Analysis of Performing Secure Remote Vehicle Diagnostics

Dennis Kengo Oka[1] Takahiro Furue[1] Stephanie Bayer[2]
Camille Vuillaume[1]

[1] ETAS K.K.
Queen's Tower C-17F, 2-3-5, Minatomirai, Nishi-ku, Yokohama, Kanagawa, 220-6217 Japan
{dennis-kengo.oka, fixed-term.Takahiro.Furue, Camille.Vuillaume}@etas.com

[2] ESCRYPT GmbH
Leopoldstr. 244, 80807 München, Germany
stephanie.bayer@escrypt.com

Abstract Traditionally, diagnostics of vehicles is done by plugging a physical device into a diagnostics interface in the vehicle; however, over the last years OEMs are considering to perform remote diagnostics. But connecting remotely to a vehicle opens a new entrypoint for attackers. Hence, it is important to secure the remote diagnostics procedure. We first provide an analysis of the security properties for remote diagnostics; this is done by giving a short overview over possible attacks. Next, we analyze and group diagnostic services and specify whether they are possible or suitable to be performed remotely. Last, we identify relevant security properties for each of the suitable diagnostic service groups.

1 Introduction

Modern vehicles are equipped with several dozen electronic control units (ECUs) that are responsible for the majority of functionality in a vehicle. ECUs often use sensor values as inputs which are processed by the ECUs software which in turn render outputs on actuators. For example, the airbag receives sensor values such as wheel speed, brake, impact, seat belt status and passenger position. Based on these sensor values, airbags situated on different places in the car can be inflated at different times at different rates to reduce the likelihood of injuries in crashes and decrease the likelihood of airbag-related injuries. Software is run on the ECUs to control such functionality. In addition, the software also monitors the vehicle or ECU conditions and can provide information regarding vehicle trouble. In such cases, diagnostic trouble codes (DTCs) are typically set on the corresponding ECUs. During vehicle maintenance, dealer workshops would then investigate the vehicle trouble based on the set DTCs, which are extracted using various diagnostics commands. It is important for OEMs to be able to perform this type of diagnostics to identify problems with software or vehicle components as well as calibrate and test functionality.

Currently, in case of vehicle trouble, vehicle owners typically need to bring their vehicle to a dealer workshop where a technician physically plugs an external test equipment tool (i.e., a diagnostics tool) into the OBD-II port in the vehicle. The technician can then send various diagnostic commands from the diagnostic tool which could be a standalone hardware tool or software running on a PC. The technician uses the diagnostic data extracted from the vehicle to analyze the problem. The solution to the problem could for example be a software update or replacement of a hardware component.

Unfortunately, there are a few issues with this approach. One, the technician can only start the analysis once the vehicle arrives at the dealer workshop, which leaves the technician little actual time to perform the analysis, prepare any spare parts that are necessary and perform any replacements or software updates. Second, the vehicle owner typically has to wait for the technician to finish the work before the vehicle is returned, which causes inconvenience for the vehicle owner. Third, OEMs can only collect information about vehicle troubles and other types of data once the vehicle arrives at the dealer workshop. The data extracted from the vehicle is uploaded to the OEM servers from the technician diagnostic tool. To remedy the issues with this approach, the trend is to perform *remote diagnostics*. Remote diagnostics allows reading out DTCs and other diagnostic data from vehicles remotely (using for example the telematics module equipped on vehicles). Consequently, it would address the three issues above respectively. One, the technician can perform part of the work prior to the vehicle even arriving at the dealer workshop. That is, the technician can first perform remote diagnostics to extract data necessary for the analysis and perform the analysis in advance. The technician can also prepare any necessary spare parts. When the vehicle is available at the dealer workshop, the technician can immediately start working based on the results of the analysis that has been made beforehand and replace any components using the prepared spare parts. Second, the wait time for the vehicle owner has been reduced to only the actual work needed to do the replacements or software updates, which means the happy vehicle owner will be back on the streets much faster. Third, OEMs can continuously collect diagnostic data which contain information about vehicle troubles and other types of data. This allows OEMs to analyze a larger set of data much sooner and would help in identifying any failure trends and in preparing to handle any large-scale vehicle trouble incidents as well as improving existing software with new features much quicker.

To allow remote diagnostics, security is necessary. For example, only authorized parties should be allowed to perform remote diagnostics. Moreover, some diagnostic commands may be considered too dangerous or not useful to perform remotely.

In this paper, we make the following contributions:

- We provide an analysis of the security properties for remote diagnostics.
- We analyze and group diagnostic services and specify whether they are possible or suitable to be performed remotely.
- We identify relevant security properties for the diagnostic service groups that are suitable to be performed remotely.

2 Remote Diagnostics Overview

In the following, we provide an overview of the remote diagnostics use case.

2.1 Definition of remote diagnostics

The term *remote diagnostics* may be interpreted differently by different people so first we provide a definition to ensure a common view of the use case.

Definition In the remote diagnostics use case, there is *no physical connection* between the diagnostics tool and the vehicle (i.e., communication between diagnostics tool and vehicle is wireless), and the technician has *no physical access* to the vehicle and *cannot perform any physical actions* on the vehicle.

2.2 Overview of remote diagnostics use case

An overview of the remote diagnostics use case is described as follows. Modern vehicles are equipped with telematics modules that connect the vehicles to the Internet. The telematics module also serves as a gateway between the Internet connection and the in-vehicle network (e.g., CAN bus). A diagnostics command is sent from the OEM server over the Internet and received in the target vehicle. The diagnostics command could have originated from an OEM technician (e.g., to perform data collection), or a dealer technician (e.g., to perform diagnostics on a vehicle prior to arriving at the workshop). The diagnostics command is transmitted on the relevant bus and processed by the target ECU in the vehicle. The result is returned via the telematics module to the OEM server. We consider the communication channel between the OEM technician/dealer technician and the OEM server to be secured using traditional IT security means.

The ISO 14229 [1] provides the standard for unified diagnostics services (UDS). The standard defines a number of diagnostics services where a diagnostic tool can control diagnostic functions in an ECU. For example, there are services such as changing the diagnostic session, resetting the ECU and reading or writing data to the ECU. Although the ISO 14229 standard also covers ECU programming, we have chosen to separate ECU programming from the remote diagnostics use case as it is very different from the rest of the diagnostics services and serves a different purpose (i.e., not used to diagnose a vehicle but rather to "fix" an issue by updating the software).

2.3 Attacker model

The attacker model in the remote diagnostics use case is defined as follows:

- The attacker can inject, modify or listen to any messages in the communication channel between the OEM server and telematics module on the vehicle.
- The attacker has physical access to the vehicle and can inject, modify or listen to any messages in the communication channel between the telematics module and the target ECUs.

As a result, rather than considering to point-to-point secure two separate communication channels (between OEM server and telematics module, and between telematics module and target ECUs), we only consider securing the end-to-end communication channel (between originator (OEM technician/dealer technician) and target ECUs). Although the focus is on securing the end-to-end communication channel, some messages in transit could be encapsulated in a lower-level protocol that may already provide some additional security features.

2.4 Security properties

We analyze the remote diagnostics use case and consider the following security properties desirable. A simplistic view of secure remote diagnostics would only consider to secure the communication channel between the OEM server and the telematics module because what happens between the telematics module and the target ECU is similar to the existing diagnostics use case today (between the ODB-II port and the target ECU). However, in this paper we consider securing the end-to-end communication channel and therefore consider the appropriate security properties for this channel.

2.4.1 Authenticity

One important security property is authenticity. It is paramount to ensure that a diagnostic message is actually coming from the

correct entity and has not been spoofed. That is, the receiving entity needs to be able to properly verify that a message comes from the claimed originator.

Researchers [2, 3, 4] have shown cases where they have broken the simple seed-key authentication that is implemented for diagnostic access in some vehicles. Even worse, some cases seem to be not employing any authentication at all or use fixed keys. Researchers have shown that they can execute arbitrary diagnostics commands to control the ECUs or read out the memory from the ECUs.

2.4.2 Integrity

Integrity is equally important as authenticity. It is imperative that messages that are sent between the communicating parties have not been modified while in transit. If messages can be modified, an attacker could modify requests sent from the OEM server to execute commands other than the intended ones or prevent a vehicle with vehicle trouble from going to a dealer workshop by modifying the trouble-indicating responses with responses that the vehicle is fine.

2.4.3 Confidentiality

There exist manufacturer specific diagnostic commands and responses which OEMs would prefer to keep secret. Moreover, some of the data collected from vehicles may contain sensitive information. Therefore, for such data there is a need to provide confidentiality in the communication channel. If an attacker is able to sniff the traffic, secret or sensitive data could be leaked; for example, secret diagnostics commands or data related to the privacy of the vehicle owner.

3 Analysis of Secure Remote Diagnostics

In this section we analyze and breakdown diagnostics services into groups and identify which are possible/suitable to perform remotely and which are not. We deem the groups that are not suitable to be performed remotely as *not allowed* to be performed remotely. We also identify the relevant security properties for each group that is suitable to be performed remotely.

3.1 Diagnostics breakdown

Common vehicle diagnostics tools provide a plethora of diagnostics capabilities [5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17]. We use these capabilities as a basis for our analysis. Different tool manufacturers and OEMs use slightly different terminology for the various diagnostics capabilities. Although terminology may be different, we believe that the respective capabilities can be assigned into one of the categories in our summary breakdown shown in Table 1.

First, we breakdown the diagnostics procedure itself into two categories: *Passive* and *Active*. The definition for passive is *no physical action on the vehicle by the technician is necessary*. Conversely, the definition for active is *requires physical action on the vehicle by the technician*. Physical action is defined as *physical input or physical inspection (e.g., visual)*. In no cases is the vehicle user required to be involved.

At the next level, there are three categories: *Read, Clear and Function test*. Read indicates any diagnostics that comprises reading data from an ECU. Clear represents clear DTCs. Function test covers all function tests.

The last level shows the individual groups of diagnostics which are further explained separately in below sections. The analysis and the

Table 1: Breakdown of diagnostics into groups

Diagnostics							
Passive						Active	
Read			Clear	Function test		Function test	
Datalist	DTC	Freezeframe	DTC	Inspection	Adjustment	Inspection	Adjustment

decision whether a diagnostics group is possible to be performed remotely is based on the actions required to perform the functions in the group. Moreover, some vehicles may require that a battery charger is connected to the vehicle or ensuring that the ignition key is in the on position with the engine off for some of the functions in the group to be executed. However, the purpose of this breakdown is to provide an *overview* of the groups and therefore does not go into all the details necessary for individual actions or tests within each group.

The results of the analysis are summarized in Table 2. For diagnostics groups that are not suitable (i.e., not allowed) to be performed remotely, no specific security properties are identified as they are not applicable (N/A).

3.1.1 Passive - Read datalist

This group is passive and consists of reading data from the ECU and displaying the values to a technician. These values are used to understand the current status or condition of the ECUs. Example values include vehicle speed, engine RPM, engine coolant temperature, open/close status of valves and gear position. Furthermore, reading law-mandated vehicle emission-related data (OBD-II PIDs) from the ECU is considered a subset of reading values from datalist, DTCs and freezeframes (DTCs and freezeframes described in the following subsections) and is therefore not considered as a separate group. Standard OBD-II PIDs are defined in SAE J1979 [18].

This group is both possible and suitable to perform remotely as it purely reads data from the ECUs and does not affect the function of the ECUs or require any active physical action by the technician.

This group requires the security properties authenticity and integrity and depending on the type of data that is read confidentiality may be required.

3.1.2 Passive - Read DTCs

This group is passive and consists of reading data from the ECU and displaying the values to a technician. The purpose of reading DTCs is to understand what could be "wrong" with a specific ECU or the vehicle and to assist in identifying the cause of vehicle trouble. Examples of DTCs are sensor circuit malfunction, injector circuit malfunction and cylinder 1 misfire detected.

This group is both possible and suitable to perform remotely as it purely reads data from the ECUs and does not affect the function of the ECUs or require any active physical action by the technician.

This group requires the security properties authenticity and integrity and depending on the type of data that is read confidentiality may be required.

3.1.3 Passive - Read freezeframe

This group is passive and consists of reading data from the ECU and displaying the values to a technician. When a fault occurs and a DTC is set, the ECU records the conditions

present when the fault occurred and stores it as a freezeframe. For example, the conditions recorded could include fuel system status, the coolant temperature and engine RPM. The freeze-frame data helps the technician to understand the conditions of the ECU when the DTC occurred to assist in troubleshooting the problem.

This group is both possible and suitable to perform remotely as it purely reads data from the ECUs and does not affect the function of the ECUs or require any active physical action by the technician.

This group requires the security properties authenticity and integrity and depending on the type of data that is read confidentiality may be required.

3.1.4 Passive - Clear DTCs

This group is passive but rather than reading data from the ECU it makes changes to the ECU by clearing or erasing DTCs that have been previously set. DTCs are typically cleared after the corresponding fault has been remedied by for example updating the software on the ECU or replacing the faulty component.

This group is possible to perform remotely although it does make changes to the ECUs, it does not require any active physical action by the technician (N.B. some vehicles may require that the ignition key is in the on position with the engine off). However, the clear DTC function is typically performed after the corresponding fault has been remedied and therefore may not be suitable to be performed remotely (unless the issue can be resolved and verified remotely).

This group requires the security properties authenticity and integrity. Assuming that the clear DTCs commands are not secret, confidentiality is not required.

3.1.5 Passive - Inspection function tests

This group is passive and includes function tests that are used for inspection. Typically this group includes tests that change a value which then can be inspected by checking the status or by reading a specific value. These tests could also be self-tests. For example, check or toggle valve open/close or perform solenoid test. This group is used for testing individual functionality by inspecting (i.e., reading a value) that the correct behavior is occurring.

This group is both possible and suitable to perform remotely although it does make changes to the ECUs, it does not require any active physical action by the technician. The inspection can be performed remotely by reading out the relevant data. N.B. there might exist some tests that require the vehicle to be in a certain state, e.g., vehicle speed 0 or gear in park. It is assumed that the vehicle will be in this state at some point naturally, and thus does not require any physical action.

This group requires the security properties authenticity and integrity. If the function test commands need to be kept secret, confidentiality is also required.

3.1.6 Passive - Adjustment function tests

This group is passive and consists of function tests that are used for adjustment and provide support for repair. This group would contain tests that allow reset and initialization of ECUs, or adjust certain parameters. For example, adjusting the height of head lights or adjusting the tire size would be considered passive adjustment tests.

This group is possible to perform remotely although it does make changes to the ECUs, it does not require any active physical action

by the technician. However, typically adjustment function tests would occur in conjunction with actual repair or replacement where physical access is necessary. Thus, it would technically be possible to perform these tests remotely but in practice it would not be suitable.

Since it is not suitable (i.e., not allowed) to execute the function tests in this group remotely, security properties for this group are not applicable.

3.1.7 Active - Inspection function tests

This group is active and consists of function tests that actively change something which a technician typically can physically inspect. Turning on/off the wipers or the hazard light, locking/unlocking the doors, and moving the power windows up and down are examples of active inspection function tests.

This group is not possible nor suitable to perform remotely because it requires physical inspection by the technician. It would be possible to execute the first half of the test which is for the vehicle to perform an action but the second half of the test requires a physical action in the sense of physical inspection.

Since it is not suitable (i.e., not allowed) to execute the function tests in this group remotely, security properties for this group are not applicable.

3.1.8 Active - Adjustment function tests

This group is active and includes function tests that are used for adjustment and provide support for repair. This group comprises tests that allow calibration of sensors, cameras or steering and as well as various learning tests. For example, an active adjustment function test would be the steering end learning where a technician physically has to turn the steering wheel from the center position to the very far left position and then back to the very far right position and finally back to the center position.

This group is not possible nor suitable to perform remotely as it requires active physical input by the technician. Moreover, typically adjustment function tests would occur in conjunction with actual repair where physical access is necessary anyway.

Since it is not suitable (i.e., not allowed) to execute the function tests in this group remotely, security properties for this group are not applicable.

4 Conclusion

As vehicle diagnostics was traditionally done over a cable (i.e., a wired connection), there was no need to separate or define diagnostics groups other than for the purpose of organizing the diagnostics functions to ease the technicians' job to perform the actual diagnostics. For example, to easily find the desired functions in the diagnostics tool, the functions are grouped and typically displayed under corresponding menus. However, in allowing remote diagnostics, there is an important need to define diagnostics into various groups with specific requirements. OEMs need to determine which diagnostics functions are allowed or suitable to be performed remotely. For the diagnostics groups that are allowed to be performed remotely, proper security requirements and solutions need to be implemented. As future work, we will investigate such requirements and suggest a suitable implementation option.

Secure remote diagnostics will provide OEMs with multiple new business models and will allow increasing the efficiency to diagnose faulty vehicles as well as reducing the waiting time for the vehicle owner.

Table 2: Summary of diagnostics groups and whether they are possible/suitable to be performed remotely and respective security properties

Group	Possible remotely	Suitable remotely	Security properties [1]		
			A	I	C
Passive - Read datalist	Yes	Yes	◯	◯	△
Passive - Read DTC	Yes	Yes	◯	◯	△
Passive - Read freezeframe	Yes	Yes	◯	◯	△
Passive - Clear DTC	Yes	Yes[2]	◯	◯	×
Passive - Inspection function tests	Yes	Yes	◯	◯	△
Passive - Adjustment function tests	Yes	No	N/A	N/A	N/A
Active - Inspection function tests	No	No	N/A	N/A	N/A
Active - Adjustment function tests	No	No	N/A	N/A	N/A

[1] A: Authenticity, I: Integrity, C: Confidentiality, ◯: Required, △: Required if transmitted data need to be kept secret, ×: Not required, N/A: Not applicable

[2] If issue can be resolved remotely yes, otherwise no.

References

[1] ISO 14229-1 Road vehicles - Unified diagnostic services (UDS) - Part 1: Specification and requirements, 2013.

[2] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage "Experimental Security Analysis of a Modern Automobile", IEEE Symposium on Security and Privacy, 2010.

[3] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno "Comprehensive Experimental Analyses of Automotive Attack Surfaces", USENIX conference on Security, 2011.

[4] Charlie Miller, Chris Valasek "Adventures in Automotive Networks and Control Units", DEFCON 21, 2013.

[5] Autologic Diagnostics "Autologic Software Technical Specifications for BMW Vehicles", 2013.

[6] Craftsman "CanOBD2 Diagnostic Tool Operator's Manual", 2008.

[7] Snap-on "Solus PRO User Manual", 2012.

[8] Innova Electronics Corp. "CanOBD2 ScanTool Owner's Manual", 2008.

[9] Gore Research "ProScan", 2006.

[10] Banzai "MST2000", 2014

[11] GIT "G-scan User Manual", 2012

[12] OTC "Genisys User Guide", 2005.

[13] SPX "Modular Vehicle Communication Interface (MVCI) User Guide", 2010.

[14] Ford Motor Company "Integrated Diagnostic Software User's Guide", 2008.

[15] EASE Diagnostics "EASE PC Scan Tool", 2012.

[16] Nissan TechNews "Consult III plus, CAN, ECU Programming", 2011.

[17] Motor "Scan Tool Assessment", 2005

[18] SAE J1979: E/E Diagnostic Test Modes, 2012.