Contribution

The Cyber Security on Automotive Industry
Hiroshi Kamiyama*

Abstract

In today’s car society, with the new function of automatic driving or connected, the car has entered the world outside and the world of “Tsunagaru”, the so-called cyber space, and has never experienced in this 100-year history, many things are going to happen. In this new world, the threat of cyber attack and the security technology to protect it, which can be a daily event, while noting the trend of communication in the world of in-vehicle controller, not only the trend of the industry but also efforts at the national level, examples We will introduce it.

Key Words: Communication System / Cyber security, Connected Car, Controller Area Network, On-Board Diagnostics

Prologue

On a rainy morning on June XX, 2018, at the house of Mr. A living in Saitama prefecture, Mrs. A pressed the engine start button to start their car to drive Mr. A to the train station as usual. Normally, the starter starts the engine in a few seconds and the engine makes a reassuring sound. But this morning, the engine did not start no matter how many times Mr. A’s wife pressed the start button. Mr. A gave up on going to the train station by car and rushed to the neighborhood bus stop. Mrs. A who was left there thought the battery had gone flat and called the Japan Automobile Federation (JAF) who also tried to start the car, but the car stayed perfectly still.

When she happened to check her e-mail on her smartphone, there was a suspicious e-mail. “Seems like you are in trouble with the engine not starting”. “I am XX of YYY Motors that specializes in car remote diagnosis. Your car is a connected car with an autonomous driving system so it is connected to various services on the Internet. Through a diagnosis service at car starting, which is one of the services, our service center received a flash report from your car this morning, informing us that your car failed to start. If you send 0.03 BTC (Note 1) by e-mail to the following address, we can immediately make a diagnosis and repair your car remotely, and restore it to a state in which the engine will start.” Such a world has become a reality.

1. Introduction

For security in the automotive world up to now, security measures have mainly been to prevent car theft or theft of items in cars, which are known as “physical attacks” by thieves, such as stealing a car using a copy of a mechanical key, tampering with door lock mechanisms and stealing money or valuables left in a car, or stealing navigation systems. As a result of these efforts, various measures are used, including the widespread use of engine immobilizers and the development and legislation of vehicle intrusion sensors. And it is an already a known fact that these measures have produced results as security methods against car theft.

Meanwhile in the IT world, with the spread of the Internet as a convenient means of communication, as represented by the term “information security”, attacks from cyberspace aimed at exploiting information on personal computers and servers have been recognized as threats since around 2000, and various countermeasures represented by anti-virus software have been taken. However, in recent years virus subspecies are being generated one after another, and these viruses remain on the rampage while the damage from them is changing from exploitation of information to demanding money and valuables. This situation generated the word “cyberwarfare” and these threats are now handled as national action items.

* Electronics Business Unit, Electronics Components Design Group

Note 1) BTC: Unit of the virtual currency bitcoin, which started operation in 2009.
2. Automobile communication and security

2.1. History of automobile communication

In the automobile world, along with the spread of electronic control systems (computer control systems) for various equipment which began as a response to the tightening of emission regulations from the 1970s, the exchange (communication) of data (information) required between controlled equipment has become active, and with the diversification of and the increase in the amount of information, means of communication have changed from analog signals to digital signals at every moment.

In recent cars, communication between controlled equipment with the Controller Area Network (CAN) protocol has spread such that it is taken for granted. Harnesses for both the communication lines and power supply lines are laid all throughout vehicles from light cars to luxury cars. It is said that the total length of such harnesses exceeds 3 km in a luxury car. Today's electronic control would not be effective without this communication system.

2.2. Provision of various services including fault diagnosis

The widespread use of the common communication protocol, CAN, has enabled a variety of in-car information to be exchanged, and the provision of services has also developed in various forms through these lines of communication.

For the purpose of improving the worsening air pollution associated with motorization, the United States Environmental Protection Agency (United States EPA) and the California Air Resources Board (CARB) established and legislated emission regulations, and fault diagnosis of in-vehicle electronic control components and the associated communication systems were standardized (OBD II in 1996). With this standardization, a special communication port (OBD port) for facilitating easy communication with components connected to CAN and targeted for diagnosis was also standardized and its installation was made compulsory. By connecting a diagnostic device with similarly standardized specifications, it has become possible to diagnose a wide range of cars.

By these standardizations, fault diagnosis and repairs of complicated electronic control systems were made more accurate and easy, and it goes without saying that convenience improved drastically.

However, as information from in-vehicle electronic control components and control communication systems is easily monitored via the OBD port, a range of services have been developed and are being provided. One example is a service that obtains and analyzes the driver's driving state and control state through a wireless system connected to this port and uses this information to calculate car insurance.

2.3. Close ⇒ Open

With the development of diagnostics and services in this way, in-vehicle communication that started for communication between in-vehicle components has rapidly changed from a closed environment to an open environment where communication is performed between the car and outside.

Along with this change, a bold experiment and research video was presented at the DEFCON hacker convention held in the U.S. in 2013, where famous hackers supported by the Defense Advanced Research Projects Agency (DARPA) used their PCs to break into and intervene an in-vehicle communication system through a direct connection to OBD II port and the communication harness of the vehicle. (4)

In the presentation, they mentioned a possibility of breaking into and controlling an in-vehicle communication system not only by a direct connection to the OBD port or communication line but also remotely. Without a doubt, they opened a Pandora’s box in terms of cars and cyber security that would come up later.

Meanwhile, open communication between cars and outside keeps developing, and it is a well-known fact that cars have started to be handled as IoT devices as represented by connected cars.

2.4. From information security to cyber security

At the presentation at DEFCON in 2013, acts for accessing a car by connecting to the OBD port or by directly connecting to the system to exploit and falsify information on the CAN communication line were introduced as threats. The term “information security” for cars was used expressed countermeasures against these kinds of acts. The first countermeasure taken was to design the network architecture (Fig. 1) so that the OBD port equipped as standard equipment is separated from the main CAN communication line to prevent information transmitted on communication line from being easily seen and falsified from the outside. Around that time,
in order to realize this architecture, automotive manufacturers started to introduce a gateway unit on the communication line to separate each ECU from the OBD connectors (previously ECUs and OBD connectors were connected to the same communication line for ease in handling and convenience).

Fig. 1 Security Network Design

2.5. Connected car

Over the past 10 years, the development of car functions and services has undergone a revolution that completely overtures the history of the previous 100 years. Cars have turned into running computers as seen by autonomous driving and car electrification, and electronic control has completely replaced mechanical control. Looking at competitors, now there are not only conventional automotive industry competitors but also many new competitors from other industries aiming to manufacture new concept cars.

The factors that brought about and made this change possible include the increased sophistication and volume of information used in controlling cars and the increasingly sophisticated and complex communication networks that enable transmission of such information.

In addition, with the aim of making functions and services more sophisticated, information that was transmitted in the closed environment of a conventional car, such as for conventional communication related to diagnostic results as well as information necessary for control, is now starting to be actively communicated to the open environment outside the vehicle.

A wide range of information from the outside and on the Internet is also actively used, and this information is received by linking the in-vehicle navigation system to a 3G or 4G connected smartphone using a wireless connection such as WiFi or Blue tooth, or by directly connecting the Data Communication Unit (DCU) incorporated as part of the car system to a 3G or 4G phone line. This shows that cars are now literally connected to cyberspace.

In the field of security, this results in car connections changing from the previously mentioned “information security” world to the “cyber security” world, and at DEFCON 2015, new threats embodied by the following attacks were made public: a vehicle traveling far away was attacked from cyberspace and stopped on an expressway, and the steering of the vehicle was controlled to take the vehicle in a direction other than intended by the driver. It is said that this presentation lead to the recall of Chrysler’s Jeep Cherokee that was used in the presentation. Needless to say, the threat of cyber attacks by which the safety of a car is jeopardized resulting in a recall sent shockwaves throughout the automotive industry.

3. Protection of cars from cyber attacks

By stepping into the cyberspace world, cars have moved a step closer to the IT world, and in terms of attacks from cyberspace and related security measures, ideas and countermeasures in line with those of the IT world are required.

The speed of development and thinking with regard to safety vary greatly between the IT world and the automobile world. As we were thrown into a world to which various ideas, standards, regulations etc. cultivated during nearly 100 years of car history do not apply at all, a new approach of fusing with IT has become extremely important.

This means we need to quickly collect information on security threats that are already happening in the IT industry and actively incorporate security measures for those threats in the development of cars. To protect the information and control of cars, activities to incorporate some of the methods already used in the IT industry have already started.

One of those activities is information protection by establishing communication topology using the gateway unit described earlier. However, based on the idea of multi-layered defense that provides protection using many defensive methods, something that is already in place in the security world, it is not a good idea to incorporate only one method. We need a second and third defensive method.
3.1. Encryption of communication
In line with these trends, the automotive industry has also started commonly adopting a method that encrypts and decrypts data sent between two devices using private keys to enhance security.

For these private keys, security is maintained by providing a different private key for each individual car and each different ECU. A mechanism for collectively managing the vehicle information that uses the key and the key information itself is also required.

In addition, because this key needs to be certified when necessary and it is necessary to show that the key is trustworthy at any time, issuance and management must be performed together as a set with a certification authority, so mechanisms and processes that did not exist in the conventional car life cycle are now required.

Generally, information transfer using these keys is performed for credit cards etc., and the keys are periodically changed at card replacement in order to maintain the security of the keys.

To maintain the security of keys and ensure safety, keys used for in-vehicle devices also require the establishment of lifecycle management from the manufacturing through to the scrapping of a car, and the construction of services and mechanisms that did not exist in the conventional car business is an urgent task.

3.2. Increasing sophistication of defensive and detection functions
The virtualization technology that started to spread with earnest from around 2010 is also one of the representative defense technologies in the IT world.

In ECUs that connect to the outside world, this technology is used to divide the software region into a virtual region and an actual control region, place data received from the outside in the virtual region and separates it from the region involved in internal control so that the range of influence will be limited to only the virtual region in the event of a virus infection, thus preventing the internal system from being affected.

We need to actively introduce defensive functions already introduced in the IT world and achieving good results to in-vehicle devices, however methods established in the IT world cannot be introduced as-is to built-in devices, such as in-vehicle devices, due to the greatly differing hardware configurations of the target ECUs so some changes and modifications that suit in-vehicle devices are required. However, due to the cost barrier for hardware generally used for built-in devices, how to create lightweight logic so that inexpensive CPUs can be used is an issue that requires solving.

4. Efforts by industry-government cooperation
4.1. Standardization and legislation
Protecting car security is tackled as the most important issue, not only in the development and evolution of technologies for countermeasures by individual automotive companies and parts suppliers, but also by the whole automotive industry and at national level, and movement towards standardization and legislation is seen in various forms.

In the United States, class action lawsuits have already been taken against automotive manufacturers that neglected cyber security measures, and preparation for a security measures bill is advancing after being invoked by a senator. As seen by this, standardization and legislation for security have accelerated as national level movements.

In 2015, the Society of Automotive Engineers (SAE) was quick to create a cyber security guidebook for cars called J3061 that shows the direction of security technologies including processes. The Ministry of Economy, Trade and Industry of Japan also created cybersecurity management guidelines in cooperation with the Information-technology Promotion Agency, Japan (IPA) at the end of 2015, and asked a wide range of industries including the automotive industry to take cyber security measures. It is certain that global standardization including ISO and legislation will further accelerate in the future.

In September 2017, legislative bill HR3388, that addresses autonomous driving, was passed by the House of Representative of the United States, and standardization and legislation toward the automotive society of the coming age are steadily advancing.

With cyber security measures defined as an area of non-competition in the automotive industry, from 2012 in Japan activities aimed at making the achievements of companies meet ISO standards across individual companies are continuing, with Jaspar (Japan Automotive Software Platform and Architecture), the Society of Automotive Engineers of Japan, and the Alliance of Automobile Manufacturers taking the lead role.

4.2. Security management
Security management throughout the life of a car from the design and manufacturing phase to delivery to the
customer and finally scrapping is newly defined in these legislation bills and standards.

Previously, car life cycle management focused on areas such as repairs, maintenance, car inspection services to maintain the performance and functions of cars delivered to customers. However, in the IT world too, cyber security is evolving every day for both attack methods by attackers and countermeasures on the defense side. As the same applies to cars, we are required to make drastic changes to car life cycle management and services to maintain and improve security performance against the threats of cyber attacks.

This means that the anti-virus software of in-vehicle security products needs to be updated in the same way that the anti-virus software on the PC use every day is updated. In order to avoid causing customers the hassle of frequent visits to service shops, establishing a software updating mechanism that uses wireless communication so that customers can update the software of in-vehicle devices no matter where they are is emerging as one of the new issues.

5. As an automotive parts supplier in the new age

Facing this age of such drastic changes in the automotive industry, with the aim of fusing with the IT industry in the security world, Calsonic Kansei Corporation not only quickly decided on cooperation with Quarkslab, a leading security vendor in France, but also established WHITE MOTION LLC as a limited liability company together with Quarkslab to specialize in automotive cyber security, something that no one had tried to address before, for the purpose of organizing a system that enables us to provide our customers with products that incorporate state-of-the-art technologies and future trends in the car industry and the latest security technologies in the IT industry.

In addition to conventional CAN communication, its evolutionary forms, new CAN-FD and Ethernet protocols have been added to in-vehicle communication systems. With these new protocols, the communication network for supporting speeding-up and increasing the volume of control information associated with more sophisticated functions of in-vehicle control parts provided for autonomous driving is steadily advancing.

The gateway unit that supports this network topology from the core is also one of the main body electronics products of Calsonic Kansei Corporation. In addition to the diversification of multi communication and the realization of multi-channel protocols, we are accelerating the development of a function capable of updating security functions throughout the lifetime of a car, and we are now organizing a system that enables us to provide our products to customers in tune with the evolution of in-vehicle communication systems.

Regarding the management of security keys, which is also important in the life cycle management of cars, Calsonic Kansei Corporation established a security key management system that enables us to support car life cycle management globally from design and manufacturing to scrapping together with a security company that has a key certification authority function, and we are now ready to respond to the demands of automotive companies and to deliver security and safety to driving customers.

6. Conclusion

The automotive industry has reached a big turning point unprecedented in the history of the past 100 years where we are facing the urgent need to tackle the issue of improving the new value we provide to customers in the form of autonomous driving and electrification and the issue of providing safety that must be maintained.

In order to defeat our competitors in the IT world, which we have never competed with before, we ventured into competitions to accelerate the technological development beyond conventional industry frameworks.

Epilogue

In the morning of July XX, 2018, just like Mr. A mentioned earlier, at the house of Mr. B who is subscribed to a connected service, as usual Mr. B’s wife was waiting for him to get ready with the engine of their car running to drive him to the local train station. Your guess is right. Mr. A and Mr. B use the same connected service to obtain information every morning on railway operations, traffic jams, and how to avoid traffic jams. But one difference between Mr. A and Mr. B was the in-vehicle architecture realizing the connected services and its component parts. In the case of Mr. B’s car, when Mrs. B started the engine, a “CK&M Inside” logo appeared on the navigation screen. The ECU installed in Mr. B’s car was fitted with the latest product for cyber attack countermeasures, as developed by Calsonic Kansei Corporation and WHITE MOTION LLC. Unfortunately, the evolution of cyber attacks and the improvement of defensive measures against them is a cat-and-mouse game. So far, we can’t see where this will lead. The important
thing for car life in the future is to understand that cars are IT devices and to perform security maintenance just like on your PCs.

In order to cope with the latest attacks and viruses, in the age where announcements recommending you update your security software come in periodically, I hope we can enjoy a comfortable car life, while keeping security maintenance in mind just like waxing a car.

References

(3) Ministry of Economy, Trade and Industry, IPA: Cybersecurity Management Guidelines Ver. 2.0, November 16, 2017
(4) Charlie Miller, Chris Valasek: Adventures in Automotive Networks and Control Units, 2013 DEF CON 21
(5) SAE International: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems, 20160219