Security-risk-mitigation Measures for Automotive Remote Diagnostic Systems

Masaaki Miyashita
The Graduate University for Advanced Studies, Department of Informatics, Graduate School of Interdisciplinary Sciences, Present affiliation is Nissan Motor Corporation
Kanagawa, Japan
e-mail: m-miyashita@nii.ac.jp

Hiroki Takakura
National Institute of Informatics
Tokyo, Japan
e-mail: takakura@nii.ac.jp

***Abstract*— Modern automobiles are equipped with numerous electric control units that require an electrical diagnosis system for efficient maintenance. With the emergence of telematics communication in connected cars, remote diagnosis has become possible, allowing for the early detection of electric-system issues. However, remote diagnostic systems, especially those with services requiring special privileges, such as firmware updates or control of vehicle actuators, are vulnerable to cyberattacks. Considering this, we present security-risk-mitigation measures for such systems.**

Keywords-Automotive cybersecurity; Remote diagnosis; UDS.

I. INTRODUCTION

As technology advances, the electronic systems in automobiles are becoming more intricate. These systems consist of numerous components that are connected through in-vehicle communication networks. Diagnostic systems specifically designed for vehicles are required to pinpoint any malfunction. These systems usually require a diagnostic tool to be directly connected to a dedicated connector on the vehicle and must be operated at a garage.

With wireless communication systems increasingly used in vehicles, remote diagnosis systems have become more prevalent. These services enable an operator to read diagnostic trouble codes and data logs through wireless communication. This prompts the driver to bring his/her vehicle to a garage for repairs before the trouble becomes more severe. Diagnostic communications are used not only to read such data but also to write data to in-vehicle parts, such as firmware updates and initial settings of replacement parts.

Studies have indicated that cyberattacks targeting vehicles through diagnostic communications can result in significant damage. For example, it has been demonstrated that some diagnostic Controller Area Network (CAN) messages impacted major critical vehicle control systems, such as the engine, brake, and steering systems [1]. Car theft and privacy breaches are also potential risks of cyberattacks through diagnostic communication [2].

To address these security risks, we present security-risk-mitigation measures for remote diagnostic systems. These systems involve reading diagnostic trouble data and remote firmware-update tasks that were previously only executed at service stations. Our measures aim to reduce the potential security risks associated with these systems.

The rest of the paper is structured as follows. In Section II, we discuss automotive diagnostic communication. In Section III, current status and issues of remote diagnosis are presented. In Section IV, we propose our security-risk-mitigation measures. In Section V, we show how to avoid constraints when implementing proposed measures in vehicle component. Finally, we conclude our work in Section VI.

II. AUTOMOTIVE DIAGNOSTIC COMMUNICATION

The process of remote diagnosis involves the use of wireless communication between a vehicle and a diagnostic server located outside the vehicle. To diagnose the various components implemented in the vehicle, the in-vehicle wireless communication unit, which serves as the entry point to the vehicle, must communicate with other components through the in-vehicle communication network. To achieve this, it is most reasonable from a system-implementation standpoint to use the diagnostic communication protocol typically used for wired-connected diagnostic tools. While this protocol is effective for wired communication, there are security concerns when using it for wireless communication.

With this in mind, we examined the characteristics and issues of automotive diagnostic communications used in the in-vehicle network.

A. Overview of Diagnostic Communication

In 1991, the California Air Resources Board mandated the implementation of the On-Board Diagnostics (OBD) connector to standardize vehicle diagnostic communications. Today, the OBD2 connector is the industry standard interface and can use several communication protocols. CAN communication is prevalent in vehicle-embedded processors, and there is a shift towards faster diagnostic communication using Diagnostics over Internet Protocol (DoIP)-based communication with an Ethernet physical layer [3]. To address the need for faster communication and accommodate the increased complexity of automotive software, ISO14229-1 standardized the Unified Diagnostic Service (UDS) Protocol, which is now used as a standard communication protocol by many automotive companies. However, as software complexity increases, so do security concerns, as outlined in previous studies [4] and [5] on DoIP.

B. Diagnostic Tool

Advancements in diagnostic-communication hardware and software have brought about changes in diagnostic tools

used to identify failures in vehicles. Handheld terminals with basic Liquid Crystal Displays (LCDs) had been commonly used for diagnostic communication before the spread of CAN communication. However, with the increasing number of vehicles supporting diagnostic communication and the complexity of systems due to the introduction of IP communication, developing software for specialized hardware has become inefficient. Thus, it is now common to use a Personal Computer (PC) or tablet in Figure 1 as a diagnostic tool and connect it to an OBD dongle through USB, Bluetooth, wireless LAN, etc.

Figure 1. Diagnostic tools using PC/Tablet.

This approach has the additional benefit of enabling developers of general diagnostic tools that support vehicles from multiple automobile companies to easily acquire diagnostic tool hardware. However, it also raises concerns that these devices, which are essentially PCs and tablets with network connectivity as standard equipment, could be used as gateways for attackers to intrude into vehicles. Since diagnostic communication protocols are standardized and diagnostic tools and software can be purchased inexpensively, attackers can find vulnerabilities through reverse analysis.

C. Security-critical Diagnostic Communication Services

In diagnostic communication, the functionalities offered by a vehicle's Electronic Control Unit (ECU) for using a diagnostic tool are referred to as "services". These services include reading and writing data to operate the ECU as well as diagnostic commands, such as fault code retrieval. The conversation surrounding automotive cybersecurity threats highlights the potential for attacks via the OBD connector by exploiting these services. Previous research [6] and [7] have demonstrated that the following UDS have been susceptible to exploitation.

- Input/Output Control Service: This service controls the input and output signals that are connected to the specified ECU from the diagnostic tool. Its primary function is to identify the failure point. For instance, if the wipers do not operate even after turning on the wiper switch, this service can be used to forcibly drive the wiper motor, and if the wipers start operating, it proves that the motor and its wiring have no problem. This approach helps in efficiently narrowing down the failure point. However, this service can lead to generating hazardous vehicle behavior that the driver did not intend.
- Write Data by Local ID Service: This service is designed for configuring the initial settings and adjusting the parameters of installed components. It can, for example, be used to write the dynamic radius value of a tire to the ECU to calibrate the speedometer or enable/disable optional parts. However, if this service is abused, users may experience adverse effects, such as inaccurate information display or suspension of certain functions.
- Reprogramming Service: This service is for rewriting ECU firmware installed in sold vehicles, usually to correct quality defects in the firmware. However, if this service is abused, it could result in various issues. For instance, the rewritten ECU may behave improperly or even spoof other ECUs, leading to more significant problems, such as sending malicious communication data to other ECUs. Therefore, it is crucial to use this service only for its intended purpose and avoid any abuse.

Decades ago, owners could modify vehicle characteristics by rewriting the ECU firmware or overriding the CAN bus signals. However, due to certain essential services' impact on crucial vehicle features, such services are locked by default within secured ECUs. To grant access to locked services, a process known as "security access (service ID27)" is typically used to verify the legitimacy of the user or diagnostic tool.

D. Authentication by Service ID27 "Security Access"

In diagnostic communication by using UDS, security access communication was generally executed using the following procedure (refer to Figure 2) with a pre-shared symmetric key K.

1. The diagnostic tool to be authenticated sends a seed request (request seed) to the ECU to be unlocked.
2. Upon receiving the request, the ECU sends back seed data X, including random numbers, to the diagnostic tool to avoid the risk of replay attacks.
3. The diagnostic tool processes the obtained X using the key data K and computes the response data Y.
4. The diagnostic tool sends Y to the ECU. ECU calculates Y' from the K & X sent by ECU itself.
5. If Y' and Y are the same value, the authentication is successful and the ECU unlocks the locked critical services.

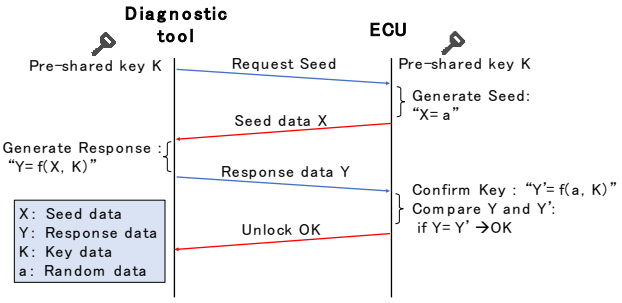

Figure 2. ECU unlock sequence by security access.

If a symmetric key is used for authentication in security access executed by such procedures, an attacker may be able to obtain the key information through reverse analysis of the ECU or diagnostic tools. Therefore, the following solutions have been devised.

- To minimize the risk of reverse key analysis, it is essential to safeguard the private key in asymmetric key authentication. The private key should not be stored in the diagnostic tool. It instead should be kept in the Hardware Security Module (HSM), which is located on the authentication server or in a secure location with restricted access outside the tool. This requires the diagnostic tool to be connected to the authentication server with the HSM. To achieve this, infrastructure development and maintenance are necessary, such as installing a network environment at the garage and managing accounts that enable the diagnostic tool to log into the authentication server.
- Service ID27 does not provide security functions, such as user-privilege management or session key exchange with authentication, requiring each auto manufacturer to develop its own customizations. To remedy these issues, ISO 14229-1 has been updated, and a new UDS service, Authentication (Service ID 29), began in 2020.

E. Authentication by Service ID 29 "Authentication"

This new authentication service has the following advantages in terms of security compared with the previously used security access.

- Support for Public Key Infrastructure (PKI)-based authentication mechanisms.
- Support for session key exchange during authentication.
- User-privilege management support.

This service is expected to spread and be implemented into in-vehicle basic software, such as AUTOSAR (AUTomotive Open System ARchitecture). This will make it easier for vehicle manufacturers and component suppliers to implement higher security measures than ever before.

Some automotive ECUs, however, use processors with low processing power, such as 16-bit microprocessors. PKI-based authentication requires certificate parsing, hash calculation, and processing of asymmetric key cryptography, which cannot be afforded by such processors.

To introduce user-privilege management, it is necessary to properly construct and operate a system outside the vehicle that manages the privilege settings for each user and their expiration dates. For example, there is a need for special diagnostic communication during the vehicle-development phase and vehicle-production processes, and the introduction of Service ID 29 will not be effective unless account management for users and production facilities with such special privileges is properly implemented. Therefore, it is necessary to improve not only technical measures, such as the development of ECUs and privilege-management systems, but also the management and operation of the user management process at the same time.

III. CURRENT STATUS AND ISSUES OF REMOTE DIAGNOSIS

A. What is Remote Diagnostics?

Section II described wired diagnostic communication. Remote diagnosis refers to diagnostic communication using a wireless communication unit installed in the vehicle, enabling remote diagnosis from a location away from the vehicle. Figure 3 shows a typical configuration for remote diagnosis.

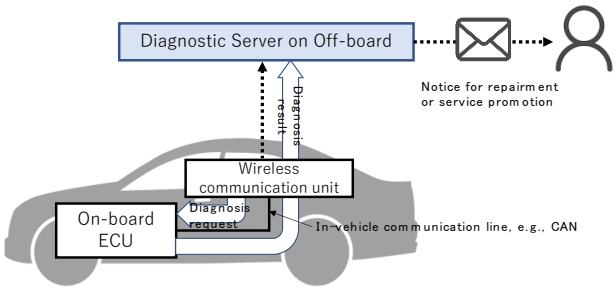

Figure 3. Example of remote diagnostic system.

In remote diagnosis, the wireless communication unit in the vehicle requests the onboard ECU to self-diagnose if any failures occur. The onboard ECU sends back the diagnosis results, which the wireless communication unit forwards to the remote diagnosis server, enabling the diagnosis results to be obtained without entering the vehicle.

If a malfunction occurs, the diagnostic server notifies the user and urges them to repair or go to a garage, preventing the malfunction from becoming a serious problem.

While it is technically possible for the wireless communication unit to transmit requests, such as program rewriting and Input-Output (IO) control, these requests are designed for use under the control of a mechanic only when the vehicle is stopped for maintenance or repair. If operated remotely and unintentionally by the driver while the vehicle is running, they may cause safety-related problems.

In a previous study [8], security measures for remote diagnostic systems were proposed. These measures are based on the assumption that the wireless communication unit (called the telematics module) is correctly installed in the vehicle and properly works. However, the vulnerability of the wireless communication unit can be exploited, making it an entry point for man-in-the-middle attacks through hijacking. This should be assumed as one of the major threats in recent automotive security risk analysis.

With current remote diagnostics, it is assumed that the wireless communication unit can be hijacked, thus the following risk mitigation measures were introduced.

- As illustrated in Figure 4, the communication path used for remote diagnosis and the OBD connector are kept separate by the gateway from the in-vehicle network. The gateway is responsible for forwarding only low-risk services, such as the reading of trouble codes and error log data, while any unauthorized

service requests are discarded. In other words, the gateway ensures that only authorized requests are processed and unauthorized ones are discarded.

- The secret keys required to unlock critical services of the ECU are not stored in the diagnostic tool or gateway to which the attacker can obtain physical access by purchasing them.
- The wireless communication unit is not equipped with a function to receive arbitrary diagnostic requests from an off-vehicle server but only push transmission of diagnostic results.
- The wireless communication unit should be able to transmit only predefined low-risk service requests, such as reading trouble codes.

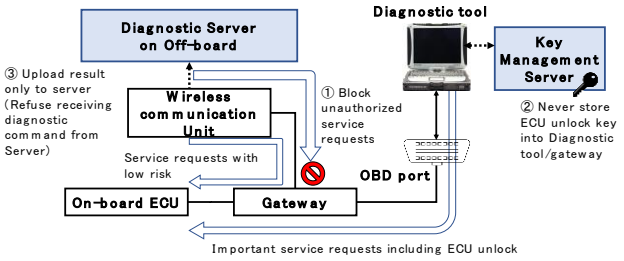

Figure 4. Example of conventional risk-mitigation measures.

B. *Service Expansion Requirements for Remote Diagnosis*

Contrary to the limitations imposed by the risk-mitigation measures described in Section III.A, the following use cases are required for remote diagnosis.

- Remote use of critical commands (e.g., IO control services listed in Section II.C) required for pre-diagnosis to identify parts to bring to a repair place of a vehicle that is stopped on the road due to a malfunction.
- Remote identification and handling of failure caused by senior mechanics (use case similar to telemedicine).

C. *Security Risks from Expansion of Remote Diagnostic Services*

When responding to the need for service expansion as described above, the abuse of critical diagnostic services increases the risk that safety will not be maintained, and fatal incidents will occur.

1) Expanding the impact of incident occurrence: The impact of abusing critical diagnostic services becomes significant because such services can manipulate or illegally modify safety-related vehicle components, for example, the braking or steering system.
2) Failure to confirm the vehicle owner's consent and safe vehicle conditions: Conventionally, the owner's consent could be indirectly obtained by receiving the vehicle key to physically access the OBD connector inside the vehicle. The repair operator had to ensure that the vehicle was in a safe condition, such as by locking the wheels. By allowing work to be done remotely, the above measures cannot be used.
3) Risk of abusing remote operation authority: Conventionally, the OBD connector cannot be accessed unless the vehicle is physically in the hands of the mechanic, so there is no need to worry about workers to whom the owner has entrusted repairs in the past without the owner's permission. Remote operations do not have these restrictions, increasing the risk of insider attack by privilege holders.

To address these risks, the following countermeasures will be necessary

- Countermeasure against risk 1): To prevent the unlocking of critical commands through external communication only requires a special in-vehicle operation to enable remote diagnostics as proof of the vehicle owner's consent.
- Countermeasure against risk 2): In addition to electronically authenticating permission from the vehicle owner, the vehicle receiving the remote diagnostic command also checks the physical condition, indicating that the vehicle is not running but awaiting servicing as one of the conditions for conducting remote diagnosis.
- Countermeasure against risk 3): When authenticating workers who conduct remote diagnosis, a mechanism to check whether the validity period of the work and the authority to carry out the work have been revoked is needed.

IV. PRPPOSED SECURITY-RISK-MITIGATION MEARURES

An overview of the remote diagnostic system operation is shown in Figure 5.

This system can execute remote diagnosis with the following procedure.

A. *Remote Operation Permission*

The vehicle owner who wants to solve a problem with the vehicle or a mechanic who receives a repair request by the owner first conducts owner authentication in the vehicle. The following permission methods are possible.

- The Human Machine Interface (HMI) in the vehicle (navigation-system screen, LCD of cluster meter, etc.) is used to authorize remote diagnosis. This can be done using a PIN or password preset by the vehicle owner to increase the reliability of the authentication.
- The presence of multiple intelligent keys in the vehicle is a condition for starting remote diagnosis permission. This is intended to detect differences from normal driving when only one key is present in the vehicle by the owner bringing a spare intelligent key into the vehicle.
- Pair the owner's smartphone with the vehicle and store the authentication information in the smartphone. The vehicle accepts remote diagnostics only for a certain period after successful Near Field Communication (NFC) authentication.

It is important to combine multiple conditions to increase the reliability of the remote diagnostic authorization described above.

B. Registration of Permitted Operations and Periods

Assuming that part of a vehicle component is malfunctioning, multiple input HMIs should be provided.

1) The owner's smartphone or operator's PC inputs the information and registers the operation information to be allowed to the remote diagnosis server and its validity period.

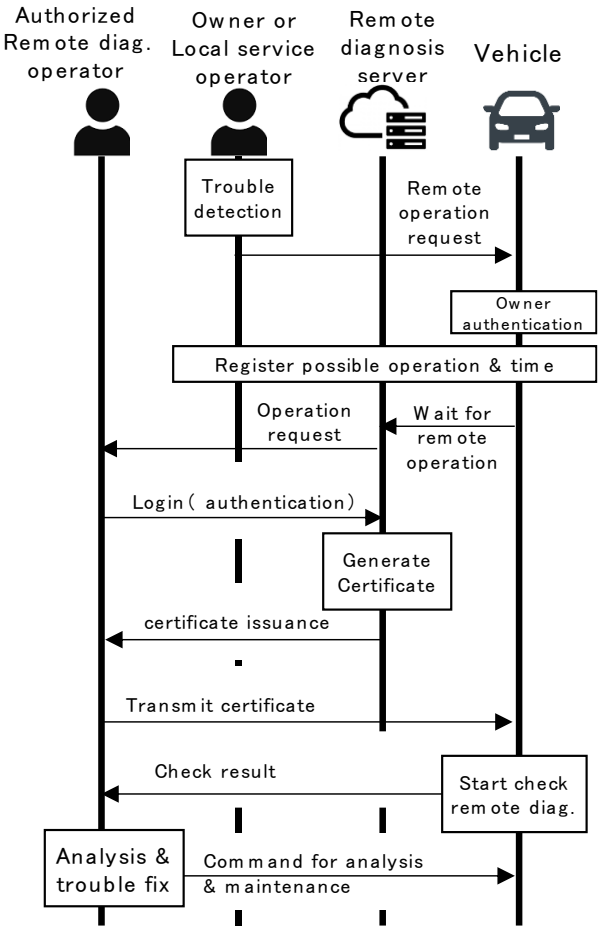

Figure 5. Overview of system operation.

2) Input the information on an HMI in the vehicle and register the operation information to be allowed to the remote diagnosis server via the vehicle's wireless communication unit.

The user can select which operations to allow by using HMI of vehicle infotainment system or Web site of Remote diagnosis server, for example, reprogramming firmware or resetting the ECU.

C. Requesting Analysis via the Diagnosis Server

The remote diagnosis server notifies the registered vehicle that the permitted operations and validity period of the work have been registered. At this time, the vehicle confirms that "permission for remote operation" has been granted in advance and that the vehicle is in a safe maintenance state (e.g., the vehicle is stopped, and the engine hood latch is open), and notifies the remote diagnosis server that it is "waiting for remote diagnosis". The notification data from the vehicle can be supplemented with the vehicle's location information obtained from GPS, etc., and a request can be made to the diagnosis server to limit the locations where remote diagnosis is permitted to the area around the current location. Upon receiving this notification, the remote diagnosis server sends a failure-analysis request to an appropriate operator from among the "authorized remote diagnosis holders" registered in advance.

It is also effective to include a one-time password in the failure-analysis request to increase the reliability of the certificate-issuance process in the next step.

D. Generating and Issuing Certificate of Remote Diagnostic Operations

When an authority holder receives the notification, they log into the remote diagnosis server and request the issuance of a working certificate. To enhance security, it is recommended to require the entry of a one-time password, which is sent only to the authority holder when they receive the notification of the analysis request, as a condition for issuing the certificate.

The issuance of this certificate is also sent to an HMI of the vehicle and the registered smartphone of the vehicle owner. If this notification indicates that a remote diagnostic request was not intended by the driver or vehicle owner in the vehicle, the "waiting for remote diagnosis" status of the vehicle can be canceled, or an instruction can be sent to the remote diagnosis server to stop remote operation for the vehicle in question as a risk-mitigation measure.

The remote diagnosis server issues a certificate to the authority holder as a token that records the expiration date and permitted operating privileges.

E. Access to Vehicles from Remote-diagnostic-authority Holders

The authority holder responsible for remote diagnosis sends a token to the target vehicle. The vehicle checks the token's signature using the remote diagnosis server's pre-shared public key, and if the token is issued by the legitimate remote diagnosis server and is still valid, the vehicle unlocks the remote diagnosis communication and authorized operation rights recorded on the token. The expiration date on the token prevents unauthorized access after the work is completed, which is not intended by the owner.

V. AVOIDING CONSTRAINTS WHEN IMPLEMENTING PROPOSED MEASURES IN VEHICLE COMPONENT

A. Implementation Constraints to Consider

The following are constraints in implementing the proposed measures in a vehicle.

- Automobiles are equipped with dozens of ECUs that execute diagnostic communications, and changing all these ECUs to components that implement security measures for remote diagnostics would require large-scale development and take too much time to implement.
- The resources required to adopt enhanced authentication algorithms, user rights management and expiry date management cannot be implemented in components with poor processors, such as 16-bit microcontrollers, which limits their applicability.
- Direct end-to-end communication between the off-vehicle server, which is the connection source for remote diagnosis, and the ECU to be diagnosed, creates a pathway for a direct attack on the ECU inside the vehicle from the off-vehicle server if a vulnerability exists in the ECU communication software, so a workaround is necessary.

B. Our measures to avoid constraints

We devised our security-risk-mitigation measures shown in Figure 6 to avoid the constraints described in Section V.A.

To reduce the security risk of remote diagnosis, these measures have the following features that the conventional measures shown in Figure 4 do not have.

1. The in-vehicle gateway is used as the master ECU to manage the remote diagnosis control.
2. The master ECU has a zone for communication with the external server via a wireless communication unit (Zone 1) and another zone for in-vehicle communication (Zone 2), which verifies certificate data for remote diagnosis and sends and receives diagnosis commands to and from multiple ECUs in the vehicle. Zones 1 and 2 are separated by hardware or software, such as a hypervisor, to prevent direct attacks from outside the vehicle to Zone 2, which executes in-vehicle communication processing.
3. Zone 1 of the master ECU communicates with the remote diagnosis server using Transport Layer Security (TLS) to prevent the in-vehicle wireless communication unit from eavesdropping on and falsifying communication data between the master ECU and remote diagnostic server (a countermeasure against man-in-the-middle attacks).
4. The master ECU boots with the remote diagnostics as locked status by default.
5. If the master ECU receives the result of the remote-diagnosis permission correctly executed with an HMI in the vehicle and the "remote diagnosis permission condition" is satisfied within a certain period after that, the master ECU unlocks the remote diagnosis process and enters the "waiting for remote diagnosis" state. The "remote-diagnosis-permission condition" is, for example, all the following conditions are satisfied.
   (1) Successful verification of certificate received from Zone 1.
   (2) The HMI executes remote diagnostic permission in the vehicle and is not canceled.
   (3) No timeout has occurred since the operation in (2).
   (4) The vehicle must be stopped.
   (5) Signals indicating that the vehicle is in a service condition (e.g., engine hood is open) are detected.
6. The target ECU for remote diagnosis connected to the master ECU operates by receiving diagnostic commands from the diagnostic communication process implemented in Zone 2. The master ECU executes the verification process of the certificate data and permission by the HMI, which are necessary as security measures of remote diagnosis, thus avoiding software and hardware changes in the target ECU.
7. Only when remote diagnosis is unlocked, the diagnostic communication process in Zone 2

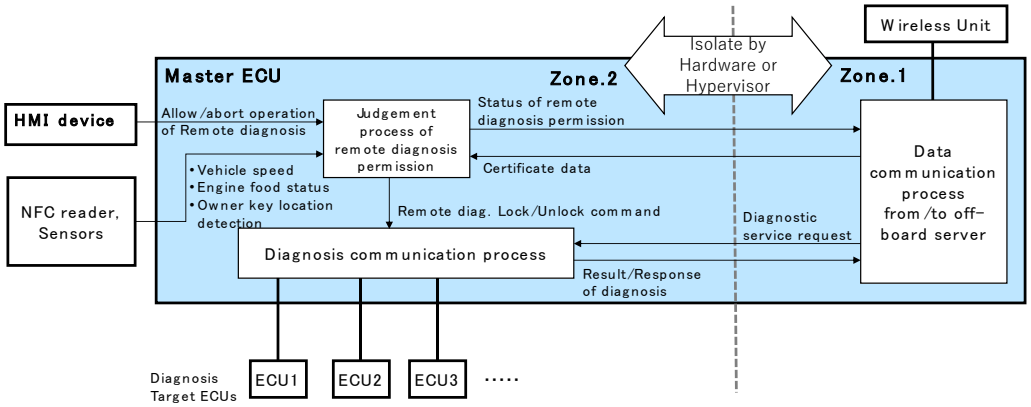

Figure 6. Implementation example using master ECU.

executes diagnostic communication in response to a remote-diagnostic-service request from Zone 1.

8. If the verification of certificate data fails more than once, the time until accepting the next verification is extended.
9. If a diagnostic-service request that is not authorized by the certificate is received, the diagnostic communication process returns a negative response. This history is stored in remote diagnosis sever. The request commands thus rejected are signed and included in the negative-response history data to prevent repudiation by the authorized remote diagnosis operator.

C. *Inspection of Decrease in Communication Speed due to Zone Separation*

To safely separate Zone 1, where communication with the outside of the vehicle takes place, from Zone 2, where important vehicle processing takes place, it is necessary to separate the processors and memory used by the master ECU for processing in each zone and to separate Zone 2 from Zone 1 by using the local network using a different local address from Zone 1. Therefore, a proxy process for address translation is required. The proxy must be implemented before each generic ECU receives data from Zone 1 and is required to relay various types of communications between Zones. Thus, communications that require strict realtime constraints, e.g., vehicle body control, must be properly treated even if other non-realtime communications, e.g., multimedia data, exist. We investigated whether the decrease in communication speed caused by this proxy process is acceptable. For this investigation, we conducted an experiment with the following processor for the master ECU.

Processor name: Renesas R-carS4N-8A
Implemented core:

- ✓ Real-time processor: ARM Cortex R52-1000MHz (1 core)
- ✓ Application processor: ARM Cortex A55-1200MHz (8 core)
- ✓ Microcontroller: RH850 G2MH-400MHz (2 core)

One of the above cores, A55, was allocated for proxy processing. The following cases were assumed for communication between Zones 1 and 2, which require the highest speed and lowest latency, and for the protocols used.

- ✓ Usage: Video transfer between Zone 1 navigation system and Zone 2 components (cluster meter or cameras)
- ✓ Protocol used: Real-time Transport Protocol (RTP)
- ✓ Target throughput 66 Mbps or more, latency 3 ms or less

The experiment was conducted in the environment shown in Figure 7, using 96-Mbps input data, which is higher than the target throughput.

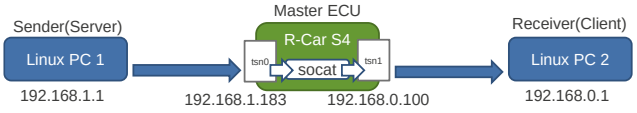

Figure 7. Experimental environment

The operating system used for both R-Car S4 and Linux PC1/PC2 was Ubuntu 20.04.

As shown in Figure 8, the proxy processing using “socat” could output 96-Mbps data without any data loss, and the CPU load at this time was only about 55%, leaving a margin.

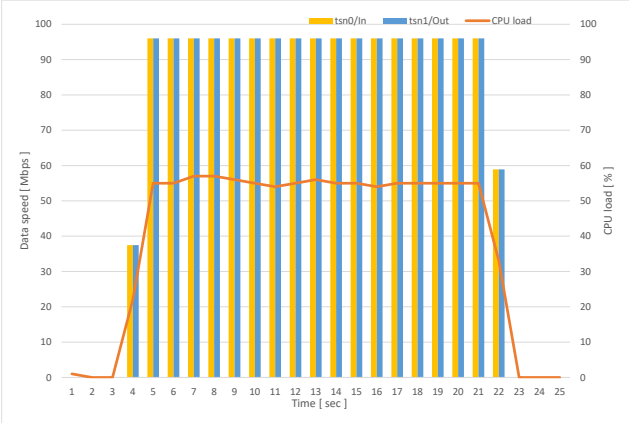

Figure 8. Performance of RTP proxy by socat.

The measured latency was 1.675 ms, achieving the target of less than 3 ms. These results confirm that a general ECU like Renesas R-carS4N-8A has sufficient processing power to function as a master ECU and show the feasibility of the proposed method.

VI. CONCLUSION

Even if a man-in-the-middle attack is carried out by in-vehicle wireless communication unit, our security-risk-mitigation measures can be effective in the following points.

- ✓ TLS communication between the remote diagnosis server in Zone 1.
- ✓ Even if an attacker can forge a certificate to conduct remote diagnostics, it is protected by multiple remote-diagnosis-permission conditions, such as vehicle-side remote-diagnostics-permission operations.
- ✓ To execute malicious code on the master ECU to bypass the remote-diagnostics-permission condition, it is necessary to break into Zone 2, but to do so from Zone 1, it is necessary to break through the separation between Zones 1 and 2.

The network separation between Zones 1 and 2 was a simple proxy using “socat”. Since the master ECU processor has sufficient processing power, we will investigate the possibility of enhancing security by, for example, adding an anomaly check for header information.

ACKNOWLEDGMENT

We thank Associate Prof. Hirokazu Hasegawa of NII for his warm advice throughout the research and Mr. Koji Yamada of Renesas Electronics Corporation for his cooperation in evaluating the performance of the master ECU.

REFERENCES

[1] C. Miller and C. Valasek, " Remote Exploitation of an Unaltered Passenger Vehicle", pp. 84–85, Blackhat Aug. 2015.

[2] H. Wen, Q. A. Chen and Z. Lin, "Plug-N-Pwned: Comprehensive Vulnerability Analysis of OBD-II Dongles as A NewOver-the-Air Attack Surface in Automotive IoT", pp. 960–961, Aug. 2020.

[3] S. Robert and J. S. Jayasudha, "Overview of Diagnostic over IP (DOIP), Ethernet Technology and Lightweight TCP/IP for Embedded System", International Journal of Advanced Research in Computer Science, pp. 296–299, 2013.

[4] R. B. Gujanatti, S. A. Urabinahatti and M. R. Hudagi, "Suvey on Security Aspects Related to DoIP", International Research Journal of Engineering and Technology, pp. 2350–2355, 2017.

[5] M. Matsubayashi et al., "Attacks Against UDS on DoIP by Exploiting Diagnostic Communications and Their Countermeasures", 2021 IEEE 93rd Vehicular Technology Conference, pp. 1922–1927, 2021.

[6] C. Miller and C. Valasek, "Remote Exploitation of an Unaltered Passenger Vehicle," in Blackhat USA. Las Vegas, NV, USA: Blackhat Press, pp. 86-88, 2015.

[7] S. Kulandaivel, "Revisiting remote attack kill-chains on modern invehicle networks," PhD thesis, Carnegie Mellon University, pp. 28, 2021.

[8] K. Daimi, "A Security Architecture for Remote Diagnosis of Vehicle Defects", The Thirteenth Advanced International Conference on Telecommunications, pp. 1-7, 2017.