Cyber-attack Countermeasures for Cars

Masashi Tanaka, Junko Takahashi, and Yoshihito Oshima

Abstract

Cyber-attacks on cars have become a serious real-world issue following recent revelations in which it was verified that cars can be illegally operated via the Internet. Thus, there is an urgent need for security countermeasures to protect the safety and security of cars. This article introduces the current trends in car security and describes car security evaluation techniques and countermeasures that we are currently working on at NTT Secure Platform Laboratories.

Keywords: car security, connected cars, in-vehicle networks

1. Introduction

The proportion of electronic systems in vehicles has increased significantly in recent years. Nowadays, a wide variety of vehicle functions are controlled electronically by numerous vehicle control computers (electronic control units; ECUs) connected to in-vehicle networks. It is expected that a rich variety of automotive services such as connected cars and automated driving will be made possible by connecting these automotive systems to external networks.

However, the high speed at which automotive systems are being introduced and connected to external networks is raising important considerations regarding the cybersecurity aspects of vehicle design. Some cases relating to cyber-attacks on vehicles that have had real-world repercussions are introduced below.

1.1 Vehicle theft by duplicating key code

These days, most vehicles are equipped with immobilizer systems. These immobilizers use cryptography to authenticate the chip inside a key fob with a microcomputer in the vehicle, and only allow the engine to start if the authentication succeeds. This authentication is sometimes performed using the manufacturer's proprietary encryption algorithm, and there have been reports of attackers exploiting weaknesses in these algorithms to illegally obtain secret authentication keys.

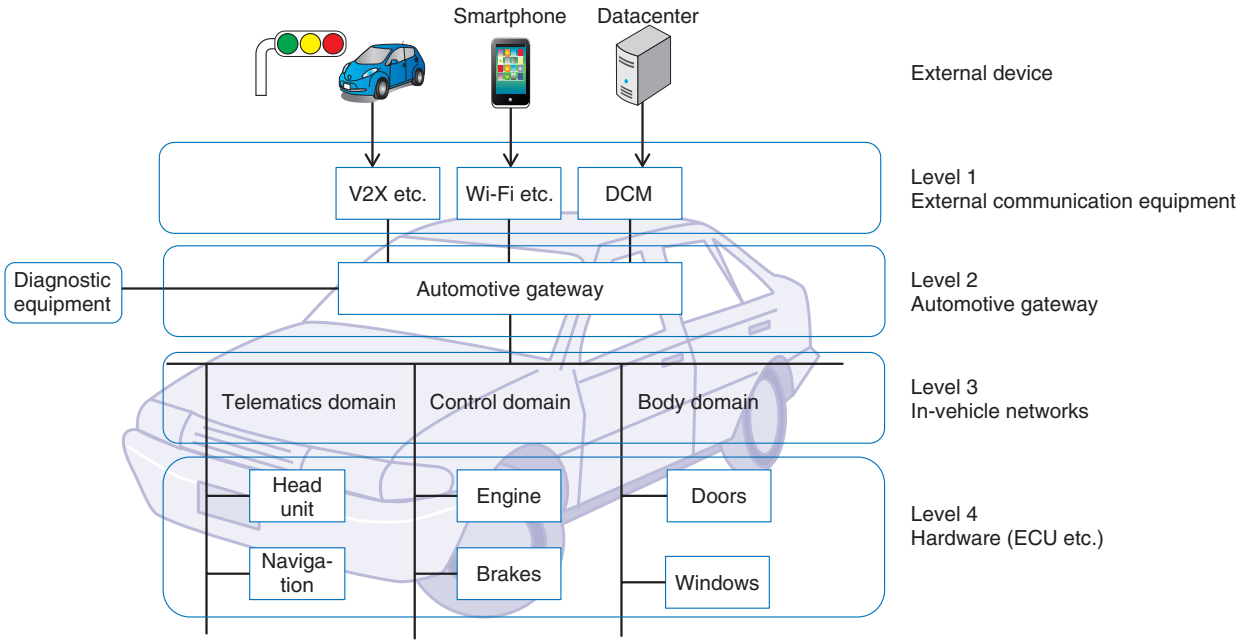
1.2 Using the OBD2 to hack a vehicle

The OBD2 (On-board Diagnostic, second generation) port is a standard diagnostic interface for vehicles. By connecting it to a data acquisition device and a personal computer (PC), it is possible to acquire and interpret messages that are exchanged via internal communication (e.g., controller area network (CAN) messages), and to infer the meaning of these messages in conjunction with the vehicle's behavior at that time [1]. It has been demonstrated that a PC can be used to exploit this information by injecting forged messages to perform actions such as tampering with the speedometer display or operating the steering and/or brakes contrary to the driver's intentions.

1.3 Unauthorized remote control of vehicles

In 2015, security researchers successfully hacked a Jeep Cherokee. They were able to take remote control of the vehicle's on-board computer and entertainment system, and remotely controlling the vehicle's brakes and steering over the Internet [2]. After that, Fiat Chrysler recalled 1.4 million vehicles. This remote hacking over the Internet had a great impact on the automotive industry.

As this example shows, cyber-attacks on vehicles



DCM: data communication module
V2X: vehicle-to-everything; a form of technology that allows vehicles to communicate with moving parts of the traffic system around them

Fig. 1. Automotive system architecture and hierarchical classification from a security viewpoint.

can have significant effects on modern society by infringing on people's property and personal safety. Efforts must therefore be made to implement security measures to prevent cyber-attacks on vehicles in order to achieve a safe and secure social infrastructure.

We introduce below some of the recent trends in countermeasures to vehicle cybersecurity threats, and the efforts that have been made so far at NTT Secure Platform Laboratories.

2. Vehicle security technology trends

The automotive system architecture that is becoming the norm in recent years is shown in **Fig. 1**, and a hierarchical classification of these systems is presented from a security viewpoint.

2.1 Automotive system architecture

(1) Level 1

Level 1 communicates with the outside world. It consists of on-board equipment for communicating with mobile networks, Wi-Fi* networks, and vehicle-to-vehicle/vehicle-to-infrastructure systems (e.g., V2X (vehicle-to-everything) communication).

(2) Level 2

Level 2 controls all the automotive systems in a vehicle. It consists of an automotive gateway that exchanges messages between internal ECUs and external devices communicated at Level 1 and exchanges messages between in-vehicle networks in the vehicle.

(3) Level 3

Level 3 is a network (in-vehicle network) that conveys messages between ECUs. It is partitioned into multiple in-vehicle networks according to the ECU applications and roles, such as a telematics domain for vehicle navigation and the like, a control domain for brakes and the like, and a body domain for door locks and the like. It uses in-vehicle communication protocols suited to each system such as a CAN or local interconnect network (LIN).

(4) Level 4

Level 4 controls each component of the vehicle such as the engine, brakes, and door lock functions. It consists of ECUs and other such components that perform a variety of functions.

2.2 Security of each level

(1) Security of Level 1 (external communication

* Wi-Fi is a registered trademark of Wi-Fi Alliance.

equipment)

This includes authentication and access control to confirm that the vehicle is communicating with trusted external systems or that the communication has been authorized, while blocking communication with other external systems. Communication channels established with external systems may need to be encrypted in order to prevent eavesdropping or the injection of unauthorized messages.

(2) Security of Level 2 (automotive gateway)

Level 2 tasks include i) filtering to ensure that only authorized messages can flow between external systems and in-vehicle networks, or between different in-vehicle networks, ii) key management to manage the keys used by the ECU for encryption and authentication, and iii) anomaly detection to detect security anomalies in messages flowing inside the vehicle.

(3) Security of Level 3 (in-vehicle networks)

This includes tamper detection by detecting when messages transmitted between ECUs have been rewritten, and performing encryption to prevent eavesdropping.

(4) Security of Level 4 (hardware (ECU etc.))

This includes the use of secure designing and programming methods to avoid the inclusion of vulnerabilities in programs running on the ECU and to secure booting to verify that the firmware and operating system have not been tampered with when starting up.

In the future, as connections to vehicle communication networks become more commonplace and a wide diversity of network-type services are made available, it is envisaged that cyber-attacks will also become more advanced and more sophisticated. Just as with the security countermeasures used in information technology systems, it is thought that it will be necessary to implement multi-stage, multi-layered defenses combining security technologies for each level of the vehicle hierarchy.

3. NTT research and development (R&D) activities in automotive security

R&D efforts focused on automotive security are underway at NTT. We describe those efforts in this section.

3.1 Overview

At NTT Secure Platform Laboratories, we are researching and developing security evaluation techniques that assess the resilience of vehicles to cyber-attacks, and countermeasures to attacks at each of the four security levels described above. As examples of security evaluation techniques and countermeasures, we introduce an attack at Level 3 that induces improper behavior in the LIN protocol and the countermeasures to this kind of attack. We also introduce some examples of our research into safety evaluation techniques and countermeasures for immobilizer authentication protocols related to Level 4 security.

3.2 Attacks that induce improper behavior in LIN and countermeasures against them

Many studies have recently been done on the security of in-vehicle networks, and most of them have been concerned with CAN, which is used to control vehicle parts such as the engine and brakes. In contrast, although significant threats would be presented if an attacker improperly gained control of LIN, which is used in controlling steering wheels, seats, and doors, it was not clear whether LIN is able to withstand attacks aimed at inducing improper behavior, or that any countermeasures are needed. In collaboration with other companies, we have therefore proposed an attack method to induce improper behavior in LIN, as well as countermeasures against this kind of attack [3].

LIN is based on a master-slave model. The master node transmits a header including the identifier (ID) that denotes the contents of the process, and the transmit/receive slave nodes corresponding to this ID start to transmit and receive data. Since the LIN specification does not define how to proceed after an error has been detected, LIN error handling mechanisms are application-dependent. For example, in some cases when the data transmitted by a node differ from the data on the bus, an error is detected, and the node handles the error simply by halting the data transmission and waiting for the next header. We have shown that the characteristics of this error handling mechanism can be used to make false data appear to be correct to the receiving slave node, thereby allowing incorrect behavior to be induced. Specifically, the attacker monitors the bus, and at the same instant that the correct data are transmitted following the reception of the header (**Fig. 2(a)**, **(b)**), the attacker injects false data to create a collision (**Fig. 2(c)**), whereby the transmission of the correct data is halted by the error handling mechanism. At the same time the transmission of the correct data is halted, the attacker injects false data, and this can be incorrectly recognized as correct data by the receiving slave node. This showed that it is possible to induce abnormal behavior contrary to the driver's intentions.

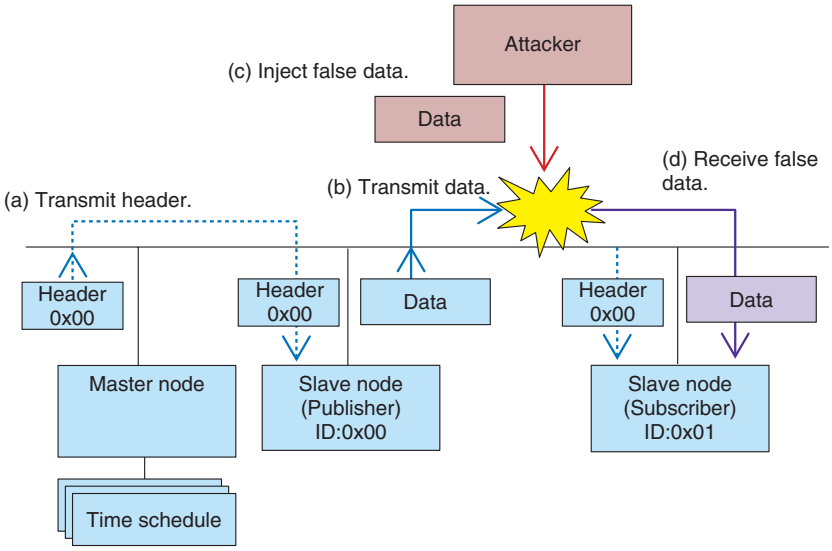


Fig. 2. Attack technique that induces abnormal behavior in LIN.

As countermeasures against this attack, we proposed a method to assign the significant bytes in data and a method to send an abnormal signal overwriting the false data when a communication error has occurred.

3.3 Evaluation techniques and countermeasures for immobilizer authentication protocols

In 2010, an authentication protocol that uses the standard cryptographic algorithm, the Advanced Encryption Standard (AES), was proposed for use in immobilizers instead of using proprietary cryptography for authentication. The authentication protocol has been subjected to previous theoretical analysis, and no vulnerabilities had yet been discovered. However, in our research, we found that the secret key stored in the key fob can be exposed by applying a fault analysis attack to the immobilizer system [4]. The fault analysis attack is a kind of implementation attack. In the protocol we targeted, the key fob contains three copies of the secret key; these copies are used in sequence in order to make it unlikely to fail even when used under harsh circumstances. By focusing on this characteristic of the key storage, we proposed an attack method that changes the value of the secret key stored in the key fob by a sequential fault injection (**Fig. 3(a)–(c)**) and reduces the key candidate space of the secret key ("Analyze" sections of Fig. 3).

There are two patterns for authentication protocols of this type: unilateral authentication, where the vehicle authenticates the key, and bilateral authentication, where the vehicle and key authenticate each other. We showed that it is possible to identify the secret key in a practical amount of time when using a unilateral authentication scheme, and that key extraction is also possible when using bilateral authentication, depending on factors such as the number of electronic key fobs that are available. We also proposed countermeasures to the proposed attack method such as performing a preliminary comparison of the encryption results calculated using each secret key in order to check for any changes in the key values.

4. Future prospects

It is expected that many more functions will be needed in order to implement the self-driving cars and connected cars of the future. In line with this trend, we can expect that the attack surfaces (attack paths) of vehicles will become broader, and that attack methods will become more advanced. At NTT Secure Platform Laboratories, we will continue with R&D relating to the security of in-vehicle networks and automotive systems, and we will provide cyber-attack countermeasures necessary to keep the next generation of vehicles safe and secure. We will also contribute to the realization of vehicle security services that work together with cloud services and a secure communication infrastructure that connects in-vehicle systems with external systems.

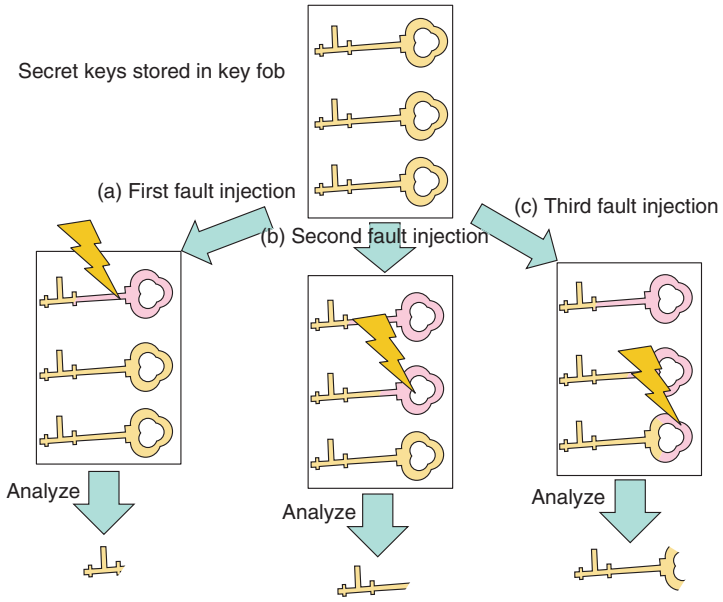


Fig. 3. Technique for evaluating immobilizer authentication protocols.

References

[1] C. Valasek and C. Miller, "Adventures in Automotive Networks and Control Units," DEF CON 21, Las Vegas, NV, USA, Aug. 2013.
[2] C. Valasek and C. Miller, "Remote Exploitation of an Unaltered Passenger Vehicle," Black Hat USA, Las Vegas, NV, USA, Aug. 2015.
[3] J. Takahashi, Y. Aragane, T. Miyazawa, H. Fuji, H. Yamashita, K. Hayakawa, S. Ukai, and H. Hayakawa, "Automotive Attacks and Countermeasures on LIN-Bus," J. Info. Process., Vol. 25, pp. 220–228, 2017.
[4] J. Takahashi and T. Fukunaga, "Fault Analysis and Countermeasures on an Immobilizer Protocol Stack," IEICE Trans. Fundamentals. (Japanese Edition), Vol. J99-A, No. 2, pp. 106–117, 2016.

Masashi Tanaka
Senior Research Engineer, Cyber Security Project, NTT Secure Platform Laboratories.
He received a B.S. and M.S. from Osaka Prefecture University in 1999 and 2001. He is presently researching cybersecurity of the Internet of Things (IoT).

Junko Takahashi
Researcher, Cyber Security Project, NTT Secure Platform Laboratories.
She received a B.S. and M.S. in physics from Waseda University, Tokyo, in 2004 and 2006, and a Ph.D. in engineering from the University of Electro-Communications, Tokyo, in 2012. She joined NTT Information Sharing Platform Laboratories in 2006. Her main research interest is the security of embedded systems such as side-channel analysis and automotive security. She was awarded the SCIS (Symposium on Cryptography and Information Security) 2008 paper prize. She is a member of the Institute of Electronics, Information and Communication Engineers (IEICE) and the Information Processing Society of Japan (IPSJ).

Yoshihito Oshima
Senior Research Engineer, Supervisor, NTT Secure Platform Laboratories.
He received a B.E. and M.E. in electrical engineering from Hokkaido University in 1994 and 1996. He joined NTT in 1996 and is currently conducting R&D on IoT cybersecurity. He is a member of IPSJ.