SURVEY ON SECURITY ASPECTS RELATED TO DOIP

Rudrappa B Gujanatti[#1], **Sachin A *Urabinahatti***[#2], **Manjunath R Hudagi**[#3]

[#1]Assistant professor, Department of ECE, KLE Dr. MSSCET, VTU, Belgaum, India
[#2] Department Of CSE, TKIET-Warananagar,Maharashtra,India
[#3] Department Of CSE, TKIET-Warananagar,Maharashtra,India

***

Abstract— *In this paper, we have presented a security analysis and mechanism of delivering diagnostics services to the connected cars in connected repair shop or external test equipment. Next generation vehicles will provide powerful connectivity and telematics services, enabling many new applications of vehicle communication and here the diagnostics service is performed between diagnostic tool and vehicle remotely, which are separated by internet protocol. The performance of the Diagnostics have been done using brand specific protocol, but as a car is getting connected, IP based network is used while communicating with the vehicle. The document in ISO 13400 DIS (Draft International Standard), Diagnostics over IP describe a protocol for this type of interaction. As the number of electronic control units increasing in the automotive system its capability and functionality have also increased to large scale. Which demand extra connectivity with external networks. So, we see the overall security analysis of the interaction between connected car and the eternal test equipment*

Keywords— *DoIP, Automotive, Remote diagnostics, ECU, security.*

I. INTRODUCTION

Access to diagnostic data from Electronic Control Unit (ECU) in vehicles is of great importance in the automotive industry. The diagnostic over IP in TCP/IP means enables a connection between diagnostic tool and in-vehicle nodes using IP protocol. Here the vehicle is connected to repair shop by using Wi-Fi technology. So, It also raise the security related questions; how mechanic will come to know that he/she is working with the right vehicle. So, there are some security mechanisms, protective measures have defined. As more and more of crucial car functionality is managed by software rather than hardware, the complexity of software increases. Unfortunately , this often leads to vulnerability, especially as testing all possible attack scenarios.

A trend over past few years has been to start equipping vehicles with capabilities enabling the diagnostic services to be carried out remotely. So, the analysis related to the security issues that arise from the fact that DoIP runs over TCP/I network and the new range of safety related problems to address.

II. METHODOLOGY

This chapter discusses about the threads of the attacks on the vehicle and the security mechanism. The module describes what are the possible actions an attacker might take are. So, To ensure the continuous operation of safety critical systems within the car, the vehicle along with its communication has to be protected. Therefore this work consists of a security analysis of a DoIP system.

A. *Attacker capability and resources*

The method of the attacker is divided into two separate classes, active and passive. A passive attacker simply earwig on communication without disturbing or altering it in anyway. An active attacker on the other hand participates in the communication during the attacks. This activity might consist of modifying or intercepting messages being sent, or possibly deleting them, or injecting new messages into the stream.

1) *DoIP Communication scenarios:*

- Direct physical connection between one vehicle and an external tool:

It was assumed that direct communication over a single cable cannot be eavesdropped or affected in any way. Since, the test equipment will be directly connected to a vehicle through a physical Ethernet connection. There will be no conflict between any other test equipment and other vehicle attacks originating from the external test equipment are considered to be out of the scope of this work, that only leaves attacks coming from the vehicle in this one-to-one connection. That is, the attacker legally connects to the tester which it then tries to attack.
Potential attacks (attack vector -> target):
Vehicle -> Tester

- Networked connection between one vehicle and an external test equipment:

It has one major difference that the communication travels over a potentially insecure medium where an attacker may operate freely. It has opportunity from the previous scenario and which are still available, but the possibilities are thus extended with deletion, injection, eavesdropping and manipulation of transmissions as well. An attacker can then use this vector in order to attack both a vehicle and a tester. In this Scenario a set of vehicles will be connected to a network (ie. repair workshop network) where the test equipment can select the vehicle to be connected with at a particular instance. The vehicle should also be able to identify the test equipment and should be able to reject multiple connections from other test equipment in the network.

Potential attacks (attack vector -> target):
Vehicle -> Tester
Communication link -> Tester
Communication link -> Vehicle

- Networked connection between multiple vehicles and one external test tool:

In this scenario, Here the external test equipment should be capable of supporting multiple communications. The test equipment will be connected to multiple vehicles whereas the vehicles will be only able to support a single test equipment. The connection is made through socket connections. So. There is a possibility of multiple cars existing in the system and is added simultaneously. The case might thus be that one of the cars is controlled by an attacker, while the others are not. The extension to the previous scenario is then logically that an attacker in control of a vehicle can attack another (potentially bouncing attacks off the tester in the process).

Potential attacks (attack vector -> target):
Vehicle -> Vehicle
Vehicle -> Tester
Communication link -> Vehicle
Communication link -> Tester

- Networked connection between one vehicle and multiple test tools or test applications on a single physical tool :

This setup is a slightly more advanced version, Here the vehicle will be able to support multiple connections to connected test equipment. In such scenario vehicle shall be able to identify diagnostic messages from different instance of test equipment. It is assumed that the testers are secured in the sense that an attacker is not in control of one of them, therefore the issues added are not as visible as that of the previous sub-section. Here, an attacker in control of the vehicle might however attempt to abuse the relation between the different external test equipment.

Potential attacks (attack vector -> target):
Vehicle -> Tester
Communication link -> Tester
Communication link -> Vehicle

2) *Resources of attacker*

Modern cars are controlled by complex distributed computer systems comprising millions of lines of code executing on tens of heterogeneous processors with rich connectivity provided by internal networks (e.g., CAN). While this structure has offered significant benefits to efficiency, safety and cost, it has also created the opportunity for new attacks. For example, We have demonstrated in previous work that a car's internal network is connected by an attacker can circumvent all computer control systems, including safety critical elements such as the brakes and engine.

B. *Security requirements*

High popularity of Ethernet and DoIP standards in vehicle industries have speeded the implementation of remote access and remote diagnostics in vehicles. This Remote diagnostics and remote access of vehicle information leads to a set of safety related problems. Safety can be normally said based on two scenarios; safety for normal operation and safety for a system that is under influence of one or several system faults. Normal safety generally helps in building a system which will be safe with respect to usage normal scenarios. Functional safety involves increasing highly fault tolerant and high scalable and reliable system. As a part of normal safety even if the skilled technicians try to access the system information, only the diagnostic information have to be communicated back to remote tester if the proper authentication is provided to the vehicle by tester and access, analysis of diagnostic data can only be performed also Network connectivity and its attack have to be considered. While in functional safety an generalized analysis of the system fault have to be done instead of looking at specific ECU's or actuators.

TABLE I: LIST OF SECURITY ATTRIBUTES

Attributes
Data origin authenticity
Integrity
Controlled access
Freshness
Non- Repudiation
Privacy/anonymity
Confidentiality
Availability

1) *Data origin authenticity:*

This property ensures that the source of a message is verifiable. The receiver of a DoIP message should in other words be able to authenticate that the claimed source is actually from where the communication came.

Applicability to DoIP in the specified system:
When fulfilled, this data origin authenticity will make sure that the vehicle can verify that diagnostic requests come from a trusted external test equipment, and the tester can in turn be asserted that it indeed gets responses from the vehicle it seeks to communicate with. Therefore, On the behalf of vehicle responses are not made by another entity.
Possible implications if the security attribute is not fully upheld:
If not fulfilled, a user with malicious intent could pretend to be an authorized party in order to have potentially dangerous commands accepted by a receiving entity.

2) *Integrity:*

When satisfied, the integrity property guarantees that a message has not been altered, maliciously or by random chance (failures or physical effects), in transit. That is, the data received is identical to the data sent.
Applicability to DoIP in the specified system:
The integrity attribute ensures that an unauthorized party cannot modify commands or data being sent in the DoIP messages.
Possible implications if the security attribute is not fully upheld:
Modifications could for example mean that an attacker intercepts a message and exchanges a contained command for another. It also allows an attacker to alter software being transmitted. Also, the scenario described under data origin authenticity might thus also occur if integrity is not guaranteed.

3) *Controlled access (authorization):*

This property describes how different entities are allowed to access resources.
Applicability to DoIP in the specified system:
Authorization can be used to make sure that only legitimate external test equipment is allowed to be perform diagnostics on a vehicle.
Possible implications if the security attribute is not fully upheld:
There is an obvious danger in the ability to execute diagnostic commands on a vehicle.

4) *Freshness:*

The freshness property is satisfied if information received is always current. That is, a message received from a previously transmitted piece of information is not be copied again.
Applicability to DoIP in the specified system:
In the specified setting this property entails that a previously sent legitimate diagnostic request cannot be re-transmitted as is.
Possible implications if the security attribute is not fully upheld:
A command that is not dangerous in given a certain scenario, that might be potentially lethal in another. Say that a workshop mechanic sends a diagnostic command to start a routine that releases the brakes of a car in order to test their functionality. But, if vehicle is receiving the previous send message then it is dangerous to the vehicle.

5) *Non-repudiation:*

Non-repudiation is an attribute which requires that an entity having performed an action cannot claim that it did not. i.e, actions can be traced and proven to have been performed by certain entities.
Applicability to DoIP in the specified system:
If damage to vehicle, passengers or surroundings arise as the result of one or several diagnostic messages the origin of said communication can be proven. This is useful in order to uphold legal accountability.
Possible implications if the security attribute is not fully upheld:
[1]Non-repudiation does not help in preventing incidents from happening. First, it carried out ease of the forensic and then work in identifies the source of an attack.

6) *Privacy/anonymity:*

Privacy is a property assuring that information about a certain entity stays confidential. Anonymity is a special case of privacy which refers to the confidentiality of the identity of an entity.
Applicability to DoIP in the specified system:
In a diagnostics system this property makes sure that information about a vehicle and its owner is not available to unauthorized parties.
Possible implications if the security attribute is not fully upheld:
The potential issues very much depends upon what kind of information that is stored in and which is accessible from the vehicle. If sensitive data, such as credit card information or related details, is stored and accessible through diagnostics the consequences might be serious. Information about the state of the car which is stored is probably not very useful for the most of the attacker, but such issues might be considered in extreme cases.

7) *Confidentiality:*

The property of confidentiality is a broader and more general concept of secrecy than privacy. This requirement pertains to the secrecy of all information transmitted, regardless of whether it can be connected to a specific entity or not.
Applicability to DoIP in the specified system:

The contents of the commands and data being sent are seen by a malicious user and can use this information in order to view the potential problems related to the car. This could possibly later be used in order to launch an attack.
Applicability to DoIP in the specified system:
The information that fails to obey this property would be problem to human being to keep the information secret.

8) *Availability:*

Availability is a property that is satisfied as long as the service being investigated is functioning. That is, as long as the service is available.
Applicability to DoIP in the specified system:
The availability requirement is satisfied in the specified DoIP system as long as the diagnostic messages sent reach their intended targets which also process and answer the transmissions in accordance with the draft standard.
Possible implications if the security attribute is not fully upheld:
Due to the Breaking of the availability property will lead to dangerous effects and annoyances, but disruption of diagnostic services is not endanger to human life, vehicle, or surroundings. It might however cause harm to the brand of the service provider.

C. *Security in DoIP*

This section describes security issues in the DoIP protocol itself. That is, the problems that are inherited from technologies used by the protocol are stem from the specifications present in the draft documents. The analysis contains references to the different requirements which is specified as [DoIP-xxx], tables and state machines of the technical documentation in the draft standard. Even though the assessment of this section can be considered to be self-contained, it is recommended to read it together with the DoIP draft documents as this analysis would be overly verbose if each requirement was to be fully explained before its weaknesses and strengths are investigated.

1) *DoIP header handling:*

This section describes issues, protective measures and mechanism related to the standard header of DoIP messages.

TABLE II: DoIP HEADER FIELDS

Items	Starting position(byte)	Length(byte)
Protocol version	0	1
Inverse protocol version	1	1
Payload type	2	2
Payload length	4	4

The DoIP header fields are shown in Table1. Each DoIP message has a special DoIP header which is prepended to it. Major security issue found in DoIP header handling is the weak integrity check (in DoIP-041) which in turn results in unauthorized modification.
DoIP header field provides the protection against: Magnification attack: Here the attackers now take advantage of weaknesses in the protocols to magnify the impact of their floods by an order of magnitude.
NACK storms: massive amounts of negative acknowledgement (NACK) traffic from the network. NACK storms can plague(affect) any reliable one-to-many communications system.

Fingerprinting:

Fuzzing: is an automated software testing technique that involves providing invalid, unexpected, or random data as inputs to a computer program.
Buffer flow: In computer security and programming, a buffer overflow is where a programmer writing data to a buffer(region of a physical memory storage used to temporarily store data while it is being moved from one place to another.). when it overruns the buffer's boundary and overwrites adjacent memory locations.

The above mentioned attacks are protected by Ignore unwanted packets, NACK policy(It is a signal used in digital communications to ensure that data is received with a minimum of errors.), Message discarding policy(A message (or a frame) is a group of consecutive packets. Often a loss of one packet from the message can result in the loss of the whole message. Selective message discarding policies have been proposed as a means for congestion avoidance.), Input validation(Input Validation is the correct testing for of any input that is supplied by something else. All applications require some type of user input. User input could come from a variety of sources, This stands to reason that all input should be checked and validated). Weak data integrity check provides Unauthorized modification potential result.

Which are given bye the references present into the DoIP draft documents such as, [DoIP-031], [DoIP-39], [DoIP-041] and so on. which defines that the DoIP entity upon reception of a transmission should perform a check against the Payload length field to see if acceptance of the message would cause the currently available DoIP protocol handler memory to be exceeded.

2) *Vehicle announcement/identification :*

This section discusses topics related to the vehicle announcement/identification phase of the DoIP protocol. The phase consists of either a Vehicle identification request followed by a Vehicle identification response.

The Vehicle identification request field does not contain any data related to request send. There are two variants to the payload. These are Vehicle identification request message with EID and Vehicle identification request message with VIN. There is a six-byte EID and a 17-byte VIN respectively and these variants are thus used when a tester wants to reach an entity with a specific EID or a vehicle with a specific VIN.

TABLE III
VEHICLE ANNOUNCEMENT MESSAGE PAYLOAD / VEHICLE IDENTIFICATION RESPONSE MESSAGE PAYLOAD

Item	Starting position (byte)	Length (bytes)
VIN	0	17
Logical address	17	2
EID	19	6
GID	25	6
Further action required	31	1
VIN/GID sync status	32	1

The data contained in the response, shown in Table 9, are all fields describing the DoIP entity that is either announcing its presence or responding to a previous request.

Vehicle announcement/identification provides the protection against:

DoS (denial-of-service): A denial-of-service attack (DoS attack) is a cyber-attack where a malicious user seeks the network resource and unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet.

Spoofing: Spoofing refers tricking or deceiving computer systems or other computer users. This is typically done by hiding one's identity or faking the identity of another user on the Internet.

The above attack can be avoided by Limiting the number of transmissions and Limiting the concurrency of transmissions. Which are provided by the references present into the DoIP draft document such as [DoIP-50], [DoIP-51] etc.

The amount of Vehicle announcement messages sent out should be limited. It also defines the minimum delay that should pass between each consecutive Vehicle announcement request/response. From the point of congestion perspective this is a nice feature. It provides the random delay between the reception of a Vehicle identification request and the sending of the corresponding response. Due to this randomness it is very much hard for an attacker to perform a coordinated distributed denial of service attack.

3) *Routing activation :*

The routing activation phase is carried out to enable routing of its messages via a DoIP gateway and on to the internal vehicular network.

TABLE IV
ROUTING ACTIVATION REQUEST MESSAGE PAYLOAD

Item	Starting position (byte)	Length (bytes)
Logical address	0	2
Activation type	2	2
[Reserved for future use]	4	4
[Reserved for OEM-specific use]	8	4

The fields of the Routing activation request message are shown in Table 4. The logical address is the address of the source of the message.

Routing activation provides the protection against:

Unauthorized access: Unauthorized access is the use of a computer or network without permission. A hacker is someone who tries to access a computer resource or network illegally. However, others can use or steal computer resources or try to corrupt a computer's data.

Access from unknown addresses and Attacks taking advantage of disclosed information: Here the access will be taken from the unknown address.

Also by fingerprinting, fuzzing

The issue of spoofing is prevalent in this phase as well. An attacker could try to modify the logical addresses of messages or simply create new transmissions containing false information.

Specification ambiguity: Which defines unclear portions in any specifications. As Software requirement specification need to be precise and accurate, to be self consistent.

The above attacks are overcome by Access control and Handling of unexpected values.

Routing activation phase of the DoIP protocol may also contains various security problems. The routing activation phase is actually needed when a tester wants to enable routing of messages through a DoIP gateway and subsequently to its internal vehicular network. Various security issues analyzed in routing activation phase are, lack of authentication, information disclosure and specification ambiguity which results in Spoofing, attacks taking advantage of disclosed information and fingerprinting respectively. As a part of routing activation handling the socket handling is also performed in parallel.

The above security measures are given into the references like [DoIP-059], [DoIP-062], [DoIP-63] and so on.

4) Socket handling:

The socket handling is performed as part of the routing activation handling. There is some confusion about the socket definition used in diagnosis, something which can lead to implementation of specific security issues. A socket handling is defined to be identified by the source and destination IP addresses along with ports and the transport layer protocol used for communication with the socket.

Socket handling provides the protection against:
Resource exhaustion: These attacks are computer security exploits that crash, hang, or otherwise interfere with the targeted program or system. They are a form of denial-of-service attack. Which involve overwhelming a network host with requests from many locations.
Along with this unauthorized access, fingerprinting and Static resource allocation.

III. CONCLUSIONS

[1] DoIP, is not secure to use without extra control mechanisms in an arbitrary environment. That is the most general conclusion that can be drawn from the results of this work.[1] If DoIP is to be used over public media, such as either over the Internet or over wireless links, the protective measures which have explained earlier need to be applied in order to fulfill the requirements stated in this report and thus guarantee the correct operation of safety-critical systems.

The stream of thought behind the security surrounding the protocol is hard to pin down. All kinds of protective measures been completely left out, and the natural conclusion would have been done by the authors is a mission of the protocol to be keep secure. So, There are some mechanisms defined in the draft documents. These are however not nearly enough to provide a proper security for a system where incorrect operation can lead to the endangerment of human life.

DoIP has been constructed by including the mechanism that offers full security only in certain operating environments, for example while using a direct cabled connection. In such a scenario the authentication mechanism in the routing activation might be enough as the connection is broken and the socket has to be registered and authenticated all over if a cable is pulled out. So, It would then explain about why the authentication and confirmation operations are only present for routing activation and not for the other phases. If this is the issue that is under some specific conditions the security is provided, then it need to be clearly stated in the final standard to avoid confusion.

REFERENCES

[1] Security Analysis of Vehicle Diagnostics using DoIP, Master of Science Thesis in the Programme Networks and Distributed Systems by Chalmers University of Technology, Department of Computer Science and Engineering, May 2011.

[2] Mathias Johanson ,Alkit Communications AB ,Mölndal, Sweden, Pål Dahle ,Volvo Car Corporation Gothenburg, Sweden, Andreas Söderberg ,SP Technical Research Institute of Sweden ,Borås, Sweden, Remote Vehicle Diagnostics over the Internet using the DoIP Protocol.

[3] Ajin V W Lekshmy, D Kumar, James , Study of security and effectiveness of DoIP in vehicle networks, Joy,2016, International Conference on Circuit, Power and Computing Technologies [ICCPCT].