," Proc. 20th USENIX Security Symposium, pp.1–6, 2011.

[46] M. Rogers and K. Mahaffey, "How To Hack a Tesla Model S," Proc. DEFCON Hacking Conference 23, 2015.

[47] J. Stelzer, "LIN Bus - An Emerging Standard for Body Control Applications," https://www.google.co.jp/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjjrpOQhqzaAhVIyLwKHWc2CasQFggnMAA&url=https%3A%2F%2Farchive.eetasia.com%2Fwww.eetasia.com%2FARTICLES%2F2004SEP%2FB%2F2004SEP16_NTEK_ID_TA.pdf%3FSOURCES%3DDOWNLOAD&usg=AOvVaw0_fJhVx--35qkxjFHv5m55, accessed April 9, 2018.

[48] A. Birnie and T. v. Roermund, "A Multilayer Vehicle Security Framework," white paper, Date of release: May 2016.

[49] C. Ebert and E. Metzker, "Cyber Security for the Automotive Industry Practical experiences on the application of Cyber Security," Vector Technical Article, Sept. 2016, https://vector.com/portal/medien/cmc/press/Vector/Security_Cyber_ElektronikAutomotive_201609_PressArticle_EN.pdf, accessed Feb. 20, 2018.

[50] L.D. Ambroggi, "Ethernet In car: from Multiplexed network to Service network," IHS Markit Technology, https://technology.ihs.com/590689/ethernet-in-car-from-multiplexed-network-to-service-network, accessed Feb. 20, 2018.

[51] AUTOSAR, "The standardized software framework for intelligent mobility," https://www.autosar.org/, accessed Feb. 20, 2018.

[52] AUTOSAR, "Specification of Secure Onboard Communication," Release 4.3.1, https://www.autosar.org/fileadmin/user_upload/standards/classic/4-3/AUTOSAR_SWS_SecureOnboardCommunication.pdf, accessed March 12, 2018.

[53] Y. Weisglass, "Practical Attacks on CAN Message Authentication," Proc. The 4th Embedded Security in Cars (escar) Asia, 2017.

[54] T. Matsumoto, M. Hata, M. Tanabe, K. Yoshioka, and K. Oishi, "A Method of Preventing Unauthorized Data Transmission in Controller Area Network," Proc. IEEE 75th Vehicular Technology Conference (VTC Spring), IEEE-CS, pp.1–5, 2012.

[55] R. Kurachi, Y. Matsubara, H. Takada, N. Adachi, Y. Miyashita, and S. Horihata, "CaCAN - Centralized Authentication System in CAN (Controller Area Network)," Proc. The 12th Embedded Security in Cars (escar) Europe, 2014.

[56] Y. Ujiie, T. Kishikawa, T. Haga, H. Matsushima, T. Wakabayashi, M. Tanabe, Y. Kitamura, and J. Anzai, "A Method for Disabling Malicious CAN Messages by Using a Centralized Monitoring and Interceptor ECU," Proc. The 13 th Embedded Security in Cars (escar) Europe, 2015.

[57] A. Taylor, N. Japkowicz, and S. Leblanc, "Frequency-Based Anomaly Detection for the Automotive CAN bus," Industrial Control Systems Security (WCICSS), IEEE-CS, pp.1–5, 2015.

[58] S. Nair, S. Mittal, and A. Joshi, "OBD SecureAlert: An Anomaly Detection System for Vehicles," Proc. IEEE International Conference on Smart Computing (SMARTCOMP), IEEE-CS, pp.1–6, 2016.

[59] S.N. Narayanan, S. Mittal, and A. Joshi, "Using Data Analytics to Detect Anomalous States in Vehicles," arXiv:1512.08048 [cs.AI], pp.1–10, 2015.

[60] W. Choi, H.J. Jo, S. Woo, J.Y. Chun, J. Park, and D.H. Lee, "Identifying ECUs Using Inimitable Characteristics of Signals in Controller Area Networks," rXiv:1607.00497 [cs.CR], pp.1–12, 2016.

[61] P.S. Murvay and B. Groza, "Source Identification Using Signal Characteristics in Controller Area Networks," Proc. IEEE SIGNAL PROCESSING LETTERS, IEEE Signal Process. Lett., vol.21, no.4, pp.395–399, 2014.

[62] K.-T. Cho and K.G. Shin, "Viden: Attacker Identification on In-Vehicle Networks," Proc. ACM conference on Computer and communications security (ACM CCS), ACM, pp.1109–1123, 2017.

[63] J. Petit, B. Stottelaar, M. Feiri, and F. Kargl, "Remote Attacks on Automated Vehicles Sensors: Experiments on Camera and LiDAR," Proc. Black Hat Europe, 2015, https://pdfs.semanticscholar.org/e06f/ef73f5bad0489bb033f490d41a046f61878a.pdf, accessed Feb. 20, 2018.

[64] H. Shin, D. Kim, Y. Kwon, and Y. Kim, "Illusion and Dazzle: Adversarial Optical Channel Exploits Against Lidars for Automotive Applications," Proc. Conference on Cryptographic Hardware and Embedded Systems (CHES) 2017, LNCS, pp.445–467, 2017.

[65] C. Yan, W. Xu, and J. Liu, "Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-Driving Vehicles," Proc. DEFCON Hacking Conference 24, 2016, https://pdfs.semanticscholar.org/6b3a/004de158c8c1af6d010ac64489d4929d2346.pdf?_ga=2.68342801.181363560.1537846941-580514357.1537846941, accessed Feb. 20, 2018.

[66] S. Glushko, "Jamming and Spoofing Attacks: Physical Layer Cybersecurity Threats to Autonomous Vehicle Systems," Before the National Highway Traffic Safety Administration Washington, DC, 2016.

[67] R. Verdult, F.D. Garcia, and J. Balasch, "Gone in 360 Seconds: Hijacking with Hitag2," Proc. 21st USENIX conference on Security symposium, pp.237–252, 2012.

[68] S.C. Bono, M. Green, A. Stubblefield, A. Juels, A.D. Rubin, and M. Szydlo, "Security analysis of a cryptographically-Enabled RFID device," Proc. 14th USENIX Security Symposium, pp.1–16, 2005.

[69] A. Francillon, B. Danev, and S. Čapkun, "Relay attacks on passive keyless entry and start systems in modern cars," Proc. 18th Network and Distributed System Security Symposium (NDSS), The Internet Society, pp.1–15, 2011.

[70] R. Verdult and F.D. Garcia, "Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer," Proc. 22nd USENIX Security Symposium, pp.703–718, 2015.

[71] Atmel, "The AES 125kHz Transponder with Open Immobilizer Software Stack," 2012, https://www.mouser.com/ds/2/36/doc9254-33290.pdf accessed April 9, 2018.

[72] S. Tillich and M. Wòjcik, "Security Analysis of an Open Car Immobilizer Protocol Stack," Proc. 10th Embedded Security in Cars Conference (escar) Europe, 2012.

[73] J. Takahashi and T. Fukunaga, "Implementation Attacks on an Immobilizer Protocol Stack," Proc. 11th Embedded Security in Cars Conference (escar) Europe, 2013.

[74] S. Mangard, E. Oswald, and P. Thomas, "Power Analysis Attacks - Revealing the Secrets of Smartcards," Springer-Verlag, US, 2007, ISBN:978-0-387-30857-9.

[75] J. Marc and T. Michael (Eds.), Fault Analysis in Cryptography Information Security and Cryptography, Springer-Verlag Berlin

Heidelberg, 2012, ISBN: 978-3-642-29655-0

[76] S.V.D. Beek, R.V.-Ardatjew, and F. Leferink, "Robustness of Remote Keyless Entry Systems to Intentional Electromagnetic Interference," Proc. International Symposium on Electromagnetic Compatibility (EMC Europe), pp.1242–1245, 2014.

[77] J. Davenport, "Thieves jam car locks to steal shopping," http://www.standard.co.uk/news/thieves-jam-car-locks-to-steal-shopping-6377639.html, accessed Feb. 20, 2018.

[78] A. Francillon, B. Danev, and S. Capkun, "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars," Proc. Network and Distributed System Security Symposium (NDSS), pp.1–15, 2011.

[79] D, Noguchi, "Potential Risks of Automotive Grade Linux," Proc. 4th Embedded Security in Cars Conference (escar) Asia, 2017.

[80] M. Wolf, R. Lambert, T. Enderle, and A.D. Schmidt, "Wanna Drive? Feasible Attack Paths and Effective Protection Against Ransomware in Modern Vehicles," Proc. Embedded Security in Cars Conference (escar) Europe, 2017.

[81] D. Spaar, "Beemer, Open Thyself! -Security vulnerabilities in BMW's ConnectedDrive," c't Feb. 2015, https://www.heise.de/ct/artikel/Beemer-Open-Thyself-Security-vulnerabilities-in-BMW-s-ConnectedDrive-2540957.html, accessed Feb. 20, 2018.

[82] GM, "On star," https://www.onstar.com/us/en/home.html, accessed Feb. 20, 2018.

[83] Audi, "Audi connect, A grown-up way to connect the dots," https://www.audiusa.com/technology/intelligence/audi-connect, accessed Feb. 20, 2018.

[84] Nissan, "Nissan connect," https://www.nissanconnect-uae.com/en-gb/Support/Quickstart, accessed Feb. 20, 2018.

[85] Mitsubishi, "2018 Mitsubishi Outlander PHEV Smartphone Remote Control App," http://www.continentalmitsubishi.com/blog/2018-mitsubishi-outlander-phev-smartphone-remote-control-app/, accessed Feb. 20, 2018.

[86] S. Kamkar, "Drive It Like You Hacked It: New Attacks and Tools to Wirelessly Steal Cars," Proc. DEFCON Hacking Conference 21, 2015.

[87] P. Paganini, "Flaws in BMW ConnectedDrive Infotainment System allow remote hack," http://securityaffairs.co/wordpress/49149/hacking/bmw-connecteddrive-hacking.html, accessed Feb. 20, 2018.

[88] T. Hunt, "Controlling vehicle features of Nissan LEAFs across the globe via vulnerable APIs," https://www.troyhunt.com/controlling-vehicle-features-of-nissan/, accessed Feb. 20, 2018.

[89] D. Lodge, "Hacking the Mitsubishi Outlander PHEV hybrid," 2016, https://www.pentestpartners.com/security-blog/hacking-the-mitsubishi-outlander-phev-hybrid-suv/, accessed Feb. 20, 2018.

[90] P. Paganini, "Security vulnerabilities in Hyundai Blue Link mobile app allowed hackers to steal vehicles," security affairs, 2017, http://securityaffairs.co/wordpress/58402/breaking-news/hyundai-blue-link-flaws.html, accessed Feb. 20, 2018.

[91] S. Vonnegut, "Mobile Application Security: 15 Best Practices for App Developers," 2015, https://www.checkmarx.com/2015/08/19/mobile-application-security-15-best-practices-for-app-developers/, accessed Feb. 20, 2018.

[92] TOYOTA, "Toyota Bringing Advanced ITS Technology to Mass-market Models," 2015, http://newsroom.toyota.co.jp/en/detail/9676551, accessed Feb. 20, 2018.

[93] K.H.-Geisler, "2017 Cadillac CTS gets V2V upgrade," 2017, https://techcrunch.com/2017/03/09/2017-cadillac-cts-gets-v2v-upgrade/, accessed Feb. 20, 2018.

[94] "Car 2 Car Communication Consortium," https://www.car-2-car.org/index.php?id=5, accessed Feb. 20, 2018.

[95] A. Kiening, D. Angermeier, H. Seudie, T. Stodart, and M. Wolf, "Trust Assurance Levels of Cybercars in V2X Communication," Proc. ACM workshop on Security Privacy & Dependability for cyber vehicles (CyCAR 13), IEEE-CS, pp.49–60, 2013.

[96] L.A. Klein, "ITS Sensors and Architectures for Traffic Management and Connected Vehicles 1st Edition," CRC Press; 1 edition, 2017, ISBN-10: 1138634077.

[97] T. v. Roermund, "Secure Connected Cars For a Smarter World," White paper, pp.1–36, 2015.

[98] CERT UK, "Denial of service attacks: what you need to know," pp.1–9, 2014, https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/Denial-of-service-attacks-what-you-need-to-know1.pdf?platform=hootsuite, accessed March 7, 2018.

[99] Y. Zhang, A. Juels, M.K. Reiter, and T. Ristenpart, "Cross-VM Side Channels and Their Use to Extract Private Keys," Proc. ACM conference on Computer and communications security (ACM CCS) ACM, pp.305–316, 2012.

[100] T. Ristenpart, E. Tromer, H. Shacham, and S. Savage, "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds," Proc. ACM conference on Computer and communications security (ACM CCS), ACM, pp.199–212, 2009.

[101] O. Aciiçmez, "Yet another MicroArchitectural Attack:: exploiting I-Cache," Proc. ACM workshop on Computer security architecture (CSAW), pp.11–18, 2007.

[102] E. Tromer, D.A. Osvik, and A. Shamir, "Efficient cache attacks on AES, and countermeasures," Journal of Cryptology, vol.23, no.1, pp.37–71, 2010.

[103] ISO 26262-1:2011 Road vehicles – Functional safety – Part 1: Vocabulary, pp.1–23, Publication date: 2011-11.

[104] P. Vembar, "A Security Engineering Process for Automotive Embedded Systems A Bosch Approach," Proc. 3rd Embedded Security in Cars Conference (escar) USA, 2015.

[105] SAE, "Cybersecurity Guidebook for Cyber-Physical Vehicle Systems," Standard: J3061_201601, Issued: 2016-01-14.

[106] A. Tschache, "The Challenges of Establishing and Maintaining a Common Security Baseline, Vehicle Security from the OEM Perspective," Proc. 4th Embedded Security in Cars Conference (escar) Asia, 2017.

Junko Takahashi received the B.S. and M.S. degrees in physics from Waseda University, Japan, in 2004 and 2006, respectively, and the Ph.D. degree in engineering from the University of Electro-Communications, Japan, in 2012. She joined the NTT Information Sharing Platform Laboratories, Nippon Telegraph and Telephone Corporation in 2006. Currently, she is a researcher with the NTT Secure Platform Laboratories, Nippon Telegraph and Telephone Corporation (NTT). At NTT, she has evaluated the resistance of smart cards against side-channel analysis and engaged in basic research of fault analysis attacks and cache timing attacks especially against block ciphers. Recently, she has been studying automotive security evaluations such as in-vehicle devices, protocols, and vehicle services associated with cloud environments. She was a member of the cryptographic module committee in the Cryptography Research and Evaluation Committees (CRYPTREC) from 2011 to 2013. She is a member of the Information and Communication Engineers (IEICE) and Information Processing Society of Japan (IPSJ). She has been a committee member of the Hardware Security technical committee from 2016 in the IEICE and the IPSJ special interest group on system architecture from 2018. She was awarded the 2008 symposium on cryptography and information security (SCIS) paper prize and her paper of JIP Vol. 25 was selected as a specially selected paper in the IPSJ in 2017.