KU LEUVEN

FACULTEIT INGENIEURSWETENSCHAPPEN

OBD–II Access Control

Michiel Willems

Thesis voorgedragen tot het behalen van de graad van Master of Science in de ingenieurswetenschappen: computerwetenschappen, hoofdoptie Veilige software

Promotor:
Prof. dr. Bruno Crispo

Begeleiders:
Mahmoud Ammar
Hassan Janjua

Academiejaar 2018 – 2019

Contents

List of Figures and Tables

List of Figures

List of Tables

List of Abbreviations and Symbols

Abbreviations

ACK	Acknowledgement
AK	Authenticated Key Agreement
AKC	Authenticated Key Agreement with key Conformation
AI	Artificial Intelligence
API	Application Programming Interface
CAN	Controller Area Network
CAR	California Air Resources Board
CHAP	Challenge-Handshake Authentication Protocol
CLC	Cyclic Redundancy Check
CPU	Central Processing Unit
DAC	Discretionary Access Control
DLC	Data Link Connector
DLC	Date Length Code
DoS	Denial of Service
DTC	Diagnostic Trouble Code
ENISA	European Union Agency For Network And Information Security
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDHE	Ephemeral Elliptic Curve Diffie-Hellman
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECDSA	Elliptic Curve Digital Signature algorithm
ECU	Electronic Control Unit
EOF	End Of Frame
HMAC	Hash-Based Message Authentication code
Hz	Hertz
ID	Identifier
IDE	Identifier Extension Bit
ITS	Intelligent Transportation Systems
LIDAR	Light Detection And Ranging
LIN	Local Interconnect Network
MAC	Mandatory Acces Control
MAC	Message Authentication Code
MOST	Media Oriented Systems Transport
PATS	Passive Anti-Theft System
RAM	Random Access Memory
RBAC	Role-Based Access Control
RKE	Remote Keyless Entry

Chapter 1

Introduction

1.1 Motivation

The automotive industry is rapidly evolving over the years, since the introduction of the Ford Model T in 1917. Although the main purpose of these machines remains the same (e.g. getting someone from point A to B swiftly), the relative comfort, speed, safety, and efficiency has been improved dramatically. Primarily due to the introduction of electronic computers into the vehicle's architecture. The modern vehicle has been appropriately called a "Computer on wheels" [14], since each one contains up to 100 millions lines of code, spread out over tens of Electronic Control Units (ECUs) [22]. Each ECU is an embedded computer that is designed to perform a specific function (e.g. braking, opening the door, speed control, etc.). In addition to having this wide variety of embedded devices, a modern vehicle will also employ a data bus that allows all ECU's inside a vehicle to communicate with each other. There are multiple standards that are employed even within a single vehicle, but the CAN (Controller Area Network) protocol is the most widely used one [29], Hence we focus on it in this paper.

Alongside internal communication networks, many modern models of vehicles also support some way of performing external communications. This can range from vehicle-to-infrastructure (V2I) (e.g. wireless gas payment at a gas station, wireless diagnostics at a repair shop or even virtual traffic lights), vehicle-to-vehicle communications (V2V) (e.g. automatically following another vehicle), vehicle-to-network (V2N) (connecting your vehicle to an already existing network, like the cellular communications network for example) and vehicle-to-pedestrian (V2P) [13][25][3]. All of the extended functionality introduced greatly improves the vehicle's flexibility, comfort and safety. This however also makes them increasingly vulnerable to a wide variety of cyber attacks through the various interfaces that can communicate with the external world, exemplified by abusing remote keyless entry (RKE) systems to gain access to a car [10][17], remotely causing a vehicle to think it is having a tire problem by interfering with the tire pressure monitoring system (TPMS) [17] or

even compromising a vehicle through the Bluetooth interface [15][8]. The On-board Diagnostics (OBD-II) port is one of the potential attack vectors. OBD-II systems are widely deployed in auto-mobiles as a way of getting diagnostics information from the vehicle. OBD-II introduces a physical interface into the vehicle (usually under the steering wheel) called the Data Link Connector (DLC). This physical interface allows full access to the internal network. It has been repeatedly shown [17][37][18][16] that a set of messages or signals could be injected on a car's CAN bus to control key components (e.g. lights, locks, brakes, and engine) as well as injecting code into key ECUs. The focus of this thesis will be to try and mitigate this kind of illegal access by introducing access control to the OBD-II interface.

1.2 Challenges

The main challenge of this research topic is to introduce a solution that ports well to the kind of hardware that is found in modern vehicles. Introducing new components into the internal vehicle network would surely simplify things (if this were the case the solution could consist of introducing a small component that acts as a firewall for the OBD-II interface). However this implies that any potential real-world implementation requires the installation of this component into millions of currently in-use vehicles, which (being a very costly endeavour) would deter any manufacturers from doing so. Therefore, a software-based approach is required. It is easy to deploy such a solution on the currently in-use cars without any hardware modification or excessive expenses. However, This approach introduces it's own challenges, namely the limitations of ECU micro controllers. Indeed, any solution that isn't portable to the network (because of memory limitations, limited processing power, incompatible architectures, etc.) is rendered useless. It is worth noting that the solution proposed here is not intended to (and will not) protect against attacks using other attack vectors (e.g. TPMS, Bluetooth, etc.) as well as physical attacks. Indeed any attacker gaining physical access to the vehicle has to ability to directly interface with the vehicle network (e.g. by physically tapping into the CAN bus). Typically only the owner of the vehicle has this privilege, and it is safe to assume this person is reluctant to compromise the safety of his or her own vehicle. unauthorised physical access should be mitigated by different means (e.g. car alarms, safe RKE systems, the authorities, etc.). The main challenges of this thesis paper are summarized as follows:

- **portability:** The solution should port well to existing vehicle networks.
- **Security:** The solution should be sufficiently secure according to current computer safety standards.
- **Speed:** The solution should not impede the operation of other processes running on the same network.

1.3 Context

As mentioned before, the goal of this paper is to secure the OBD-II interface in modern cars. Before we move on it is interesting to take a look at some other issues regarding internal vehicle networks, as well as some proposed solutions to these problems. Aside from the OBD-II interface there are numerous points of entry to the internal vehicle network, both physical (Breaking into the vehicle and directly connecting to the network) or remote (Bluetooth, TPMS or Tire Pressure Monitoring System, Radio system, etc.) [17]. Take Bluetooth for example: many cars include Bluetooth functionality to allow users to connect their phones and play music. The Bluetooth protocol has a large protocol-stack and has been known to have problems in the past [17] like discoverability, bluejacking, bluesnarfing and backdoor attacks [9]. By exploiting the vulnerabilities of a car's Bluetooth interface, a malicious agent is able to interfere with the internal network remotely (using his/her mobile phone). Another problem is that it is easy for a phone to get compromised (visiting a malicious website) [37]. This problem would be solved by using a more secure version that does not contain the aforementioned vulnerabilities.

Another approach is to secure the protocol that is used for communication within the network. As mentioned before, the CAN protocol is probably the most popular one since almost every new passenger car manufactured in Europe is equipped with at least one CAN network [11]. CAN in itself is a simple bus protocol that allows nodes on a network to send and receive messages. However CAN is a low-level protocol and does not natively support any security features. A number of secure CAN variations have been proposed: Leia [23], VatiCAN [29], VulCAN [19] and CANopen [21].

1.4 Contributions

The contribution of this thesis can be summarized as follows:

- Overcoming the security limitation identified by the unauthorised access to the vehicle CAN network via the OBD-II port by designing and developing a role-based access control model based on public key cryptography.
- Advancing the security of OBD-II ports by bringing it closer to reality through a proper implementation on CAN-enabled resource-constrained ECU that is used in various automotive models. Furthermore, we evaluate and show that our approach is secure, feasible and lightweight in terms of memory footprint and runtime overhead.

Chapter 2

Background

> "Today, CAN has established itself worldwide as the backbone for the networking of embedded systems, and this not only in automotive technology"
>
> Dr. Siegfried Dais, Prof. Dr. Uwe Kiencke, Martin Litschel

2.1 Intra Vehicle Networks

Today's automobiles contain a series of different electronic components networked together to be responsible for monitoring and controlling the state of the vehicle. Each component can communicate with all other components on the same sub-network. The safety of the vehicle relies on near real time communication between these various ECUs. While communicating with each other, ECU's are responsible for predicting crashes, detecting skids, performing anti-lock braking (ABS), etc. [37]. There are only a couple of operations that are performed without using computer control (with the parking brake and steering being the last holdouts) [8].

2.1.1 Sub-Networks

In most real architectures a series of domains are defined that correspond to different features of the car, often corresponding to dedicated sub-networks (i.e. Powertrain Control Module) within a single vehicle. The European Union Agency For Network And Information Security (ENISA) distinguishes between 6 different domains[1], as is illustrated in figure 2.1.1. These are:

- **Powertrain Control Module (PCM):** Consists of engine control Units that control a set of actuators on the internal combustion engine, as well as transmission control units that change the gears to ensure optimal engine performance.

- **Chassis Control:** Ensures control of the vehicle with regard to it's surroundings (e.g. steering, airbag, braking, etc.)
- **Body Control:** Compromises all ECU's that perform functions within the context of the passenger's compartment and/or trunk (e.g. dashboard, doors, windows and seatbelt, etc.).
- **Infotainment Control:** This domain includes navigational services (i.e. GPS), communications (i.e. Cellular) and entertainment (i.e. Radio).
- **Communications Control:** Unlike all previous modules this one does not compromise a single sub-network but rather a series of communication features offered by a telematics control unit (e.g. Wifi).
- **Diagnostic and Maintenance systems** This concerns all the various diagnostics and maintenance solutions that can be connected to the OBD-II port.

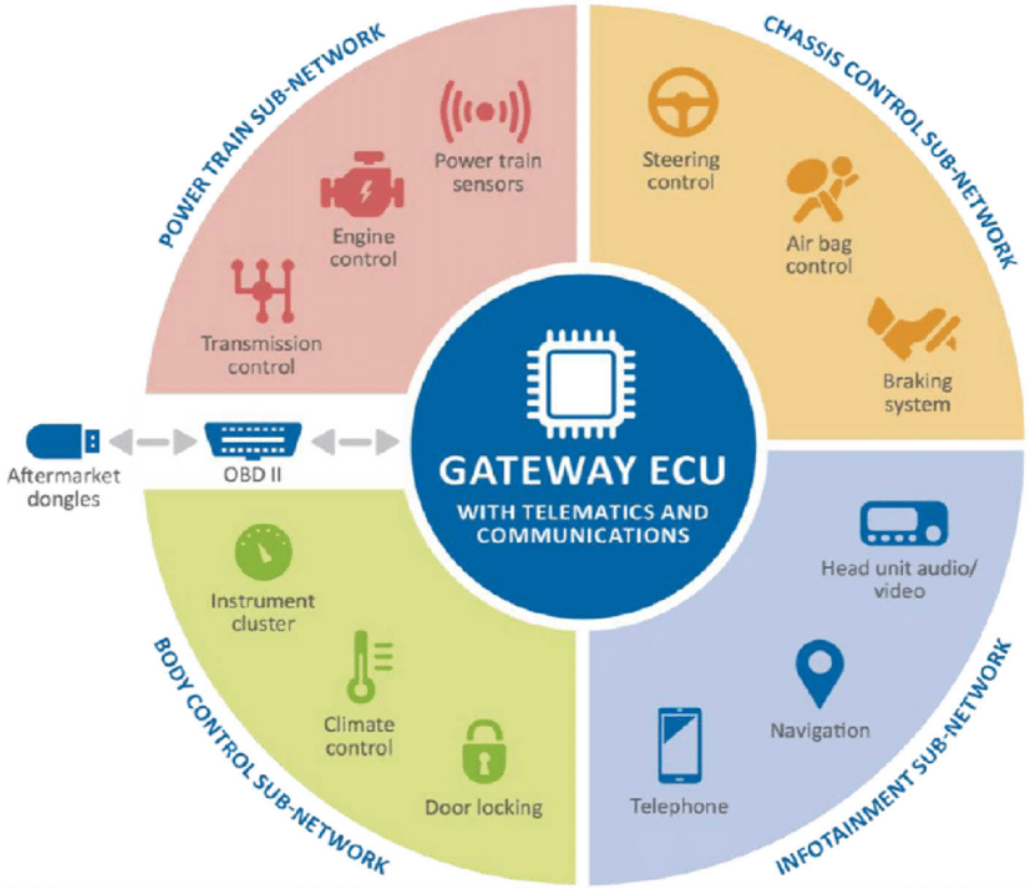

Figure 2.1: Typical intra vehicle network infrastructure [1]

On top of their functional differences, these sub-networks often implement different network communications protocols. This means that there are multiple communication standards that are employed even within a single vehicle. The most common ones are: Controller Area Network (CAN), Local Interconnect Network (LIN), Media Oriented Systems Transport (MOST), FlexRay and LVDS[28]. Each of these protocols specifies how messages are exchanged within the appropriate sub-network and are chosen to best service the needs of a specific domain, as is illustrated in figure 2.1.1 and 2.1.1.

Protocol	Bitrate	Medium	Protocol
LIN	19.2 Kbps	Single Wire	Serial
CAN	1 Mbps	Twisted Pair	CSMA/CR
FlexRay	20 Mbps	Twisted Pair/Optical Fibre	TDMA
MOST	150 Mbps	Optical Fibre	TDMA
LVDS	655 Mbps	Twisted Pair	Serial/Parallel

FIGURE 2.2: An overview of different network technologies and their characteristics [28].

A critical component in these types of networks (the presence of sub-networks with different communication protocols) is the Gateway ECU. This component performs a frame or signal mapping function between two communication systems, thereby allowing ECU's on different sub-networks using distinct communication protocols to exchange messages nonetheless. On top of acting as an intermediate between the different sub-networks of the vehicle, the Gateway also acts as an entry point for OBD-II messages. Any message sent via the OBD-II DLC will be translated and forwarded by the Gateway to the appropriate sub-network. It comes as no surprise that this component will play a crucial role when introducing access control to the OBD-II interface.

2.1.2 Example: ABS

Let's take a closer look at ABS to get a sense of how the intra vehicle network operates. ABS was designed to keep the wheels from locking up during braking. It consists of 3 main components: wheel speed sensors, a pump and a controller. Here's how it works[30]:

- The controller monitors the wheel speed sensors constantly (So each speed sensor periodically sends a message to the Controller).
- The controller will recognize a wheel locking whenever it detects a rapid deceleration.

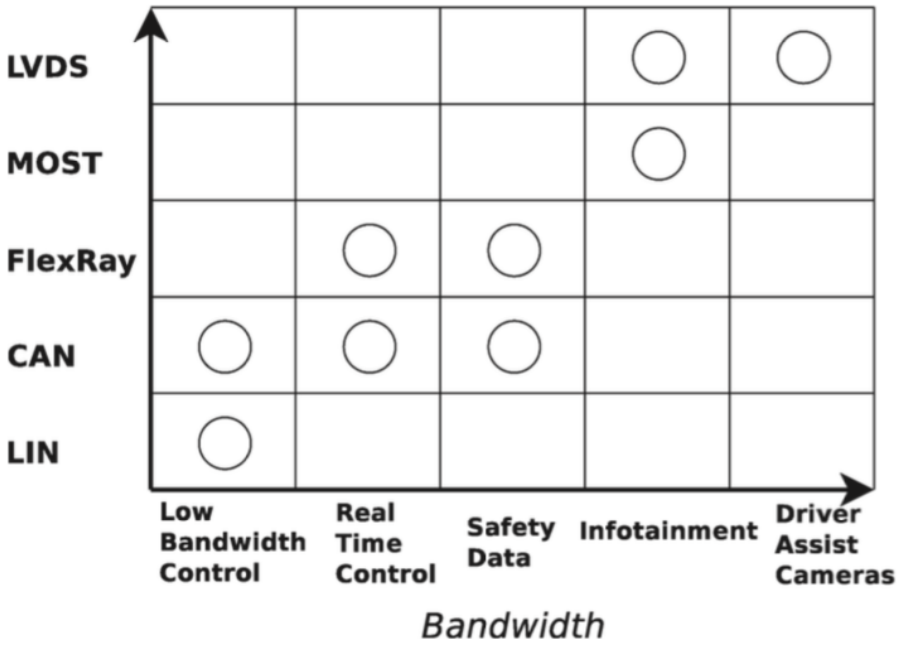

Figure 2.3: Mapping of traffic types to network technologies [28].

- Whenever it does detect a wheel locking up, it will use the pump (again by sending a message over the network) to regulate the pressure on the brake of that particular wheel, thereby keeping it from locking up.

2.2 CAN

The CAN protocol has become a ubiquitous part of the automotive industry. In the context of internal vehicle networks, CAN messages have multiple purposes: First, there are informative messages that are designed to transmit data from and to ECU's (e.g. the Anti-Lock System (ABS) broadcasting the speed of each wheel). Second, there are action messages that are designed to request another ECU to perform an action (e.g. adaptive Cruise Control (ACC) module requesting the brakes to be applied). Third, there are the diagnostic messages defined by the OBD-II protocol. [18] Naturally the last type of message is the focus of this paper. The following paragraphs are dedicated to the CAN protocol.

2.2.1 Brief History

The history of CAN starts in 1983 when a couple of engineers at Bosch (soon aided by engineers from Mercedes-Benz and Intel) start developing a new serial bus system for use in the automobile industry. It wasn't long before CAN was officially introduced

at the SAE congress in Detroit as: 'Automotive Serial Controller Area Network'. The main characteristics of this protocol were:

- An arbitration method that allows bus access to the message with the highest priority without delays.
- No master CAN node that is in charge of the bus.
- Transmitted messages are identified by their content, not by their destination or origin.
- This identification also determines the priority of the message within the network.

It didn't take long before the first CAN controller chips were developed in 1987 (by Intel and Philips respectively) and the first official CAN specifications were standardised in the 90's, effectively paving the way for the CAN protocol to become an industry staple as it is today. To this day Bosh has been making sure that all CAN chips comply with their proposed standards in order to avoid incompatible implementations. [1].

2.2.2 Architecture

A typical CAN network consists of a series of nodes (with a minimal of 2 in order for the network to be functional) connected by a two-wire bus. It is important to note that there are 2 physical CAN specifications: high speed CAN (see [12]) and low speed (or fault tolerant) CAN (see [2]). Every CAN node consists of:

- CPU: effectively the 'brain' of the node, deciding what messages are sent and taking the appropriate course of action whenever a message is received.
- Controller: in charge of reading and writing bits to and from the CAN bus.
- Transceiver: acts as in an intermediate between the bus and the controller, thereby translating between different signal levels.

This architecture specifies the minimum requirements of a CAN node. More often than not these nodes will include other components (e.g. sensors, actuators) that are connected to the CPU. It should be clear from this specification that this architecture applies to any common vehicle network (e.g. ECU's act as CAN nodes).

2.2.3 CAN Frames

Since CAN is a message based protocol, it facilitates communication by transmitting short bursts of data called CAN frames. There are four different types of CAN frames:

[1] For a comprehensive history of the CAN protocol confer [11]

name	size (bits)	purpose
start-of-frame	1	Denote start of transmission
identifier (ID)	11	Unique identifier + determines priority
remote transmission request (RTR)	1	must be 1 for remote frames
identifier extension bit (IDE)	1	must be 1 for extended frames
reserved bit	1	reserved for future use
data length code (DLC)	4	length of data field
data field	64	data to be transmitted
cyclic redundancy check (CLC)	15	check for errors [2]
CRC delimiter	1	must be 1
acknowledgement slot (ACK)	1	used for message acknowledgement
ACK delimiter	1	must be 1
end-of-frame (EOF)	7	must be 1

Table 2.1: base frame format [32]

- Data frame: used to transmit data with a specific identifier.
- Remote frame: used to request the transmission of data with a specific identifier.
- Error frame: transmitted whenever a node detects an error on the bus.
- Overload frame: transmitted by a node to include a delay between data or remote frame.

There are 2 frame formats: base frame format and the extended frame format. The only difference being that the extended frame format uses a 29 identifier bits and the base frame format only uses 11. Table 2.1 lists all the fields of a base format data frame. The extended frame format is the same except for an additional identifier field (18 bits) right after the identifier extension bit (IDE) field.

2.2.4 Data Transmission

The operation of the CAN protocol is pretty straightforward: a node transmits a message with a specific ID on the bus. Any node that is connected to the same bus is able to receive the message (broadcast), but only the nodes that are listening for this specific ID will take action. It is worth noting that the ID is used to identify the content, not the sender or receiver. As a matter of fact CAN does not provide any way of authenticating the sender or receiver, which results in various security related difficulties (see **??**) . Aside from identifying the content, this ID is also used to solve the issue of message arbitration. CAN is a carrier sense multiple access protocol, whereby each nodes observes the bus before transmitting data on it, if it detects that

[2] A cyclic redundancy check is a way of detecting accidental changes to transmitted data (e.g. due to noise, interference, etc). For more information on cyclic redundancy checking see [33].

the bus is in use it waits for some time before trying again. This does not prevent nodes from starting a data transfer at the same time, this is where bit wise message arbitration provides a solution. [4].

2.2.5 Message Arbitration

Whenever 2 (or more) nodes initiate a transmission on the bus at the same time, bit wise message arbitration is performed. Every bit of the message ID can be either 1 or 0. The CAN specifications use the term dominant (logical 0) and recessive (logical 1). These terms originate from the fact that whenever more than one bit is simultaneously written to the bus, and one of these is dominant, the dominant bit 'wins', meaning a logical 0 will be seen on the bus. Whenever a node transmits a logical 1 but sees a logical 0, it realizes that there is a contention and re-queues its message for later transmission. Since the identifier is transmitted at the start of the CAN frame, the node with the numerically lowest identifier transmits more zeros at the start of the frame, and that is the node that wins the arbitration. Concisely put we can say that messages with lower ID's have priority over messages with higher ID's. The decision to identify messages by their content (instead of their sender or receiver) is motivated by the fact that certain very important types of messages (e.g. errors) can be given a very low id, thereby ensuring they are less prone to be delayed. This approach does introduce some issues when it comes to security (see **??**).

2.2.6 Layering

In line with most networking protocols, it is common practice to decompose them into different abstract layers. This is done to simplify the design and make modularisation easier [36]. In the case of CAN the layers are:

- **Application layer:** OBD-II, CANOpen, VulCAN etc.
- **Object layer:** message filtering and status handling.
- **Transfer layer:** error detection, message arbitration, bit timing, etc.
- **Physical layer:** signal voltages, pin-out configuration, etc.

2.2.7 Security Issues

The CAN protocol has a number of inherent vulnerabilities that are common to any implementation. The most obvious and important ones are:

- **Broadcast nature:** CAN frames are both physically and logically (no destination address) broadcasted on the network. This means that a malicious node on the bus can snoop on all communications or even worse: send packets to any other node on the network [8].

- **No authentication:** CAN frames do not have source identifier fields, so there is no way for any node to be aware of the source of any messages it receives. This means that any compromised component (or any other form of unsanctioned access to the CAN bus for that matter) can inject arbitrary messages. Whereas the system has no way of knowing these messages were not sent by the appropriate component [8][6].
- **No encryption:** We've mentioned that speed and timing are deemed more important to the safety and performance of the vehicle than data security. A clear result of this is the decision to omit any encryption capabilities. This is because the limited computational power of ECU's makes it difficult to implement robust cryptographic algorithms. [6].
- **Susceptibility to Denial of Service (DoS):** This problem arises mainly from the protocol's message arbitration method. Any malicious node can effectively spam the bus with high priority messages (only zeroes as ID) causing all other nodes to back off (no protection against "babbling idiots"[22])[8].
- **Not Byzantine fault tolerant:** In most distributed systems, malicious attacks and software errors can cause a node to exhibit Byzantine (i.e. arbitrary) behaviour[7]. Because of the distributed nature of any CAN system, there is imperfect information on whether a component has failed (or has been compromised by attack) or not. This could result in situations where entire system services fail since a common consensus cannot be reached[31]. [3].

For more information on the CAN protocol see [12] and [2].

2.3 OBD-II

2.3.1 Design Goals

OBD-II (On Board Diagnostics) is a specification that was introduced to allow for self diagnostic and reporting functionality for ECU's inside a vehicle, and has been mandatory in every car produced in the united states since 1996. [35]. It allows users (testers, developers, repairmen, etc) to query ECU's about diagnostics information in order to perform a detailed analysis of the vehicles internal systems. Specifically the goals of OBD-II upon introduction were:

- Standardisation: information is communicated in a standardized format to allow for 1 tool to be used on many vehicles.
- Certification: Every vehicle manufacturer required to submit certification application for review and approval, which includes a detailed description of how the OBD-II protocol was implemented.
- Help lowering emissions by identifying emission controls in need of repair.

[3] For more information on Byzantine faults, and how it is tolerated in a system see [7] and [31].

The system can also be very useful in a number of other situations: A repairman looking for a specific component that is to be repaired, an employee at the factory testing all components before the vehicle is ready to be sold, a policeman analysing a vehicle after a crash to determine what caused the accident, a software developer testing the operation of a newly developed ECU, etc.

2.3.2 Brief History

There were a lot of different proprietary diagnostics systems introduced over the years, before a standard arrived with the introduction of OBD-II. This brief history cited from [27] does a decent job of concisely explaining how OBD-II came to be:

> The origins of OBD-II actually date back to 1982 in California, when the California Air Resources Board (ARB) began developing regulations that would require all vehicles sold in that state starting in 1988 to have an onboard diagnostic system to detect emission failures. The original onboard diagnostic system (which has since become known as OBD-I) was relatively simple and only monitored the oxygen sensor, exhaust gas circulation system, fuel delivery system and engine control module.
>
> OBD-I was a step in the right direction, but lacked any requirement for standardization between different makes and models of vehicles. You still had to have different adapters to work on different vehicles, and some systems could only be accessed with costly "dealer" scan tools. So when ARB set about to develop standards for the current OBDII system, standardization was a priority: a standardized 16-pin data link connector (DLC) with specific pins assigned specific functions, standardized electronic protocols, standardized diagnostic trouble codes (DTCs), and standardized terminology.
>
> Another limitation of OBD-I was that it couldn't detect certain kinds of problems such as a dead catalytic converter or one that had been removed. Nor could it detect ignition misfires or evaporative emission problems. Furthermore, OBD-I systems would only illuminate the MIL light after a failure had occurred. It had no way of monitoring progressive deterioration of emissions-related components. So it became apparent that a more sophisticated system would be required. The California Air Resources Board eventually developed standards for the next generation OBD system, which were proposed in 1989 and became known as OBD-II. The new standards required a phase-in starting in 1994. The auto makers were given until the 1996 model year to complete the phase-in for their California vehicles.
>
> Similar standards were incorporated into the federal Clean Air Act in 1990 which also required all 49-state vehicles to be OBD-II equipped by 1996 – with one loophole. The OBD-II systems would not have to be

fully compliant until 1999. So some 1996 OBD-II systems may lack one of the features normally required to meet the OBD-II specs, such as the evaporative emissions purge test.

2.3.3 DLC

In order to allow a user to communicate with the vehicle's internal network, OBD-II introduces the data link connector (DLC). The DLC is a 16-pin hardware interface (although only 9 pins are specified by the standard) that is generally found close to the steering wheel (by law it is required to be installed within 0.61 m of the steering wheel) [35]. There are 2 basic types of connectors: Type A as seen in figure 2.3.3 (using a 12V power supply) and Type B as seen in figure 2.3.3 (using a 24V power supply). the design of the two connector types prevents the insertion of a type A male plug into a type B female socket.

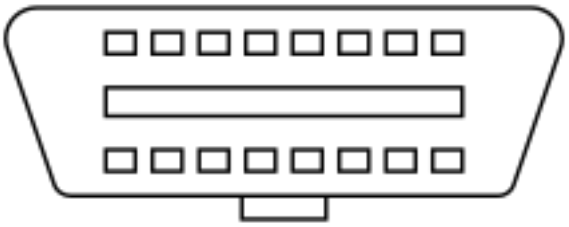

Figure 2.4: Type A female connector [35]

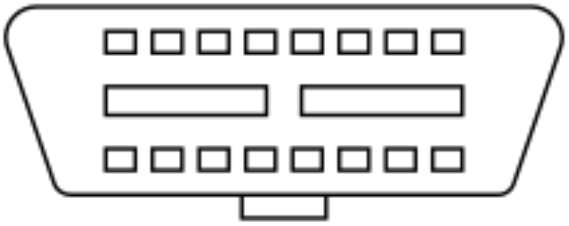

Figure 2.5: Type B female connector [35]

2.3.4 PID's

OBD-II introduces parameter PID's, which are codes used to identify and query specific data. The protocol is designed to work with multiple signalling protocols (the messaging protocol that is used to request and receive data from the network) but the CAN protocol is mostly implemented (Since 2008 all new vehicles sold in the us implement this signalling protocol[26]).

There are multiple ways for a user to interact with this interface:

- Standard Diagnostic scanning tool: a dedicated device that consists of a small hand-held module (equipped with a small screen and some buttons) connected to a male DLC-connector (The DLC inside the vehicle is always female).
- An advanced Diagnostic scanning tool that includes a DLC-connector with wifi/Bluetooth compatibility, allowing for remote diagnostics using a smartphone.
- A DLC-connector with a usb adapter allowing access via dedicated software on a pc. Since 2014 all new cars in the US support the SAE J2534 "PassThru" standard, which is a Windows API (Application Programming Interface) that provides a standard way to communicate with a car's internal buses [8].[4]
- A data logger, which is designed to capture real-time data while the vehicle is in operation.

Typically the ODB-II is used like this (CAN as signalling protocol): First, the user enters the PID of the data he/she wants to query into a diagnostic tool. Second, this data is packaged in a CAN frame and sent on the CAN-bus. Third, the ECU that is responsible for the data identified by the PID in the message recognizes it as it's own, and transmits a CAN frame containing the requested data. Fourth, the diagnostic tool recognizes the response and displays the data to the user [34]. Aside from this, the OBD-II port can then be used to upgrade the ECU's firmware or to perform a myriad of diagnostic tasks.

2.3.5 Security Issues

It is a well-known fact that the automotive industry has always considered safety a critical engineering concern (especially since the public awareness around lethal accidents has only increased over the years). Unfortunately it is unclear whether developers (especially concerning the internal network) have considered the security in their design. However it seems this is not the case because of three reasons. First, there is no inherent support for addressing, encryption or authentication [18]. Second, most of the networks and ECU's were designed when access to the bus required physical access to the vehicle, therefore security was not a primary concern. Third, speed and timing are deemed more important to the safety and performance of the vehicle than data security [14]. This vulnerability is worsened by the fact that the attack surface for modern automobiles is growing swiftly as more sophisticated services and communications features are incorporated into vehicles [8]. The OBD-II specification is one of these since the interface it introduces provides direct access to the internal vehicle network. This allows malicious agents to easily construct and insert CAN messages to alter the vehicle's behaviour, as has been frequently demonstrated by Charlie Miller and Chris Valasek's exploits [17][18][16]. The goal of this research paper is to design a solution that prevents malicious agents from

[4] For more information on SAE J2534, see the full API reference at: https://tunertools.com/prodimages/DrewTech/Manuals/PassThru_API-1.pdf

mounting attacks via the OBD-II interface, while still allowing for the system (i.e. performing diagnostics and maintenance) to function properly. This problem will be more suitably defined in the next chapter, where the problem statement is presented.

Chapter 3

Problem Statement

From the discussion in chapter 3 it follows that the use of CAN as signalling protocol for performing OBD-II operations, thereby inheriting all of CAN's security related shortcomings, attributes to a system that is inherently insecure. This chapter serves as a description of the security related problems that arise from the OBD-II specification, as well as providing a series of examples illustrating these problems.

3.1 Current State

Figure 3.1 shows the typical topography of the OBD-II system. The user interacts with the intra vehicle network via the OBD-II interface using some computerised device (see section 2.3.4). The central gateway receives and interprets all messages issued by this device, before forwarding them to the appropriate sub-networks. Optionally, upon reception by the intended ECU, a response could be issued and forwarded back to the user. All of this happens concurrently with the normal operation of the intra vehicle network, i.e. messages are exchanged by ECU's over the entire intra vehicle network to guarantee the optimal operation of the vehicle. The problem of this system is the indiscriminate nature at which the gateway forwards the messages it receives from the OBD-II interface. It does not discern between a normal message and a potentially harmful one. This results in an interface that is rendered wide open to any message that the gateway understands. While in theory, it was designed solely for diagnostic and maintenance purposes. This discrepancy between the intention of the OBD-II design and the wide open nature of it's implementation is apparent. As a result of this, the OBD-II interface can be used to mount a series of attacks. To get a sense of the scope, difficulty and impact of these attacks, a couple of real examples are discussed next.

3.1.1 Example attacks

The exploits that are presented here were performed by Charlie Miller and Chris Valasek, in an effort to raise awareness about the issue, as well as allowing car manufacturers to build safer cars in the future. They accomplished this by not only

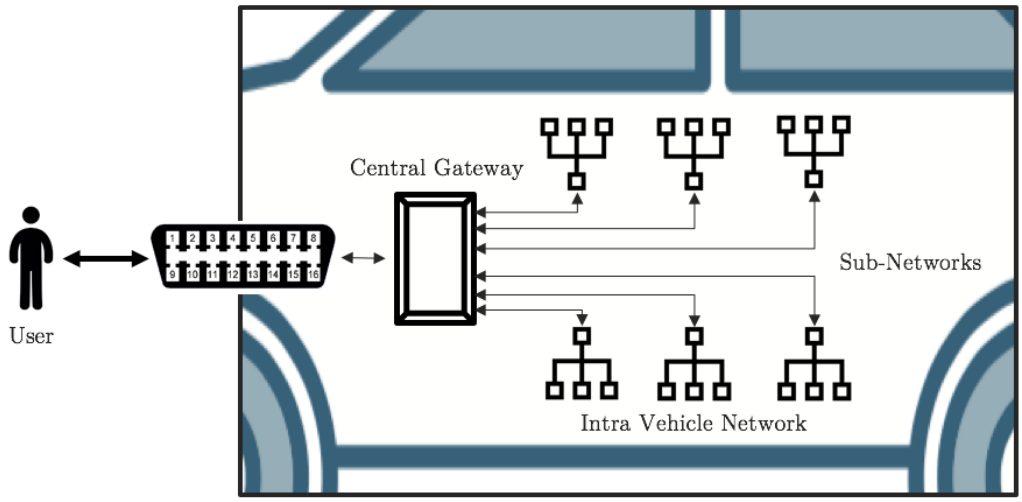

Figure 3.1: OBD-II System Topography

finding and exploiting various vulnerabilities in extant vehicles, but also sharing any software that made these exploits possible. An example of this is EcomCat, which is software written to aid in the reading and writing of data to the CAN bus through one or more Ecom cables [16]. The Ecom cable is then used to connect a laptop to the OBD-II DLC, allowing the researchers to use their EcomCat software to inject their own CAN messages onto the internal bus. Although seemingly straightforward there are many potential problems in attempting to make the vehicle perform actions by injecting packets on the CAN bus. First, not everything can be controlled via the CAN bus (e.g. cruise control). Second, if a specific type of CAN packet is found to be a request (An ECU asking for another ECU to perform an action) replaying a fake copy does not guarantee that the message is accepted. This is because the original message is still sent, possibly confusing the ECU with conflicting information. Third, It is also possible that fake messages are ignored because of built-in security features inside the ECU. Despite these difficulties, these researchers did manage to mount a series of interesting exploits, two of which are presented here.

Speedometer

In this example ,performed on a 2010 Toyota Prius, the researchers managed to identify the messages that are sent to the speedometer to display the current velocity of the vehicle. Replaying this message with custom data fields allowed them to display any arbitrary speed on the speedometer display.

Denial of Service

Here the researches cleverly take advantage of how the CAN protocol works. Remember from 2.2 that CAN uses priority scheduling over the ID's of the messages

that are sent on the bus. This means that spamming a high priority message would prevent all other messages from being transmitted. This vulnerability is exploited here by flooding the bus with CAN messages with an ID of 0. This flooding of the CAN bus halts the engine from being turned on, as well as putting the system in an all out state of disarray.

Diagnostic session

The aforementioned examples used injection of messages that are normally sent from ECU to ECU, thereby erroneously invoking certain actions. Another approach is to trick the vehicle network into starting a diagnostic session. These are used in normal circumstances by a technician at a garage. It allows them to test the function of an ECU without having to take the vehicle on the road, as well as recalibrating them. Starting a diagnostic session does require circumventing an authentication procedure (see **??**) but this proved rather easy (they did this by reverse engineering an official authentication device and extracting the keys). Once a diagnostic session was established it opened up a wide array of possible attacks: Killing the engine, disabling the brakes, honking the horn, unlocking/locking doors, and even reprogramming of certain ECU's (see [16] for a detailed description of the attacks).

3.1.2 Impact

It is clear that the level of control that is obtainable via the OBD-II port is worrying. Especially if we consider that there exist OBD-II devices with Bluetooth or Wifi capabilities, allowing attacks to be mounted from a distance (imagine a DoS attack being mounted while driving a car at high speed). It is these scenarios that elevate the concern from mere vehicular integrity, to concern over the physical safety of the driver and his/her passengers. Sure it could be stated that this danger originates from a malicious agent gaining illegal access to the vehicle, rather than the security of the internal vehicle system. But this assertion would gloss over the fact that the OBD-II interface was designed to be used only by repairman, testers, policemen, etc. Therefore it is only logical that this privileged use is enforced by the system, rather than being merely implied.

3.2 Attacker model

Here, an attempt is made to define the types of attackers that this paper aims to defend against. a similar classification as [24] and [20] is followed:

- **Insider or outsider:** The insider is considered an interactive member of the network, meaning he/she can communicate with other members freely. The outsider however is limited in the diversity of attacks he/she can mount.

  Classification: **outsider**, since the attacker is not part of the CAN bus. It is worth noting however that when the attacker uses the OBD port to mount an attack, he/she can communicate with the other nodes on the bus. This

however is treated by this paper as part of a successful attack, not as an a priori capability of the attacker.

- **Malicious or rational:** A malicious attacker exploits the system for reasons other than personal gain, making them more unpredictable since their motives and resources can vary. A rational attacker however is motivated solely by personal profit, be it money or fame, making them more predictable.

  Classification: **both**, since an attacker using the OBD port as attack vector could be both malicious (e.g. Endangering the life of a rival) and rational (e.g. lowering the internal odometer value before selling the vehicle).

- **Active or passive:** An active attacker is able to generate and transmit messages, whereas a passive attacker is constrained to eavesdropping.

  Classification: **active**, since we know the attacker can have access to tools (e.g. PassThru) that grant him/her active capabilities.

- **Local or extended:** This criterion is based on the scope of the attacker. A local attacker has only limited attack vectors, whereas an extended attacker has access to lots.

  Classification: **local**, since a comprehensive analysis of multiple attack vectors, although touched upon in section **??**, is considered out of scope for this paper (c.f. [22][13][25][17][20][8][15][5]).

Bibliography

[1] Cyber security and resilience of smart cars. Technical report, Agency for Network and Information Security (ENISA), 2016.

[2] Iso11898-3:2006: Road vehicles – controller area network (can) – part 3: Low-speed, fault-tolerant, medium-dependent interface. Standard, International Organization for Standardization, 2016.

[3] Siam Ahmed. Get to know connected vehicle technology: V2v, v2x, v2i. 2018. URL: https://www.geotab.com/blog/connected-vehicle-technology/.

[4] Abdul Rehwan Anwar. Bus arbitration in can (controller area network). URL: https://www.linkedin.com/pulse/bus-arbitration-can-controller-area-network-abdul-rehman-anwer, 2017.

[5] Stephanie Bayer, Thomas Enderle, Dennis Kengo Oka, and Marko Wolf. Security crash test –practical security evaluations of automotive onboard it components. Technical report, 2015.

[6] Robert Buttigieg, Mario Farrugia, and Clyde Meli. Security issues in controller area networks in automobiles. Technical report, University of Malta, 2017.

[7] Miguel Castro and Barabara Liskov. Practical byzantine fault tolerance. In *the Proceedings of the Third Symposium on Operating Systems Design and Implementation*, New Orleans USA, February 1999.

[8] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. Comprehensive experimental analyses of automotive attack surfaces. Technical report, University of California, San Diego and University of Washington.

[9] Pauric Doherty, Alan Molloy, Martin Glavin, and Fearghal Morgan. A review of bluetooth security in the automotive environment. In *Proceedings, the Irish Signals and Systems Conference 2004 : ISSC 2004*, 2004.

[10] Thomas Eisenbarth, Timo Kasper, Amir Moradi, Christof Paar, Mahmoud Salmasizadeh, and Mohammad T. Manzuri Shalman. On the power of power

analysis in the real world: A complete break of the keeloq code hopping scheme. Technical report, Horst Görtz Institute for IT Security Ruhr University Bochum, Germany and Department of Computer Engineering and Electronic Research Center Sharif University of Technology, Tehran, Iran, 2008.

[11] CAN in Automation (CiA). History of can technology. URL: https://www.can-cia.org/can-knowledge/can/can-history/.

[12] ISO11898-2. Iso11898-2:2016: Road vehicles – controller area network (can) – part 2: High-speed medium access unit. Standard, International Organization for Standardization, 2016.

[13] Pierre Kleberger. *On Securing the Connected Car*. PhD thesis, Department of Computer Science and Engineering Chalmers University of Technology SE–412 96 Gothenburg, Sweden, 2015.

[14] Dan Klinedinst and Christopher King. On board diagnostics: Risks and vulnerabilities of the connected vehicle. 2016.

[15] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, and Stefan Savage. Technical report, Department of Computer Science and Engineering University of Washington and Department of Computer Science and Engineering University of California San Diego, 2010. Experimental Security Analysis of a Modern Automobile.

[16] Charlie Miller and Chris Valasek. Adventures in automotive networks and control units.

[17] Charlie Miller and Chris Valasek. A survey of remote automotive attack surfaces. Technical report, 2015.

[18] Charlie Miller and Chris Valasek. Can message injection. OG Dynamite Edition, 2016.

[19] Jan Tobias Mühlberg, Frank Piessens, and Jo Van Bulck. Vulcan: Efficient component authentication and so ware isolation for automotive control networks. Technical report, Imec-Distrinet KuLeuven, 2017.

[20] Jonathan Petit and Steven E. Schladover. Potential cyberattacks on automated vehicles. *IEEE Transactions on Intelligent Transportation Systems*, September 2014.

[21] Olaf Pfeiffer and Christian Keydel. Scalable can security for can, canopen and other protocols. 2017.

[22] Lee Pike, Jamey Sharp, Mark Tullsen, Patrick C. Hickey, and James Bielman. Securing the automobile: A comprehensive approach. 2015.

[23] Andreea-Ina Radu and D. Flavio. Technical report, Garcia School of Computer Science, University of Birmingham, UK, LeiA: A Lightweight Authentication Protocol for CAN.

[24] Maxim Raya and Jean-Pierre Hubaux. Securing vehicular ad hoc networks. *Journal of Computer Security*, 15, 2007.

[25] Brian Russell, Aaron Guzman, Paul Lanois, and Drew Van Duren. Observations and recommendations on connected vehicle security. Technical report, Cloud Security Alliance Internet of Things Working group, 2017.

[26] AutoTap –OBDII Automotive Diagnostic Tool. Does my car have obd-ii? [Online; accessed 29-November-2018]. URL: http://www.obdii.com/connector.html.

[27] AutoTap –OBDII Automotive Diagnostic Tool. Obdii: Past, present and future. [Online; accessed 29-November-2018]. URL: http://www.autotap.com/techlibrary/obdii_past_present_future.asp.

[28] Shane Tuhoy, Martin Glavin, Ciarán Hughes, Edward Jones, Mohan Trivedi, and Liam Kilmartin. Intra-vehicle networks: A review. *IEEE Transactions on Intelligent Transportation Systems*, January 2014.

[29] Stefan N. ürnberger and Christian Rossow Cispa. Vatican vetted authenticated can bus. Technical report, CISPA, Saarland University, Germany, 2016.

[30] Wikipedia contributors. Anti-lock braking system — Wikipedia, the free encyclopedia, 2018. [Online; accessed 29-November-2018]. URL: https://en.wikipedia.org/w/index.php?title=Anti-lock_braking_system&oldid=870064581.

[31] Wikipedia contributors. Byzantine fault tolerance — Wikipedia, the free encyclopedia, 2018. [Online; accessed 29-November-2018]. URL: https://en.wikipedia.org/w/index.php?title=Byzantine_fault_tolerance&oldid=869107483.

[32] Wikipedia contributors. Can bus — Wikipedia, the free encyclopedia, 2018. [Online; accessed 29-November-2018]. URL: https://en.wikipedia.org/w/index.php?title=CAN_bus&oldid=870995924.

[33] Wikipedia contributors. Cyclic redundancy check — Wikipedia, the free encyclopedia, 2018. [Online; accessed 29-November-2018]. URL: https://en.wikipedia.org/w/index.php?title=Cyclic_redundancy_check&oldid=867705976.

[34] Wikipedia contributors. Obd-ii pids — Wikipedia, the free encyclopedia, 2018. [Online; accessed 29-November-2018]. URL: https://en.wikipedia.org/w/index.php?title=OBD-II_PIDs&oldid=870365927.

[35] Wikipedia contributors. On-board diagnostics — Wikipedia, the free encyclopedia, 2018. [Online; accessed 29-November-2018]. URL: https://en.wikipedia.org/w/index.php?title=On-board_diagnostics&oldid=870086948.

[36] Wikipedia contributors. Protocol stack — Wikipedia, the free encyclopedia, 2018. [Online; accessed 29-November-2018]. URL: https://en.wikipedia.org/w/index.php?title=Protocol_stack&oldid=866619457.

[37] Aastha Yadav, Gaurav Bose, Radhika Bhange, Karan Kapoor, N. Ch.S. N Iyengar, and Ronnie D. Caytiles. Security, vulnerability and protection of vehicular on-board diagnostics. *International Journal of Security and Its Applications*, Vol. 10, No. 4:405–422, 2016.

Fiche masterproef

Student: Michiel Willems

Titel: OBD–II Access Control

Nederlandse titel: Beste masterproef ooit al geschreven

UDC: 621.3

Korte inhoud:

Thesis voorgedragen tot het behalen van de graad van Master of Science in de ingenieurswetenschappen: computerwetenschappen, hoofdoptie Veilige software

Promotor: Prof. dr. Bruno Crispo

Assessor:

Begeleiders: Mahmoud Ammar
Hassan Janjua