Universiteit Leiden

ICT in Business

Security challenges and viable solutions for continuously connected near-autonomous vehicles

Name: David Virag
Student-no: s2075474

Date: 23/07/2019

1st supervisor: Mike Preuss

2nd supervisor: Tyron Offerman

Company supervisor: Bart de Jong (Accenture Security)

MASTER'S THESIS

Leiden Institute of Advanced Computer Science (LIACS)

Leiden University

Niels Bohrweg 1

2333 CA Leiden

The Netherlands

Abstract

Connected cars are becoming more popular and will be the standard in all cars in the near future. However, connected cars also raise a problem, such as, a wider attack surface than offline cars.

This paper analyses what the current state of IT security is in continuously connected near-autonomous vehicles as well as possible solutions to the security vulnerabilities.

To answer this question, the existing literature on this topic was studied. Furthermore, ten experts working in this field were interviewed to gain insights. A survey was also published and analysed about the awareness of connected car security in the general public.

The results showed that there is room for improvements for car manufacturers. The survey also showed that the awareness about the possible vulnerabilities are not yet widely known. Solutions were also provided by the experts, which were discussed in this paper.

This study emphasizes the need for better security in connected cars. Moreover, more experts are needed in this area to be able to further develop appropriate security measure for connected cars. The survey also showed the lack of awareness about connected cars which shows that the public needs to be more aware of the dangers of the cars they drive every day.

Keywords: connected car security; vehicular IoT; security mechanisms; Vehicular communication systems

Acknowledgments

Throughout the writing of this thesis, I have received a great deal of support and assistance. I would like to first thank my first supervisor M. Preuss for his guidance throughout the thesis writing process. Furthermore, thanking my second supervisor T. Offerman for his supervision.

I would particularly like to single out my supervisor at Accenture, B. de Jong. I want to thank you for your excellent cooperation and for all the opportunities I was given to conduct my research and further my thesis at Accenture. Furthermore, I would like to acknowledge my colleagues from my internship at Accenture Security for their motivation and help throughout the writing of this thesis.

Last but not least, I would like to thank my girlfriend for her patience in these past six months. Her motivation and support made it possible to finish this thesis.

Acronyms

ADAS	Advanced driver-assistance system
AP	Access Point
CAN	Controller Area Network
CRC	Cyclic Redundancy Check
D2B	Domestic Digital Bus
ECU	Electronic Control Unit
IOT	Internet of Things
IIOT	Industrial Internet of Things
ICS	Industrial Control Systems
MITM	Man-in-the-Middle
MOST	Media Oriented Systems Transport
OBD-II	On-Board Diagnostics II
OTA	Over the Air
PbD	Privacy by Design
R&D	Research and Development
RDS	Radio Data System
TPMS	Tire-pressure monitoring system
TT-CAN	Time-Triggered CAN
TTP	Time-Triggered Protocol
VANET	Vehicle Ad Hoc Network
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-everything
VC	Vehicular Communication

Contents

1. Introduction

Computers and network connected computer systems are playing an increasingly important role in our lives, thus the use of information systems is more and more important, and we are becoming gradually dependent on them. With this dependency, information is becoming more valuable, hence it involves problems of its security and their ways of protecting them (Young, 1998). With the rising popularity of Internet of Things (IoT), devices that were previously not connected to the internet offer a new point of attack, thus they need special attention regarding security (Zhoue et al., 2018). According to Hung (2017), over 20 billion connected things are projected to be in use by 2020. These devices aim to facilitate the life of its customers by offering features that are not possible without connecting to the internet. Manufacturers continuously improve the safety of their connected devices, however there are no adequate holistic concepts for IT security (Hoppe et al., 2008).

Connecting things and making them smarter also applies to cars. In 2013, it is estimated that 23 million cars were connected to the internet. By 2020 this number is expected to grow to over 152 million, making connected cars an important element of the IoT devices ecosystem (McCarthy, 2015).

The first electronics systems assembled into cars were vacuum tube car radios from the beginning of the 1930s (Berkowitz, 2010). Since then, the variety of electronic systems that can be installed into a vehicle has only broadened. Adaptive Cruise Control, Blind spot monitors, Automatic parking, and many more features are standard equipment now.

For example, manufacturers are storing and analyzing telematics data from connected cars to offer services like real-time health diagnostics with automated maintenance scheduling, location-based concierge services, and automated electronic payments at toll gates, parking slots and, gas stations (Bajaj et al., 2018). Furthermore, insurance companies can track connected cars' usage, thereby offering policies with rates based on usage, driving behavior, and other variables, helping both the driver and the company (Coppola, 2016). Furthermore, the insurance company's risks are lower since if a car gets stolen, they can get the car's location and proceed with the police. The users of these cars can enjoy the benefits of these services and are willing to pay more to have a car that offers these functionalities (Accenture, 2016).

A pioneer in connected cars, Tesla, introduced their first commercially available electric car in 2012. It featured a 17-inch infotainment control touchscreen like a computer display and other advanced technologies like radars, cameras, LTE and WIFI connectivity (Fleming, 2014). Furthermore, all new cars built after the 31st of March 2018 and sold in the European Economic Area (EEA) are now equipped with a SIM card to provide the so-called 'eCall' service in case of emergency (Oorni et. al, 2017). The eCall service is supposed to contact emergency services and send GPS coordinates to them so they can arrive at the location quicker. This technology is made mandatory by the European Commission and concerns all private cars sold in the EEA (Oorni et. al, 2017).

Additionally, a modern car is equipped with 50-100 embedded electronic control units (Charette, 2009). Car manufacturers are also equipping their cars with a mobile data connection to provide up-to-date maps, in-car entertainment, and many other functionalities that make a car journey more pleasant. Both Apple and Google developed their own system that allows supported phones to interface with the car's built-in infotainment system to offer functionalities like phone calls, messaging, and media playback (Fleming, 2014).

Furthermore, the car manufacturers store the telematics data from these electronic systems in the cars to offer services and to improve their products (Grymek et. Al, 2017). Hence, car manufacturers are in connection with these cars.

With all these functionalities equipped, cybersecurity risks need to be taken seriously. If the manufacturer can access these data, it can also be possible for third parties without the appropriate security measures. A recent high-profile demonstration was reported by the Chinese Tencent Keen Security (2016) lab in which researchers were able to remotely control some systems on the Tesla Model S in both driving and parking modes by exploiting weaknesses in the Tesla web browser. Tesla was able to roll out an over-the-air upgrade to fix the exploits within 10 days of being notified about them. Another demonstration was done by ethical hackers on a Jeep, including showing how to use a remote laptop to control the steering, brakes, and other functionality in a moving vehicle, exploiting the near-autonomous possibilities of the vehicle. These demonstrations have raised concerns about the cybersecurity and safety of connected vehicles (Greenberg, 2015). These demonstrations show that systems, where the vehicle is continuously connected to the outer world, are increasingly complicated thus more and more security flaws are present in these vehicles, providing a risk of exploiting the near-autonomous possibilities of vehicles. While near-autonomous cars can be driven by algorithms in limited situations, however, human supervision is still required

1.1 Research setting

This thesis was written with help from Accenture as part of my graduation internship within the master ICT in Business of Leiden University. During the internship, I was part of the security team of Accenture, which counts over 60 employees in the Netherlands and over 5.500 international. Accenture serves multinational companies in several topics like Strategy, Consulting, Digital, Technology, Operations and (Cyber)Security. While the number of experts in connected car security on the market is relatively small, Accenture has experts from all over the world.

1.2 Problem Relevance

The importance of security in connected cars is exemplified in Figure 1. According to Greenough (2016), by 2020, 75% of cars shipped globally will have connected features. Connected cars can be found everywhere nowadays and it is not a rare niche. By living in a connected world where computers, phones or with the help of IoT almost anything can be connected to the internet. Car manufacturers had must move on with the world and support connected services. Car owners usually tend to like their car, and with the additional benefits of connected services, the car is made more valuable to its users.

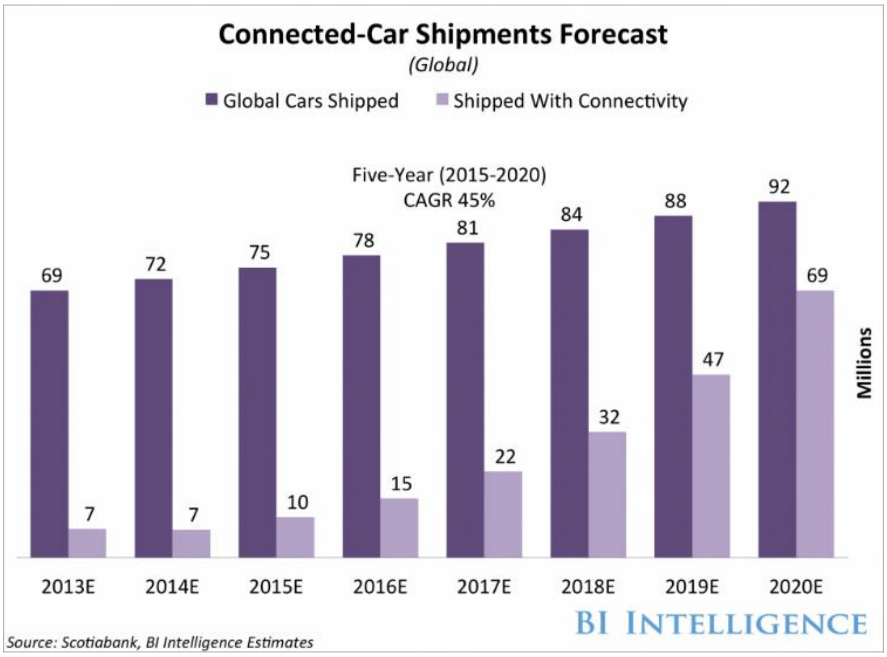

Figure 1. Global Connected-Car Shipments Forecast

One of the main features of connected cars is the possibility to access the car's status via a smartphone app and even control some functionalities like heating, windows, and door lock. Furthermore, autonomous cars can and will benefit from the in-car connectivity. Vehicles with predictive drive functionality like Tesla are sending the data generated by the cameras and sensors back to the manufacturers in order to improve their self-driving capabilities.

1.3 Assumptions

This thesis will assume that:

1. Connected cars are continuously connected to the internet.
2. All new cars sold today have at least one external communication channel (E-call).

1.4 Definitions

This section is meant to give clear definitions for the terms that emerged around connected car security.

1.4.1 Connected Cars

When searching for the term connected cars, various definitions emerge and the interpretation varies across authors. For this research, we use the following definition (Kollaikal, Ravuri, & Ruvinsky, 2017): A Connected Car is a car that is connected to the internet. Cars are collecting more and more data. Amongst others, data is collected on fuel consumption, driving behavior, the technical condition of the car and where the car has been. This data can be shared via the internet with the driver, but also with manufacturers and dealers. The term ‘continuously’ means that the cars not only use the mobile data to send back telematics to the manufacturer, but it can be used for navigation, media, remotely functionate the car’s heating unit or to see the car’s location. The near-autonomous term specifies that these cars are not yet fully autonomous, but they all have some or many Advanced driver-assistance systems (ADAS) installed. With systems like lane departure warning, automatic lane centering, and adaptive cruise control, most connected cars can travel autonomously, but only for a limited time, and with the driver’s full attention. The main difference between a connected car and an autonomous car is in the way of self-driving. Where connected cars rely on a few sensors to drive nearly autonomous, autonomous cars have several sensors redundantly installed all over the chassis to allow the car to drive autonomous.

1.4.2 Attack vector

An attack vector is a possible way by which a malicious third party can gain access to a computer or server in order to cause a malicious outcome. Attack vectors make possible for hackers to exploit security vulnerabilities. The more attack vectors an object has, the less secure it is.

1.4.3 Electronic Control Unit (ECU)

Electronics in the automotive industry originated from the need to control engines. The first electronic parts were used to control engine functions and were referred to as Engine Control Units (ECU). However, as electronic controls began to be used for more automotive applications, the ECU acronym got a more general meaning of Electronic Control Unit. After the name change, the acronym ECU is given to devices that control one or more electrical systems in a vehicle. The ECU is providing instructions for various electrical systems telling what to do and how to do it. A modern high-end car can have more than 100 ECUs, while lower-end models operate with less than a 100. Some examples of important ECUs found in every modern car includes the Engine Control Module (ECM), Transmission Control Module (TCM), Antilock braking module (ABS), and Telematic Control Unit (TCU).

1.4.4 OBD

On-Board Diagnostics (OBD) is the vehicle’s built-in self-diagnostic system. The OBD system gives access to technicians to access the vehicle’s subsystems. The early version of OBD could only indicate a malfunction by flashing an indicator light on the vehicle’s dashboard, without additional information on the cause of the problem. However, modern OBD implementations like OBD-II use a standardized digital communications port to provide real-time data in addition to a standardized series of diagnostic codes, which allow technicians to identify and fix malfunctions within the vehicle (Checkoway et al., 2011).

1.4.5 CAN Bus

CAN (Controlled Area Network) is an event triggered bus system used for soft real-time communication between controllers. It was invented in the 80s, with the goal of reducing the number of wires needed, hence reducing the weight of the car and its price. The use of the

CAN bus varies amongst car models; however, it is often used for tasks like managing the engine's system, A/C unit, central lock, Airbag, and many more (Corrigan, 2016).

1.4.6 MOST, D2B, and GigaStar

MOST (Media Oriented System Transport), D2B (Domestic Digital Bus) and GigaStar are multimedia bus systems aimed to offer high-performance and wide-band communications channels. These networks are used to diffuse in-vehicle high-quality media (Wolf, Weimerskirch, & Paar, 2004).

1.4.7 FlexRay, TT-CAN, and TTP

FlexRay, TT-CAN (Time-Triggered CAN), and TTP (Time-Triggered Protocol) are time-triggered hard real-time bus systems. They all guarantee determined transmission times, hence they can be used with Drive-by-Wire systems (Wolf et al., 2004).

1.4.8 LIN

Local sub-networks like LIN (Local Interconnect Network) are used to control small autonomous networks used for various use cases like electric window regulation, door locking mechanisms, and communication with several sensors (Wolf et al., 2004).

1.5 Research question

The development as outlined in the introduction leads up to the following main research question:

What are the security challenges and viable solutions for continuously connected near-autonomous vehicles?

To answer this question, a qualitative approach will be followed to obtain a deeper understanding of the problem. Consequently, apart from the literature review, semi-structured interviews will be conducted with experts working with connected cars. Hence, data will be collected by performing interviews which will provide this study with further understanding about connected car security.

Supporting the main research question, the following research sub-questions will also be observed:

1. *What is the difference in term of security with in-car networks (LIN, CAN, MOST, FlexRay)?*

2. *How can the in-car networks be protected?*
3. *Do the various vehicular communication systems (V2I, V2V, V2N, etc) have different security issues?*
4. *To what extent are external attacks probable?*
5. *Which attack vectors present the biggest risk?*

The purpose of this thesis is to present proposals for mitigation of the security issues of the IoT technologies used in the automotive industry based on literature review, interview with experts, and a survey. This topic is relevant because cars are getting increasingly connected, while their software security is not evolving at the same pace. Millennials who grew up having computers and smartphones with mobile data connectivity will become the primary target for car manufacturers (Giffi et. Al, 2017). These potential clients like to have a connected and 'smart' car since they are used to the other connected devices. More and more features will be developed by the manufacturers and with the rise of autonomous cars, the security aspect will become a primary concern. With more connected cars being in use by people all over the world, security flaws will be more apparent (KPMG, 2017).

2. Literature review

The topic of connected car security has been extensively researched already and various papers and articles have been written detailing the different security risks that connected cars can have as well as demonstrating them with different experiments. Some papers have also offered solutions to these risks. In this chapter, the literature covering connected car security will be summarized and the different risks will be presented along with solutions to them where available.

2.1 The Jeep hack

One of the first and most popular connected car hacking demonstration was done by Charlie Miller and Chris Valasek (2015). They are the researchers who made the public and manufacturers aware of the possibility of remote car hacking, by successfully performing a remote attack against an unaltered Jeep Cherokee in 2015 (Miller & Valasek, 2015). The vehicle was hacked through the Uconnect system which operates the telematics, internet, radio, and apps. The exploit was able to control vital functions like brakes and steering. They demonstrated this live with a reporter in the car while the two researchers were remotely connected to the Uconnect system. They were able to remotely control the air-conditioning, radio, and windshield wipers and, they were able to cut the transmission. The reporter in the car was unable to accelerate on the highway. Finally, the researchers disabled the brakes and let the car run into a ditch. This was all possible by modifying the firmware of the Uconnect system over the air. The attackers only needed the IP address of the system. The rewritten firmware made it possible to send commands through the CAN bus, thus granting complete access to the vehicle. Although this model had an online connection, the patch that Chrysler made for the Uconnect system had to be installed manually, or by a dealership mechanic (Miller & Valasek, 2015).

2.2 Senator Markey’s investigation

The senator of Massachusetts, Ed Markey, sent a letter to 20 major car manufacturers requesting information about how consumers are protected from cyberattacks or privacy violations. In the press release Senator Markey (2013) specified why this is important: "As vehicles become more integrated with wireless technology, there are more avenues through which a hacker could introduce malicious code and more avenues through which a driver's basic right to privacy could be compromised," writes Senator Markey (2013), a member of the

Commerce, Science and Transportation Committee, in the letter to the car companies. "These threats demonstrate the need for robust vehicle security policies to ensure the safety and privacy of our nation's drivers. Airbags and seat belts protect the safety of drivers, but we also need car companies to ensure the security and privacy of those in automobiles in this new wireless age," citing Senator Markey. From the answers received from the automotive manufacturers, the staff of Senator Markey wrote a paper (Markey, 2015). The most interesting finding is that ”Security measures to prevent remote access to vehicle electronics are inconsistent and haphazard across all automobile manufacturers, and many manufacturers did not seem to understand the questions posed by Senator Markey.” (Markey, 2015). Furthermore, “Only two automobile manufacturers were able to describe any capabilities to diagnose or meaningfully respond to an infiltration in real-time, and most say they rely on technologies that cannot be used for this purpose at all.” (Markey, 2015). Unfortunately, this is the most reliable information that we have on the market because the automotive manufacturers are reluctant to reveal what they are doing.

2.3 Previous research

Previous research has shown that compromising the connected cars’ internal network can result in compromising the entire vehicle (Becsi, Aradi & Gaspar, 2015; Checkoway et al., 2011; Thing & Wu, 2016; Wolf et al. 2004). Thing & Wu (2016) found that connected cars are more susceptible to malicious cyber-attacks mainly due to two factors. First, the increased intra-vehicular communication requires many ECUs, which are interconnected with CAN bus. Safety-critical components, like the engine control module, or the emergency brake control module are using the high-speed CAN layer, while the other components are using the regular, low-speed CAN layer. Since there is a connection between these two layers via gateway bridges, it is possible that malicious data packets are introduced at the low-speed CAN layer, which can propagate to the High-speed, safety-critical CAN layer. This can be done because CAN packets do not contain an authenticator field, thus by infecting one node, it is possible to listen to all communications or even broadcast packets to other components. Second, the external communication in connected cars is also more vulnerable because it is more complex, as the internal communication. The external communication of connected cars is much more advanced because it needs to support several types of communication. Vehicle-to-Vehicle communication, to facilitate the on-road information transmission, furthermore Vehicle-to-Infrastructure, and Vehicle-to-IoT communication will become more common on the roads.

However, if an infected car gets connected to its surrounding, the other cars could get compromised too.

Becsi and colleagues (2015) also found similar results. They distinguish three types of areas within a connected car; the first area is the electronics under the hood, namely: ECU, vehicular network, and communication gateway. The second is the mobile device of the user which can be connected to the car's infotainment system. The third area is the cloud infrastructure managed by the manufacturer. The first problem with ECUs is that they are not protected by reverse engineering by disassembling or circuit probing. Another issue can be the presence of backdoors – the developers working on the ECU might leave a backdoor open for testing purposes, negligently or in an intended way. This issue seems to be widespread since Checkoway and colleagues (2011) also found services for file transport and a screen-oriented text editor in the ECUs which should be removed, since these programs make it easier for an attacker to exploit the ECU. Another big issue is the possibility to reflash the ECU by a third party. Like any computer, the ECU has software with different settings, and these can be changed to alter the performance, driving characteristics, or it can be remapped with malicious intents. This process is known as ECU remapping or reflashing. If the ECU is susceptible to reflashing, several problems arise:

1. *Authentication: how to ensure that the identity of the sender is accurate?*
2. *Authorization: do they have the rights to reflash?*
3. *Non-repudiation: how to keep track of the changes made?*
4. *Integrity: is the data modified?*

If the attacker is able to reflash the ECU firmware, then they can carry out a Direct-access attack and do anything with the car.

The vulnerabilities of vehicular networks lay in the fact the vehicular networks, like CAN, FlexRay, LIN or MOST were developed to be reliable and cost-effective (Johansson, Torngren & Nielsen, 2005). The main assumption was that these systems will not get in contact with the outer world, furthermore, they will remain in a closed network with a closed topology. Thus, these vehicular networks are not designed to protect from attacks, but they still need to provide the same security as any other ICT network. Furthermore, connected cars are offering more and more functionalities which are powered by the operating systems of the vehicle. For this reason and because of the lack of software patches, the connected cars can become less secure. Moreover, older models, which are no longer under warranty are not getting bug fixes, thus newly found vulnerabilities remain unchanged (Mohs & Schulte, 2016).

2.4 Remote exploit

Checkoway and colleagues (2011) aimed to exploit connected cars remotely, without prior physical access. Previous research has proven (Koscher et al., 2010) that the internal networks of some modern cars are not secure, however, prior physical access was needed, which is viewed as unrealistic as physical access is not possible in most cases. Furthermore, it has also been proven that an attacker connected to the car's internal network can circumvent all control systems even critical equipment like brakes and engine (Koscher et al., 2010).

Checkoway and colleagues (2011) distinguish several possible attack vectors on connected cars using the following approaches: indirect physical access, short-range wireless access, and long-range wireless access. The vulnerabilities that they discovered have resemblances and they believe that the cause of these vulnerabilities is the structural issues in the automotive ecosystem. A modern luxury vehicle has up to 70 distinct ECUs with tens of millions of lines of code. The ECUs are interconnected with either a type of CAN or FlexRay bus. This interconnection provides many practical features like an adaption of the radio volume to the car's speed or the pre-tensioning of the seatbelts in possible crash situations. These functionalities, however, introduce a broad internal attack surface on a given bus since each component can access the other components (Becsi, Aradi & Gaspar, 2015; Checkoway et al., 2011; Wolf et al. 2004; Thing & Wu, 2016). According to Checkoway and colleagues (2011) there has no research been done on the external attack surface of modern vehicles, except one analysis by Rouf and colleagues (2010) on the wireless Tire Pressure Monitoring System (TPMS). While this study mainly focused on the privacy aspects of the TPMS broadcasts, they also managed by accident to stop the ECU managing the TPMS data by spoofing erroneous readings. Other researchers like Francillon and colleagues (2011) have demonstrated relay attacks against keyless entry systems, however, this research is the first one to consider the full external attack surface of the modern-day automobile.

The experimental work that Checkoway and colleagues (2011) have done was based on a moderately priced, late model sedan featuring standard options. This car has less than 30 ECUs, which are connected amongst themselves with CAN buses and bridged when required.

In terms of external vectors, this car has many, including the OBD-II port, media player, Bluetooth, wireless TPMS sensors, keyless entry, satellite radio, RDS, and telematics. The telematics is using a mobile data connection to transfer its data to the manufacturer, moreover, it connects to all the CAN buses while also having access to the Bluetooth and GPS connection. To test the ECUs, they extracted their firmware and reverse engineered its I/O code. Almost all the ECUs were accessible via the CAN bus, which made their work much easier. One of the most installed indirect physical channels that an attacker could use is the media player, which are present in almost all the cars sold today and can receive AM and FM signal and digital signals like RDS. Most media players also have a CD reader which can decode audio formats such as WMA and MP3. Checkoway and colleagues (2011) found two vulnerabilities affecting the media player. First, they found that this specific media player automatically recognizes a CD with a specific formatting style and can reflash the unit with the data written on the CD. Second, they found that with creating a special file and when launched on the media player it causes a buffer overflow. This can be especially problematic when the audio file is distributed by a third party with the malicious code inside, possibly able to render inoperable the media players when the file is played.

Another indirect physical channel is the OBD-II port. This port can access all the CAN buses in the vehicle because it is designed for technicians to diagnose the car and update ECUs. Since 2004, all new cars in the US is compatible with the SAE J2534 “PassThru” standard which is an API that offers an interface to communicate with the vehicle’s internal buses (Hellberg & Pettersson, 2013). This standard has two vulnerabilities. First, if the attacker and the PassThru device are on the same WiFi network and the PassThru is connected to the car, it can give access to the reprogramming of the car. The second problem is the PassThru device itself. The researchers were able to implant malicious code to the device, and thus it can infect the car that is connected to (Checkoway et al., 2011).

A popular short-range wireless channel is Bluetooth. Ryan (2013) already proved that it is possible to render useless the encryption of any Bluetooth Low Energy link. In the studied car, the Bluetooth capabilities were built into the car’s telematics unit. After reverse-engineering the telematics system’s operating system, they found the service in charge of handling the Bluetooth functionality. This system made exploitable by an unchecked “strcpy” call when handling a Bluetooth configuration command, which is dangerous because this function does not allow to specify the size of the output buffer so buffer overruns are often a risk. It is challenging for an attacker to pair their phone to the car’s system, however, the researchers managed to infect a smartphone running Android 2.1 with a malicious app. If an app like this is downloaded, it monitors the background Bluetooth activity and when a smartphone is connected to the car’s head unit, it sends the attack payload. A malicious app like this can be disastrous when it is uploaded to the Google play store or Apple App Store, and users download it without knowing the risks.

In the case of long-range wireless communication, cellular is the main channel. The car’s cellular capability offers both safety and convenience features like emergency call upon a crash. The car has a cell phone interface with voice, SMS, and 3G data support. The 3G data is mainly used for navigation and location-based services, while the voice channel is used for critical telematics functions since it has better coverage than mobile data. After reverse-engineering the protocol, which is responsible for controlling both the voice and mobile data communication, the researchers were able to bypass the authentication process by using a logic flaw in the unit’s authentication system which enabled them to succeed with the authentication challenge after 128 calls. Since this attack is using voice to transmit data, the researchers managed to compromise the car with only an iPod and an office landline phone by simply dialing the car’s number and playing the file close to the microphone (Checkoway et al., 2011).

Furthermore, Checkoway and colleagues (2011) did not only demonstrate the vulnerabilities and showed them in action, but they also pointed out how these vulnerabilities could be used by an attacker. One of the most obvious cases is theft, however, these vulnerabilities can offer way more to an attacker than unlocking the car. If an attacker tries to compromise the vehicle as much as possible, telling them to contact a central server and communicate their GPS locations, and their Vehicle Identification Number (VIN) the attacker has a list of the compromised cars with precise locations. Furthermore, from the VIN, the thief can decode the car’s-built year, manufacturer, and model, thus it is easy to approximate each car’s value. This workaround can also be sold by the attacker to thieves, thus the danger of getting caught is less pressing. Another use could be compromising the car's telematics unit and record the conversations with the built-in microphone, and exfiltrate the data using the car's mobile data connection.

2.5 Implementation fixes

Checkoway and colleagues (2011) also suggested implementation fixes for the vulnerabilities they have found. The fixes can be categorized as restricting access and improve code robustness. For the Bluetooth vulnerability, the fix could simply be not letting the car pair with devices without switching the car to pairing mode by the owner. Moreover, the PassThru's configuration protocol should use application-level authentication and encryption to protect its code from abuse. Furthermore, the debugging symbols and error strings should be removed from the ECU code, and the ECUs should only be allowed to be reflashed by a bus with the smallest attack surface. Moreover, services like FTP and vi should be removed from the PassThru and telematics devices, since these programs make it easier for an attacker to exploit the ECUs. Checkoway and colleagues (2011) also give their opinion about why these basic recommendations are not yet in place. First, automobiles were not connected to the internet in the past, thus they did not have to anticipate the actions of an external opponent. This is similar to the evolution of personal computer security in the 90s. When the internet became available the computers connected to it were directly exposed to vulnerabilities that could not be foreseen. Hopefully, automotive manufacturers will fix the vulnerabilities and making security a top priority before any high-profile attack happens like it did with the PC industry. Second, it can be observed that all the vulnerabilities discovered were at the interface boundaries between code written by distinct organizations. Most vulnerabilities were not in the ECU's software itself, but in the glue code that is supposed to integrate it with the car's system. Meaning the manufacturer is not responsible for the software development but only the integration. This is due to the fact that manufacturers do not have access to the source code of the ECUs since the codebase is the intellectual property of the supplier. And while the supplier does unit testing on their ECUs, the manufacturers have a hard time finding security vulnerabilities at the integration stage.

3. Methodology

3.1 Introduction and Overview

According to the Cambridge dictionary (n.d.), a methodology is: “a system of ways of doing, teaching, or studying something.” Defining the research methodology helps to lead and give a structure to the research. The first step in defining the methodology is to set the focus and scope of the study. To be able to do that, a literature review has been done in chapter 2. This literature review enables the reader to see what has already been researched in this topic and to which conclusions that research led. This thesis uses qualitative data to draw conclusions and uses more than one research method for data collection. The first step was to perform a literature review to gain a thorough understanding of the topic. Following up on the literature review, interviews were performed with subject matter experts. Chapter 3 is about Methodology, or also known as Research design explaining how the research is done. Chapter 4 focuses on the findings of the interviews and provides data to analyze in the next chapter, called Analysis and Discussion. The last chapter, Conclusion, and Discussion, shows how the research plan has been addressed in such means that a conclusion is formed from the evidence of this thesis.

3.2 Overview of Information Needed

According to Bloomberg & Volpe (2008)**,** this sub-section is meant to describe the type of information needed in order to answer the research question. This thesis makes use of different types of information; theoretical, demographic, and interviews with experts. Theoretical information is the knowledge that already exists and can be found in general literature. For this reason, a literature review has been done in Chapter 2. It sets the context, gives information on the research that has been done in this area, and helps in setting the direction for the interview questions. Demographic information contains data that describes the participants. The participants’ demographics could influence their answers and thus, could explain their different views on the topic. Moreover, it could explain their motivations to their answers. Similarly, the companies that they work for could influence their answers and their views.

Most commonly, qualitative research makes use of interviews as the source of data. Interviews are a good source of the interviewee’s thoughts and beliefs. There are three types of research interviews: structured, semi-structured, and unstructured. Structured interviews use a set of questions that are asked in a standardized order, and the interviewer cannot deviate from the pre-defined questions. Furthermore, the questions are closed-ended so the answers are going to fit into pre-decided categories. The advantage of structured interviews lays in the fact that they are easy to replicate. Moreover, structured interviews are shorter than other types of interviews. This can be useful when a lot of interviews need to be conducted within a short time period. Furthermore, with large sample size, the findings can become representative and thus can be generalized to a large population. The main disadvantage of doing structured interviews is that new questions during the interview cannot be asked since the interview schedule must be followed. Moreover, since structured interviews only create quantitative data, the motivations behind the answers are not known. For this research, the semi-structured approach was used. Semi-structured interviews have numerous key questions to define the areas meant to be explored, however, it also allows the interviewee to explore other ideas or to give a more detailed response. This interview structure also allows to emerge key findings that were not thought of before the interviews. The disadvantage of the semi-structured interview is that it is harder than the other types. First of all, it is time-consuming and interview skills are required to maintain an interesting and useful conversation. It is also important to prepare the questions but also to avoid leading or prescriptive questions. In order to make comparisons, a sufficient amount of people are needed, and the analysis is harder than for structured interviews since the answers can be different. On the other hand, unstructured interviews or so-called discovery interviews resemble to guided conversations and an interview schedule is not mandatory, and if there is one, the questions are open-ended, and they can be asked in any order. Additionally, questions can be added or discarded during the interview. The main strength of unstructured interviews is the flexibility. Since the questions can be adapted based on the responses from the interviewee, the interview can diverge from the interview schedule. However, this type of interviews can be time-consuming and hard to analyze the qualitative data.

The interview questions were designed to induce as much information about the topic as possible while being able to address the goals and purposes of the research. The questions are open-ended; thus, they require more information, and the expert can really talk about the topic without being constrained by close-ended questions. The first few questions are simpler, so participants could answer them more easily and get acquainted with the topic of the research. The remaining questions went into more detail concerning the research topic. This was done to make the interviewee more at ease during the interview.

Before the actual interviews, a pilot interview was conducted with a university supervisor. This practice is favorable because it can verify if the questions are understandable and that the interviewees will be able to answer them. If these terms were not met, the question was fine-tuned to be compliant with the previous requirements. The overall length of the interview was also tested since the experts did not have time for multi-hour interviews.

An interview schedule was used, thus before the interview, the interview questions were sent to the interviewees to help them familiarize with the questions, therefore they will not be surprised by the questions. Furthermore, participants were informed about the study details and were assured about the ethics, such as anonymity and confidentiality. This is important because the respondents will more likely be honest, and it is also a fundamental step in the consent process. The interviews will also be recorded to be able to use later for the data analysis. The respondents were informed about the recording of the interviews beforehand and at the beginning of the interview.

At the end of the interviews, the participants were thanked for their time and they were asked if they wanted to add anything. This enables the participants to discuss issues that they were thinking of during the interview but did not ask. These ideas can lead to discover new and unforeseen information.

3.3 Research Sample

This research started without a network or connections to the automotive industry. The sampling method used is theory-based, so it is possible to develop a theory and concepts that are grounded in or emergent from real-life events. Since the research has been done at Accenture, the first set of research participants were selected based on previous work done on connected car security within Accenture. These people are security consultants with knowledge in IoT, Industrial IoT (IIOT), and Internal Control Systems (ICS). Their work was uploaded to the internal repository, thus easy to find the relevant documents and to contact the authors. These experts were asked if they know more people who are also experts in the topic and should be interviewed next.

3.4 Data-Collection Methods

The interview that was conducted with each expert was a semi-structured interview. There were set questions, however when the experts wanted to add something or if a different topic came up, then it was also encouraged as long as it was relevant to the research. The questions were all the same for each expert. This allowed the interviews to be comparable and to be analyzed. The questions are based on literature review; thus, they question real problems.

The experts were contacted via e-mail, and the interviews were conducted via Skype due to geographical limitations. Their consent to be included in this research was also asked through e-mail prior to the interview taking place. The questions were sent by e-mail before the interview to provide the participants enough time to prepare for the questions. In all, 10 experts were interviewed. After the seventh interview, the data started to become saturated, meaning there was no new information received after the seventh interview, thus with 10 interviews the topic was well covered.

The following interview questions were asked in this research:

1. *What is your role in your organization?*
2. *What is your opinion on the current state of in-vehicle IT security?*
3. *Are connected cars less or more secure than "offline" cars, why?*
4. *Where do manufacturers spend a considerable amount of attention/time/money, and where should they spend more?*
5. *How much attention/time/money do manufacturers spend on IT security in contrast with the previous question?*
6. *What is the biggest problem in automotive IoT security in 2019?*
7. *How did the automotive IoT security change over the last five years?*
8. *What are the weak points of connected cars?*
9. *What is the most likely attack vector on a connected car?*
10. *What is the best defence to prevent hacking in general?*
11. *What is the best defence to prevent hacking via direct physical access?*
12. *What is the best defence to prevent hacking via wireless access?*
13. *What is the possible solution to mitigate security risks?*
14. *Could vehicular communication systems like Vehicle-to-vehicle or vehicle-to-infrastructure communication pose security risks?*

15. *Is there a difference in terms of security between the different types of automotive network communications protocols (LIN, CAN, MOST, FlexRay)?*
16. *Could the encryption of network communication protocol data improve security?*
17. *All new cars sold in the EEA has an integrated E-call feature which requires a cellular connection, do you think this service is safe?*
18. *Would you like to add something?*

The first three questions are more general, and they are about the current state of connected car security. These questions were added to find out whether the expert thinks that online cars are safe or not compared to offline cars and current trends. Question four and five aim to find out the priorities of the manufacturers and the opinion of the experts on this. Question six and seven investigate the state of automotive IoT and the current trends amongst manufacturers. Question eight through 13 explore the weak points of connected cars and tries to find possible solutions to make connected cars more secure. Question 14 can be traced back to chapter 1.5, research sub-question 3, precisely: *"Do the various vehicular communication systems (V2I, V2V, V2N, etc.) have different security issues?"*. To be able to answer the research question, in this question the different types of vulnerabilities of the vehicular communication systems are discussed. Similarly to question 14, question 15 tries to find an answer for the research sub-question 1: "*Do the various in-car networks (LIN, CAN, MOST, FlexRay) have different security issues?".*

The literature review also provided some directions to what questions to ask, for example in question 16 a specific example of a possible solution is referenced. Question 17 looks at mandatory connected safety equipment, specifically the E-call feature and asks for the opinion of the expert. The last question is asked to suggest to the interviewee to feel free to express other ideas or opinions that they want to add but has not been explicitly asked.

As previously stated, the main research question is, '*What are the security challenges and viable solutions for continuously connected near-autonomous vehicles*.' To answer this research question, the vulnerabilities of connected cars need to be explored. Moreover, some solutions also need to be proposed. The questions in the interview help to answer the research question by having experts give their opinion on what the actual vulnerabilities are applicable on connected cars. The literature review has already given possible vulnerabilities; however, the experts can answer from a more practical side as well. Thus, the interviews in combination with the literature review will provide sufficient information to be able to answer the research question as well as to draw appropriate conclusions.

Moreover, a survey with 100 respondents was also used to study the awareness of connected car security of the public. The margin of error (or confidence interval) is given by 1/√N, where N is the number of participants or sample size (Niles, 2006). With a sample size of a 100 people, the margin of error is 10%. This means that if for example 60% of the participants reported a fear of snakes, there would be a 95% probability that between 50% and 70% of the total population have a fear of snakes. It is essential to have at least 100 respondents in order to have acceptable accuracy. For this reason, the survey was closed when it reached 100 respondents. The survey showed that 90% of respondents were between ages 18 and 30, 8% between 31 and 45, and 2% between 46 and 60. From the 100 respondents 52% were male, and 48% were female. From the respondents, 58% indicated that they have a Master's degree, 37% a Bachelor's degree, and 5% a High school degree. Table 1 below summarises this data in a demographic table.

	Percentage
Gender	
Male	52%
Female	48%
Age	
18 – 30	90%
31 – 45	8%
46 - 60	2%
Education level	
High school degree	5%
Bachelor's degree	37%
Master's degree	58%

Table 1. Demographic table

The survey consisted of ten questions (see Appendix K). The first four questions were general questions about the participants of the study; their age, gender, education level, and the industry the participants work in. The other six questions were more specific, question five asks if the participant has or leases a car with or without connected features. This is important to see if people owning a connected car are more aware of its security. Question six asks the participant if they think that most of the currently sold cars are connected to the internet or not. This question is meant to know the awareness about connected cars being connected to the internet. Questions seven asks the participant if a car connected to the internet would lower or raise the level of car security. Question eight asks if the participant is familiar with the possibility of connected cars being hacked. Question nine asks the participant that assuming a connected car can be hacked would they still buy one without hesitation, with precaution, or would not buy one. The last question asks about the preference of the participant about what kind of car they prefer, connected cars, or "offline" cars.

The participants were recruited online on multiple platforms. First, the Accenture Security team got the invitation to complete the survey via Whatsapp. Following this, the Accenture interns were asked via Whatsapp. The ICT in Business students also got the survey link in the Whatsapp group. The survey link was also shared on Facebook, and LinkedIn. Through this distribution method the age and gender were not predetermined. The participants filled out all questionnaires online, through Qualtrics.com provided by the University of Leiden.

3.5 Interview Analysis

In qualitative research, data analysis takes place at the same time as data collection. Since the process is iterative, the data is analyzed several times and each time the data is better understood.

After an interview, notes are made of the ideas and questions that arise. After this, data is organized and stored. The data is labeled without attaching the participant's names to them and are stored securely in order to maintain confidentiality. Since the interviews were recorded, each of them was transcribed. To interpret the data, a qualitative data analysis software package was used, called QDA miner. After reading a transcript, the themes were identified. These themes were given a name. This procedure is called coding. In qualitative research coding is "how you define what the data you are analyzing are about" (Gibbs, 2007). It is also important not just only label the data, but to find concepts and relations between the data. Notes are were taken during the coding to motivate the choices behind the naming and information that were not expected or surprising were also noted down. This method was used to transcribe and code each interview recording. When all the recordings were transcribed and coded. Recurring themes amongst the interviews were identified as well. After discovering the connections, the analysis describes the links between the themes and patterns that were discovered. These themes and patterns were also compared to existing theory to see if it is consistent or not. In cases where the interview data differed from the theory, a possible explanation about the mismatch was given.

3.6 Survey Analysis

Regarding the survey, the analyses were performed in SPSS, version 23. Furthermore, the percentages for each question was calculated using SPSS, and for questions with important findings pie charts were made to facilitate the visualisation of the data. Moreover, to check the differences within the demographics of age, gender, and education crosstabs were used. Crosstabs showed us whether there is a significant in the participant's response if for example they are male or female.

3.7 Ethical Consideration

No connected car or other device was hacked for the purpose of this thesis, however, some of the interviewed experts have experience in this domain.

Consent was given by all experts to participate in this research, considering that they stay anonymous. Moreover, written information was provided to all parties about the research prior to being interviewed. This was done to let them know exactly why the interview was done and why these questions were asked.

All interviews were voice recorded and consent was given for this by all participants. The participants will remain anonymous even with voice recordings, which will also be confidential.

The transcripts with coding can be found in the Appendix without personally identifiable information.

4. Analysis and findings

4.1 Interview

This chapter is meant to analyze and show the findings from the semi-structured interview and the survey. To analyze the survey crosstabs were used to show the differences between demographics such as age, gender, and education for each question.

After all the interviews the experts gave an in-depth look into the topic. The first question asked the interviewees about their specific jobs, which will not be included here to keep the participants anonymous.

4.1.1 *What is your opinion on the current state of in-vehicle IT security?*

The general impression was that it is not good enough, and manufacturers need to improve their connected car security. Interviewee number 4 was less critical and explained why manufacturers are slow to adopt better security practices: "Legislation and technical solutions are still being written and developed. If you know the car manufacturers, you know that they are very process-oriented, and they need time to adopt new processes. First, they roll out the first version, then they modify this version to make it better, and so on."

4.1.2 *Are connected cars less or more secure than "offline" cars, why?*

Most interviewees said that online connectivity will always increase the attack surface, hence connected cars are less secure than offline cars. However, interviewee four and eight pointed out that while the attack surface is wider for connected cars, the new possibilities introduced like over the air updates might render the overall risk similar.

4.1.3 *Where do manufacturers spend a considerable amount of attention/time/money, and where should they spend more?*

The common answer was that manufacturers invest intensively on functional safety enabling them to have good ratings on crash tests. However, they do not spend enough resources on standardisation and manufacturers should work together to share their knowledge. Another issue was that manufacturers do not involve security professionals from the beginning of a new project, but rather at the end when everything is fixed, thus hard or impossible for the experts to secure the in-vehicle IT system.

4.1.4 *How much attention/time/money do manufacturers spend on IT security in contrast with the previous question?*

Most of them said that manufacturers are becoming more aware of the need for cybersecurity, however, it is not the priority thus they do not spend enough resources on it. Furthermore, it is hard to tell from the outside since manufacturers do not communicate these kinds of details.

4.1.5 *What is the biggest problem in automotive IoT security in 2019?*

The responses to this question were not always the same in this case. The most common answer was that manufacturers do not spend enough on IT security while they are implementing new features at a fast pace. Thus, the complexity of the systems implemented for a modern car prevents manufacturers from implementing effective security measures. Another issue was that automotive car manufacturers do not really have the security requirements written anywhere for the tier 1 suppliers or for the suppliers in general, thus it is very hard for automotive car manufacturers to dictate what security features they would expect from their suppliers. Another issue that emerged is that there are not enough security experts in the automotive industry.

4.1.6 *How did the automotive IoT security change over the last five years?*

The most common answer was related to the Jeep hack in 2015. Before that manufacturers did not care about IT security. When the hack happened, it frightened automotive car manufacturers and they started to invest in IT security capabilities. Another point was that manufacturers moved from operating systems which were not designed primarily for automotive, to an operating system which is already designed for automotive applications.

4.1.7 *What are the weak points of connected cars?*

One of the biggest weak point according to the experts is the interconnectability. All the endpoints that are connected to legacy systems and legacy protocols, systems that weren't developed with security in mind increase the attack surface of a system that is not supposed to be connected. Furthermore, another weak point mentioned was the device aftermarket and remote communication. For example, a Tesla for autonomous driving uses cameras, LIDAR, and sensors. All devices installed on the car that interacts with the external environment can be a potential threat.

4.1.8 *What is the most likely attack vector on a connected car?*

For this question, the common answer was the combination of human factor and external communications. For example, the user of the vehicle connects to an unsecure WiFi, or the user's phone gets compromised, thus infecting the car. In a lot of cases, the owner of the car is the one that wants his car to be 'hacked', to get better performance or to lower the mileage of the car.

4.1.9 *What is the best defense to prevent hacking in general?*

The most common answers were about implementing secure software development practices and following the security by design implementation. Other responses included encryption of the communication bus inside the car, isolation of the ECUs, and smart authentication (biometric authentication).

4.1.10 *What is the best defense to prevent hacking via direct physical access?*

The experts agreed that having physical access (even if the car is locked) is one of the hardest to secure. The common answer was segregation between the critical components. Furthermore, hardware security (e.g. secure boot, hardware cryptography) is also essential to secure the car from hacking via direct physical access. Other responses included having a reliable loud car alarm, and tamper detection in order to detect when there is an attempt to compromise the vehicle's integrity or the data associated with the vehicle.

4.1.11 *What is the best defense to prevent hacking via wireless access?*

The common answer was to use secure wireless communication. It needs to be encrypted, signed, authenticated, and using certificates. Furthermore, it is also important to protect the servers (can be in the cloud), because if the car is safe but the servers aren't the car becomes vulnerable too. Another popular answer was to use distance bounding protocols, meaning the distance between the car and the key-fob is measured, thus when someone tries to record what the key-fob is sending and tries to replay it, the car knows it is not a legit request and the car will not open.

4.1.12 ***What is the best possible solution to mitigate these security risks?***

The common answer was that before doing anything it is important to understand what can happen and what the potential risks are. In other words, manufacturers first need to understand the context, the vehicle they are protecting. Second, manufacturers need to understand the threat landscape, so they can recognize what are they protecting themselves against. Once they understand the context, and the specific threat landscape it's important to protect not only the single components but focusing on the entire vehicle value chain.

4.1.13 *Could vehicular communication systems like Vehicle-to-vehicle or vehicle-to-infrastructure communication pose security risks?*

All the experts agreed that Vehicle-to-vehicle and Vehicle-to-infrastructure communication widens the attack vector, since the car has more sources that can communicate to it, and it is guaranteed that the car can trust them or not.

4.1.14 *Is there a difference in terms of security between the different types of automotive network communications protocols (LIN, CAN, MOST, FlexRay)?*

The experts were consistent, and mentioned the following details: for LIN, CAN, and FlexRay it is very easy to connect and analyze the traffic. To be able to send LIN or CAN messages it is also easy if the attacker can connect to the system. For FlexRay, it is a bit more difficult because it isn't as trivial but it's possible. Nowadays CAN is well known thus it is not an exclusive knowledge. FlexRay is a bit harder to access but it is a public standard, so everyone who wants to manipulate these protocols can learn and experiment.

4.1.15 *Could the encryption of network communication protocol data improve security?*

All the experts agreed that encryption improves security, however not everyone was positive about the feasibility of encryption of communication data. Since encryption complicates the architecture, and because all these cars have never been tested with encryption. Furthermore, encryption takes a load on the processing capacity of small sensors and actuators that have a lack of computing power for these operations.

4.1.16 *All new cars sold in the EEA has an integrated E-call feature which requires a cellular connection, do you think this service is secure?*

Unfortunately, not all experts were familiar with the technology behind this feature. Three of the experts said it is secure, and three said it is not. However, the only expert who had more experience with this feature was certain that it is secure. Furthermore, another expert who was familiar with the technical implementation of the feature explained that the feature is safe because it is one way only communication. When the button is pressed the car calls a verified, and hard-coded number in order to transfer the location data of the vehicle.

4.2 Survey

The survey consisted of 10 questions. The first four questions asked for general information about the respondents. To see whether there were differences between the answers based on demographic differences, crosstabs were used in SPSS. To see these differences, the participants were compared by age, sex, and educational level. The following results were obtained.

4.2.1 *Do you think currently sold cars are continuously connected to the internet?*

The possible answers on this question were, yes, no, or maybe. The results obtained from SPSS showed that there were no significant differences between the answers based on age X^2 (4, N=100)=3.24, p=0.519, gender, X^2 (1, N=100)=1.24, p=0.538, or education level, X^2 (4, N=100)=1.62, p=0.805. For example, a higher percentage of males (39.6%) answered this question with a yes compared to females (32.7%).

4.2.2 *Do you think that a continuous internet connection would raise or lower the level of car security?*

The possible answers on this question were, raise, lower, or no change. The results obtained from SPSS showed that there were no significant differences between the answers based on age X^2 (4, N=100)=2.55, p=0.637, gender, X^2 (2, N=100)=2.18, p=0.336, or education level, X^2 (4, N=100)=0.90, p=0.924. For example, the majority of people (39.7%) with a Master's degree answered with lower, while equal percentage (40.5%) of people with a Bachelor's degree answered with raise and lower.

4.2.3 *Are you familiar with the possibility of hacking connected cars?*

The possible answers on this question were, extremely familiar, very familiar, moderately familiar, or slightly familiar, not familiar at all. The results obtained from SPSS showed that there were no significant differences between the answers based on age X^2 (8, N=100)=13.72, p=0.089, or education level, X^2 (8, N=100)=12.21, p=0.190. However, there were significant differences for gender, X^2 (4, N=100)=12.18, $p<.05$. This is shown from the percentages, as 16.7% of males answered with extremely familiar, while 3.8% of females answered with the same answer. Similarly, 22.9% of males answered with very familiar, 9.6% of females picked the same answer.

4.2.4 *Knowing connected cars can be vulnerable to hacking, would you still buy one?*

The possible answers on this question were, yes, yes but with precaution, or no. The results obtained from SPSS showed that there were no significant differences between the answers based on age X^2 (4, N=100)=2.72, p=0.606, or education level, X^2 (4, N=100)=4.48, p=0.345. However, there were significant differences for gender, gender, X^2 (2, N=100)=9.56, $p<.05$. This is shown from the percentages, as 27.1% of males answered with yes, while 5.8% of females gave the same answer. Similarly, 14.6% of males answered with no, and 28.8% of females picked the same answer.

4.2.5 *Would you prefer to buy a connected car or an offline car?*

The possible answers on this question were, connected, or offline car. The results obtained from SPSS showed that there were no significant differences between the answers based on age X^2 (2, N=100)=3.21, p=0.201, gender, X^2 (1, N=100)=1.09, p=0.296, or education level, X^2 (2, N=100)=1.73, p=0.422. For example, a higher percentage of 31-45 year old's (75.0%) would prefer to buy a connected car, compared to 25.0% who would buy an offline car.

4.2.6 Visualization

Furthermore, answers to some of the questions were also presented in a pie chart below. As well as, the percentage of respondents to each answer were obtained and presented in this paragraph. Question five asked the respondents if they own a car, and if it has connected features or not. Seven percent of the respondents have a car with connected features while 23% of the respondents own a car without connected features. The remaining 70% of the respondents do not have a car. Question six asked the respondents if they think that currently sold cars are continuously connected to the internet, 36% of the respondents said yes, and 46% said maybe. The remaining 28% responded no. Question seven's answers can be seen in Figure 2. 42% of the respondents said that continuous internet connection lowers, while 39% said it raises the level of car security. The remaining 19% said there is no change when a car is continuously connected to the internet.

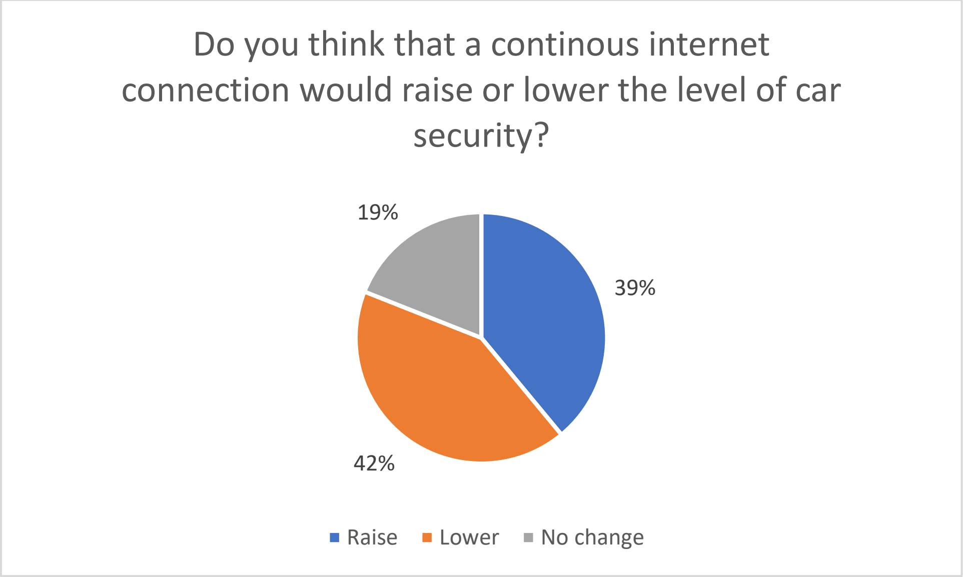

Figure 2. Pie chart representation of question seven

Question eight questioned the respondents about their knowledge about connected car hacking. The results can be seen on the Figure 3.

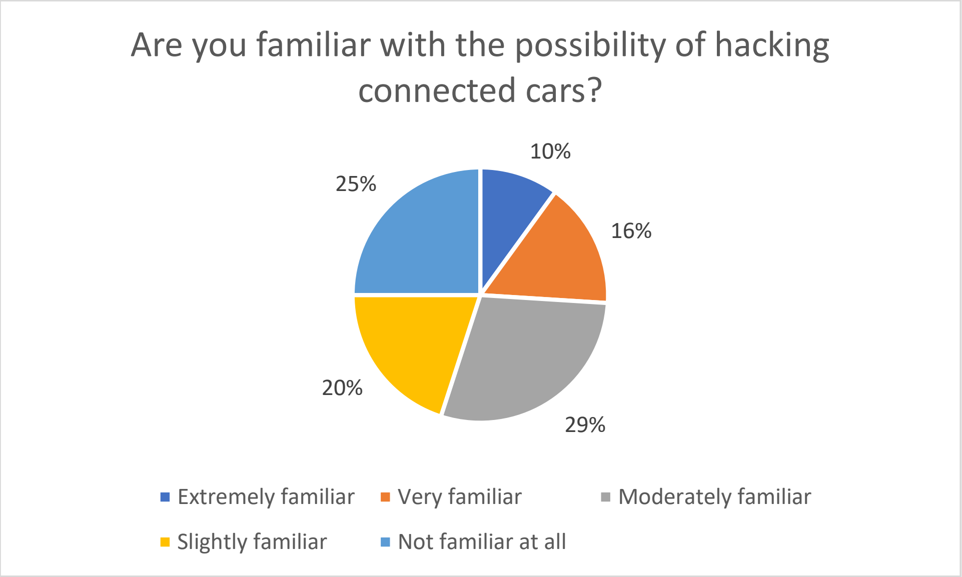

Figure 3. Pie chart representation of question eight

Question nine asked the respondents if they would buy a connected car knowing they can be vulnerable to hacking. 16% of the respondents said they would buy a connected car, and 62% of them said they would buy one, but with precautions. The remaining 22% said they would not buy a connected car.

Question 10 was meant to know the preference of the respondents about connected and offline cars. 55% of the respondents said they would prefer to buy a connected car over an offline car, while the remaining 45% said they prefer to buy offline cars.

5. Conclusion and future work

5.1 Conclusion

From this study, a few conclusions can be drawn. First, connected cars are not secure. They can be hacked, and all experts and research support this. This study offers a few solutions that are already known to experts and possibly some manufacturers, however they are not yet implemented. This is an area that needs to be worked on in the future and needs to be taken more seriously as car security is crucial for everybody. Since many things intertwine with each other, the improvements must be made in small steps before the security level can be stabilized.

Second, from the survey, it is evident that connected car security has low awareness. This means that most people are not aware of the risks of a connected car or are not even aware that there are risks. In the future, experts should not only prioritize augment connected car security but also on raising awareness about the risks and promoting safe car usage. After all, a car cannot be safe without being secure.

5.2 Future work

The next step in this research would be to implements some of the proposal to see if they work in real life. The proposals could also be improved by experts to fit better the car manufacturer's needs. For example, adopting an offensive mindset by assuming that each component in the system may be compromised at some point by an attacker. Every component should verify minimal level of trust in every other component. Furthermore, use segregation between the critical components, thus limiting the extent of the problems that could occur.

6. Discussion and limitations

6.1 Discussion

This thesis examined the current state of security in connected cars. Connected car security is a new topic that emerged in 2015, and it is still not mature. This industry is still emerging, with too few people that have actual experience in this domain. This is due to the complexity of the industry. People who are skilled in IT security, in embedded systems, and know about the car industry are very hard to find. Legislation and standards are currently in progress. All these are going forward with a lot of work which would require a lot of experts, which the industry lacks. This research provides new insights into the risks of connected cars. This chapter is meant for discussion of concrete directions for increasing security, based on the literature review, the expert interviews, and the survey.

During the interviews, the experts gave an in-depth look into the topic. When asked what their opinion was on the current state of in-vehicle IT security, the first interviewee's impression is that this level varies across brands, the premium brands tend to invest more in security. However, there is no standard when it comes to what features they should have already implemented thus, everybody is going at their own pace. The expert pointed out that at this day and age automotive manufacturers cannot produce cars without cybersecurity in mind, however everything is at the beginning, and unfortunately, they are doing 'bolt-on' security rather than security by design. Interviewee number five said that it is still an emerging market. For automotive security, in general, the efforts started in 2015, after the Jeep Cherokee hack. Before that, the automotive industry was not interested in security for vehicles even if they are using all the protocols like the CAN bus that was created in the 1980s. A major focus for manufacturers is to have a short time to market and they did not consider the risk of cybersecurity because before 2015 there was no proof of a working remote attack. After that happened the cybersecurity in the automotive industry started to improve. From a regulation's perspective, the senator of Massachusetts in the United States called EJ. Markey requested a report on the current state of connected cars. Most of the manufacturers didn't reply which is a demonstration about the feeling on the market. This is the most reliable information that we have on the market because the automotive manufacturers don't want to reveal what they are doing. This paper (Markey, 2013) was also discussed in the literature review. All the other interviewees were similarly concerned about the state of in-vehicle IT security.

The general opinion about the security of connected cars versus offline cars was that older cars that use all mechanical instruments will be more secure. The reason is simple, connected cars started to use radio wave features. Not just internet connectivity, but Bluetooth, remote keyless entry, remote key fobs, digital radio, and RDS. When the cars were purely mechanical, CAN bus was not the standard choice. In the transition when CAN bus, or LIN bus first appeared, attacks became possible on the bus itself (Thing & Wu, 2016). An interviewee mentioned that at that time, the technology was so new that the tools which we have available right now were not available for an average person on the street. Execution of any attack was very expensive, and it was not worth it. No one really thought about that. The information was hard to get because the internet did not exist as we know it today. However, another expert explained that although we can see that connected cars have a wider attack surface, to update software it is indispensable to be network connected. Before the cars were connected to the network, no one wanted to hack cars, but a physical attack was still as easy as today. So, if someone gets under a car, connects to the car via the wires and starts sending malicious messages, the car doesn't have to be network connected. And like in old movies, where they cut the brake wire, the same type of attack is possible today through the IT system.

From the survey, it was evident that not all respondents share the same view as the experts did as 39% of respondents said that continuous connection to the internet would raise the security of a car, with 42% saying that it would lower the security. The remaining 19% responded with no change to the level of car security, which could mean that they are not sure what the effects of continuous internet connection would be on the security of the car.

Expert number eight had a remark about the awareness of consumers about in-vehicle IT security. Although the European New Car Assessment Programme (Euro NCAP) was founded in 1997 and is meant to test the safety of new vehicles, there is no assessment program for the embedded IT security system of new cars. For this reason, it is hard to know which model from which manufacturer is more secure than the competition. Although 78% of the survey respondents would buy a connected car knowing that these cars could be vulnerable, however from this group 62% would only buy one with precautions. When asked if they prefer connected or offline cars, 55% said they prefer connected cars, while 45% prefer offline cars. These data indicate that although most consumers would buy a connected car with precautions, 45% of them prefer to buy an offline car over a connected car. However, from other questions in the survey, it is also possible that most respondents in the survey are not aware of the dangers of a connected car. The results from the survey also show that 70% of respondents do not own a car, which further demonstrates the possibility that respondents would not be aware of the dangers of connected cars.

When the experts were asked about possible solutions to prevent connected car hacking the suggestions were mixed. The experts highlighted that connected car systems are very complex with more than 100 million lines of code. For this reason, the investment that manufacturers should do is to maintain the supply chain, and invest in secure software development, and monitor and manage the risk in a more formal way. Another expert explained that this all starts with security by design. When software is meant to have good security, it should be deployed having proper monitoring in place to be able to detect when someone is being hacked, and knowing how to respond to it with proper incident and response. Furthermore, if there are regular backups and a restore program, even if something happens, and it is detected, the car can get back to the default operating state if the restoration can be done quickly. Another expert explained that companies are increasingly better in securing the debugging access of the motherboard and system on-chip devices. Meaning that before the car leaves the factory all the jtag ports, and any other debugging interfaces are closed, and they make sure that without getting the car back to the factory, or without triggering some function that only a few dealerships are advised to make, it is not possible to make modifications to the car. These precautions would have made it harder or even impossible to exploit the Jeep Cherokee by Charlie Miller and Chris Valasek in 2015. Similarly, Becsi and colleagues (2015) found that the first problem with ECUs is that they are not protected by reverse engineering by disassembling or circuit probing. Another issue that they have found is the presence of backdoors. The developers working on the ECU might leave a backdoor open for testing purposes, negligently or in an intended way. This issue seems to be widespread since Checkoway and colleagues (2011) also found services for file transport and a screen-oriented text editor in the ECUs which should be removed since these programs make it easier for an attacker to exploit the ECU. Another issue is the possibility to reflash the ECU by a third party. Like any computer, the ECU has software with different settings, and these can be changed to alter the performance, driving characteristics, or it can be remapped with malicious intents.

When asked about the best defense to prevent hacking via direct physical access, the first expert explained that firms like Arilou, Argus, and Enigmatos are focusing on creating a so-called hardware fingerprinting where they are using analogue ways and specific physical phenomenons which they can observe on the “wire”. If there is a topology change or if there is something suspicious, for example, a new signature of device appears, most likely there is an anomaly or that someone plugged in a tool like a raspberry pi. Detection is essential to be able to prevent an attack in the future. Unfortunately, this is not yet the default technology that manufacturers use. Expert number eight suggested that the OBD port should be isolated from the critical parts of the CAN network. In newer cars there is a gateway after the OBD port, so even if someone plugs in their device, he cannot talk to the ECUs that control the engine, brakes, or the gears. Only diagnostics’ messages can get out. Although this is an easy way of securing the OBD port, it is not a general practice yet. This was proven by Checkoway and colleagues (2011); since 2004, all new cars in the US are compatible with the SAE J2534 “PassThru” standard which is an API that offers an interface to communicate with the vehicle’s internal buses. This standard has two vulnerabilities. First, if the attacker and the PassThru device are on the same WiFi network and the PassThru is connected to the car, it can give access to the reprogramming of the car. The second problem is the PassThru device itself. The researchers were able to implant malicious code to the device, and thus it can infect the car that is connected.

Experts were also asked about the best defense to prevent hacking via wireless access. The experts agreed that wireless communication needs to be encrypted, signed, with authentication and certificates. It is also important to protect the servers because if the car is safe, but the servers are not the car becomes vulnerable too. Expert number one and eight gave a solution to stop replay attacks by using the key-fob of the vehicle. These keys that the owners can just keep in their pocket, open the car and start the engine are vulnerable to relay attacks, and the attacker can just start the car in the driveway while the keys are inside the house of the owner. They pointed out that by using distance bounding protocols, meaning measuring the distance between the key-fob and the vehicle could solve the relay attack possibility. When using a distance bounding protocol it is not going to work, because the combination of the signature and the physical phenomenon is not valid. Another option might be establishing a pool based physical unclonable function-based keys, where each key would have a unique and unclonable chip or small device which will make it irreplaceable. Expert number five gave a more general approach. They explained that there are a lot of security controls that can be included, but manufacturers should start by analyzing the attack surface, and possible risks, and understanding if the security control that they implemented are strong enough. Furthermore, the best defense that you can have managing the risk is also doing penetration testing and understanding what are the possible scenarios that could happen. Regular penetration testing is also the best defense in this scenario. In contrast, Tillich and Wojcik (2012) reported that using a distance bounding protocol is not the best option. If the third-party key-fob fakes an uplink CRC error, this forces the car to send a “Repeat Last Response” command. The attacker can use the extra time for the repeated response to get the actual response from the genuine key-fob. They proposed a more secure version. This remote attack could be protected against with the measurement of the communication delay of the key fob by the vehicle and by abandoning the mechanism of requesting a repeat of the key fob’s response in answer to a CRC error. Instead, the whole sequence of commands and responses should be repeated when a CRC error is encountered. This gives the attacker no time to hide the extra communication delay introduced by the third-party reader and key fob (Tillich & Wojcik, 2012).

6.2 Recommendations and solutions

The following recommendations are aimed for the three involved parties, governments, manufacturers, and users. Using these recommendations improves the general security level and promotes a better security culture.

6.2.1 Recommendations to governments

- Create regulatory bodies that will engage manufacturers and research groups alike to establish and maintain a universal standard for vehicle cyber security.
- Establish penalties for the manufacturers that are non-compliant.
- Establish security threat intelligence and vulnerability sharing programmes to improve collaboration within the automotive ecosystem and encourage consistent and standardized approaches to cyber defense.
- Enforce Privacy by Design principles. Privacy must be addressed and include up front within the design of the service function. Regulations such as GSPR are only part of the solution.

6.2.2 Recommendations to manufacturers

- Track emerging standards from organizations like RITA, SAE, ISO, etc. and consider joining standards bodies and groups to better align business objectives and security.
- Assume that multiple adversaries exist, so understanding emerging threats and continuous intelligence sharing is necessary across the automotive ecosystem.
- Adopt an offensive mindset – assume each component in the system may be compromised at some point by an attacker. Every component should verify minimal level of trust in every other component.
- Ensure secure connectivity, segregation, and access controls between non safety and safety critical systems.
- Establish security as an end to end model. The vehicle is only part of the battle – backend systems and services can be exploited to gain access to the vehicle through trusted channels. Adopt a policy of aggressive pen testing at all levels.

6.2.3 Recommendations to users

- Block all communication ports by default and allow only the traffic of those ports that are relevant (whitelisting).
- Use strong password and change the default credentials (both username and password)
- Do not allow promiscuous, automatic connection to unknown Wi-Fi hotspots.
- Regularly update the product and use only manufacturer approved firmware.

6.3 Limitations

The findings presented in this study should be considered in light of their limitations. First, the discussed vulnerabilities, and possible solutions were not tested on real cars. Second, question seven of the survey could have been misinterpreted by some respondents as some people have reported that after completing it, they have realized that they misunderstood the question. This could mean that their response is not valid and could show that more people think that a connected car lowers the security in comparison to the 42% that the results currently show.

References

Accenture. (2016, April 28). Consumers Willing to Pay Extra for In-Car Technologies, Accenture Research Reveals. Retrieved from https://newsroom.accenture.com/news/consumers-willing-to-pay-extra-for-in-car-technologies-accenture-research-reveals.htm

Bajaj, R. K., Rao, M., & Agrawal, H. (2018). Internet Of Things (IoT) In The Smart Automotive Sector: A Review. IOSR Journal of Computer Engineering,36-44.

Becsi, T., Aradi, S., & Gaspar, P. (2015). Security issues and vulnerabilities in connected car systems. 2015 International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS). doi:10.1109/mtits.2015.7223297

Berkowitz, J. (2010, October/November). The History of Car Radios. Retrieved from https://www.caranddriver.com/features/a15128476/the-history-of-car-radios/

Bloomberg, L. D., & Volpe, M. (2008). Completing your qualitative dissertation a roadmap from beginning to end. SAGE.

Charette, R. N. (2009, February 01). This Car Runs on Code. Retrieved from https://spectrum.ieee.org/transportation/systems/this-car-runs-on-code

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., . . . Kohno, T. (2011). Comprehensive experimental analyses of automotive attack surfaces. Proceedings of the 20th USENIX Conference on Security,sec'11, 6-6. doi:http://dl.acm.org/citation.cfm?id=2028067.2028073

Coppola, R., & Morisio, M. (2016). Connected Car. ACM Computing Surveys,49(3), 1-36. doi:10.1145/2971482

Edward, M., J. (2015, February). Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk (Rep.). Retrieved https://www.hsdl.org/?abstract&did=762359

Fleming, B. (2014). An Overview of Advances in Automotive Electronics [Automotive Electronics]. IEEE Vehicular Technology Magazine,9(1), 4-9. doi:10.1109/mvt.2013.2295285

Fleming, B. (2014). An Overview of Advances in Automotive Electronics [Automotive Electronics]. IEEE Vehicular Technology Magazine,9(1), 4-9. doi:10.1109/mvt.2013.2295285

Francillon, A., Danev, B., & Capkun, S. (2010). Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars. IACR Cryptology EPrint Archive}.

Gibbs, G. (2018). Analyzing qualitative data. Los Angeles: SAGE.

Giffi, C. A., Vitale, J., Robinson, R., & Pingitore, G. (2017, January 23). The race to autonomous driving Winning American consumers' trust. Retrieved from https://www2.deloitte.com/insights/us/en/deloitte-review/issue-20/winning-consumer-trust-future-of-automotive-technology.html

Greenberg, A. (2015, July 21). Hackers Remotely Kill a Jeep on the Highway-With Me in It. Retrieved from https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

Greenough, J. (2016, April 29). THE CONNECTED CAR REPORT: Forecasts, competing technologies, and leading manufacturers. Retrieved from https://www.businessinsider.com/connected-car-forecasts-top-manufacturers-leading-car-makers-2016-4-29?international=true&r=US&IR=T

Grymek, L., Singh, S., & Pattipati, K. (2007). Vehicular dependence adds to telematics allure. IEEE Potentials,26(2), 12-16. doi:10.1109/mp.2007.343053

Hellberg, J. (2013). Remotely access real-time system in a modern car. Retrieved from https://pdfs.semanticscholar.org/ad91/f9f53af3c2b4351fad1efe0d5c33fbcb6be7.pdf

Hoppe, T., Kiltz, S., & Dittmann, J. (2008). Security Threats to Automotive CAN Networks – Practical Examples and Selected Short-Term Countermeasures. Lecture Notes in Computer Science Computer Safety, Reliability, and Security,235-248. doi:10.1007/978-3-540-87698-4_21

Hung, M. (2017). Leading the IoT - Gartner Insights on How to Lead in a Connected World. Retrieved from https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

Johansson, K. H., Törngren, M., & Nielsen, L. (2005). Vehicle Applications of Controller Area Network. Handbook of Networked and Embedded Control Systems,741-765. doi:10.1007/0-8176-4404-0_32

Keen Security Lab of Tencent. (2016, September 20). Car Hacking Research: Remote Attack Tesla Motors. Retrieved from https://keenlab.tencent.com/en/2016/09/19/Keen-Security-Lab-of-Tencent-Car-Hacking-Research-Remote-Attack-to-Tesla-Cars/

Kollaikal, P., Ravuri, S., & Ruvinsky, E. (2017). Connected cars (Rep.).

Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., . . . Savage, S. (2010). Experimental Security Analysis of a Modern Automobile. 2010 IEEE Symposium on Security and Privacy. doi:10.1109/sp.2010.34

Koster, A., Ahlemann, D., Hirsh, E., & Viereckl, R. (2016, September 27). Connected car report 2016: Opportunities, risk, and turmoil on the road to autonomous vehicles. Retrieved from https://www.strategyand.pwc.com/report/connected-car-2016-study

KPMG. (2017). The Connected Car is here to Stay Driving digital transformation in the automotive industry. Retrieved from https://assets.kpmg/content/dam/kpmg/nl/pdf/2017/sector/automotive/the-connected-car-is-here-to-stay.pdf

Markey, E. (2013, December 02). As Wireless Technology Becomes Standard, Markey Queries Car Companies about Security, Privacy. Retrieved from https://www.markey.senate.gov/news/press-releases/as-wireless-technology-becomes-standard-markey-queries-car-companies-about-security-privacy

McCarthy, N. (2015, January 27). Connected Cars By The Numbers [Infographic]. Retrieved from https://www.forbes.com/sites/niallmccarthy/2015/01/27/connected-cars-by-the-numbers-infographic/#1c6006710288

METHODOLOGY | meaning in the Cambridge English Dictionary. (n.d.). Retrieved from https://dictionary.cambridge.org/dictionary/english/methodology

Miller, C., & Valasek, C. (2015, August 10). Remote Exploitation of an Unaltered Passenger Vehicle. Retrieved from http://illmatics.com/Remote Car Hacking.pdf

Oorni, R., & Goulart, A. (2017). In-Vehicle Emergency Call Services: ECall and Beyond. IEEE Communications Magazine,55(1), 159-165. doi:10.1109/mcom.2017.1600289cm

Rouf, I., Miller, R., Mustafa, H., Taylor, T., Oh, S., Xu, W., . . . Seskar, I. (2010). Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study. In Proceedings of the 19th USENIX Conference on Security(USENIX Security'10, p. 21). Washington, DC.

Ryan, M. (2013). Bluetooth: With Low Energy Comes Low Security. Retrieved May 9, 2019, from https://www.usenix.org/conference/woot13/workshop-program/presentation/Ryan

Thing, V. L., & Wu, J. (2016). Autonomous Vehicle Security: A Taxonomy of Attacks and Defences. 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). doi:10.1109/ithings-greencom-cpscom-smartdata.2016.52

Tillich, S., & Wojcik, M. (2012). Security Analysis of an Open Car Immobilizer Protocol Stack. Retrieved from https://research-information.bristol.ac.uk/files/9588694/ACNS2012_paperID_49_camera_ready.pdf

Wolf, M., Weimerskirch, A., & Paar, C. (2004). Security in automotive bus systems. Retrieved May 9, 2019, from https://www.researchgate.net/publication/228707984_Security_in_automotive_bus_systems.

Young, K. S. (1998). Internet Addiction: The Emergence of a New Clinical Disorder. CyberPsychology & Behavior,1(3), 237-244. doi:10.1089/cpb.1998.1.237

Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2018). The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. IEEE Internet of Things Journal. doi:10.1109/jiot.2018.2847733

Appendix A

Interview transcript A

2. What is your opinion on the current state of in vehicle IT security?
Research results have drawn attention to the importance of the topic, it is being addressed by the industry.
About the current state of vehicular IT security, we can see that there are research groups that have found vulnerabilities. We can also see that it's relatively easy to steal a car, but we never saw a real-life example of accident caused by a hacked connected car. There are only rumors about it. However, all the manufacturers that I talked to considers IT security as a real problem that needs to be solved, but it's not top priority yet. It is not a direct threat, so it's not like if a new car rolls out the dealership and gets hacked, but it's not impossible so we need to work on it. All my colleagues, and clients has the same point of view: we need to take this seriously and do something about it. This wasn't always the case. Since the Jeep hack in 2015 which became widely known and caused a big financial impact due to the recall of 1.4 million vehicle, manufacturers started to care because no one wants to recall millions of vehicles. Legislation and technical solutions are still being written and developed. If you know the car manufacturers, you know that they are very process oriented, and they need time to adopt new processes. First, they roll out the first version, then they modify this version to make it better, and so on. Furthermore, it is very hard to formulate the requirements. In this sense I would like to steer this to the IT security part. Because people who work in IT security say that using experimental knowledge it's not possible to defend with requirements. I think this makes things a bit harder.

3. Are connected cars less or more secure than "offline" cars, why?
While the connectivity increases the attack surface, it enables easier updates, so the overall risk may be similar.
We can see that connected car has a wider attack surface, however to update software it is indispensable to be network connected. Obviously, it needs to be done properly, but I think today's IT methods are good enough to make a wireless communication secure. Obviously, before the cars being connected to the network, no one wanted to hack cars, but a physical attack was still as easy as today. So, if someone gets under a car, connects to the car via the wires and starts sending malicious messages, the car doesn't have to be network connected. And like in old movies, where they cut the brake wire, the same type of attack is possible today through the IT systems.

4. Where do manufacturers spend a considerable amount of attention/time/money, and where should they spend more?
The current focus seems to be on defining security standards, processes and requirements, which is the first step. Secure implementation and verification is still gaining momentum.
Obviously, it's important for car manufacturers to sell the most vehicles, thus they'll focus on what the consumers need, mostly things that can be seen and interesting. At the same time, we hear about IT security problems with cars more and more, and it is also important for manufacturers that their cars don't appear in this news. I believe that there is a good balance between the fact that the manufacturers first goal is not to make service costs low, but in car

reviews this data becomes public so they also spend time on this particular issue. It's the same with vehicular IT security, it's not their first priority to make it secure, but it needs to be secured to avoid bad reviews. Furthermore, the more sophisticated features they built in a car, the more users ask the question is this safe? In the US this became an issue faster than in Europe, but it is now also established in Europe.

5. How much attention/time/money do manufacturers spend on IT security in contrast with the previous question?
The importance of IT security is definitely recognized, perhaps not yet as the most
urgent topic.

6. What is the biggest problem in automotive IoT security in 2019?
There are not enough security experts in the automotive industry.
The biggest problem for me is that there is not enough specialists. The whole vehicular IT security started in 2015, when the first Jeep hack happened. Before the Jeep hack car hacking was only a theoretical possibility. This industry is still emerging, with too few people that have actual experience in this domain. This is due to the complexity of the industry. To have someone who is skilled in IT security, in embedded systems, and also knows about the car industry is very hard to find. Legislation and standards are currently in progress. All these are going forward with a lot of work which would require a lot of experts, but there aren't that many.

7. How did the automotive IoT security change over the last five years?
Automotive security was unknown five years ago. The Jeep hack frightened automotive manufacturers and they started to assemble capabilities to work in IT security. Another reason why automotive IoT security wasn't evolved is because cars at that time did not have that many connected features. Playing with the OBD-II port was already a well know practice for chip tuners, and of course mechanics but it wasn't used for malicious activities, thus security wasn't really required. Nowadays, there is an industry for this, and available materials to learn it.

8. What are the weak points of connected cars?
I don't think you can really know it yet. The vulnerabilities that were used in the past, are all fixed now. The core concept of IT security is to keep everything safe using the same level of security, because the weakest link will be attacked first. The weakest links were already attacked by researchers, these vulnerabilities were fixed, and new ones appears. For this reason, it is hard to formulate what are the weak points, since if we would know manufacturers would spend more money in that affected area and it would be alright.

9. What is the most likely attack vector on a connected car?
The Jeep was attacked through the telematics system, I suppose the manufacturers of telematics systems fixed the vulnerabilities. In IT security human factor is usually the weakest which has the most attacks, probably this is the same for vehicular IoT security too. For example, the user of the vehicle connects to not secure WiFi, or the user's phone gets compromised, and thus infecting the car. In a lot of cases the owner of the car is the one that wants his car to be hacked. To get better performance or to lower the mileage of the car.

10. What is the best defense to prevent hacking in general?
If we fix a weak point there will be a new one. Usually defense in depth, when we defend in many layers, is used. The car is globally defended, especially its external communication channels. Definitely a global and systematic approach is needed.

11. What is the best defense to prevent hacking via direct physical access?
If someone has physical access to the car, then tamper detection. Tamper detection is the ability of a device to sense that an active attempt to compromise the device integrity or the data associated with the device is in progress; the detection of the threat may enable the device to initiate appropriate defensive actions. Thus, critical components are protected with tamper detection.

12. What is the best defense to prevent hacking via wireless access?
The same approach that is used for a laptop or a smartphone. This is a regular IT problem about how to secure wireless communication. It needs to be encrypted, signed, authentication, certificates. So, use only secure communication channels. But it is also important to protect the servers (can be in the cloud), because if the car is safe but the servers aren't the car becomes vulnerable too. End-to-end protection is needed everywhere. This is also a traditional IT problem.

13. What is the possible solution to mitigate security risks?
I cannot say anything concrete, but good design, implementation and verification is the key to good security. I am working in testing and it is important to not only test what is written down, but to test if the whole system is well thought through.

An ISO standard is also in development. Like with functional safety there is now standard to say what to do so the car won't break. Here too, it is not possible to write down that this and this technology must be used to be secure. However, it can be advised what kind of development process needs to be accomplished, what kind of tests are required, and then we hope it will be secure. This can only be done on process level. All the standards are moving towards this idea. The standard should come out soon, let's say next year, but this still won't give the technological solutions about how to protect the cars, but more about how to work to cover all the vulnerabilities.

Should cyber security testing by a third party become obligatory to all manufacturers?
I think it is useless to centralize this, because manufacturer's interest is also to be secure, and researchers are also motivated to find vulnerabilities. All the bigger vulnerabilities in the past were found by researchers because they were interested and when they succeeded they got fame. I think this model is still working. And with NCAP if a car has a bad rating, it can still be sold, but consumers won't buy it. This mechanism also works here. I'm also worried that if some critical vulnerabilities come to light, people will only talk about that, and will not buy modern cars. This is huge risk for manufacturers, because if there is a fatal accident due to hackers and the lack of vehicular IoT security, then it will setback the development of autonomous cars. I think this is an important point why car manufacturers need to take security seriously. Third party testing is possible to make it mandatory, but most manufacturers and suppliers are already using third parties to inspect/pen test their products. There are already service providers like this. So, I think that for now, centralization would be unnecessary.

14. Could vehicular communication systems like Vehicle-to-vehicle or vehicle-to-

infrastructure communication poses security risks?
Obviously when there is a communication going on there is a risk. There are a lot of questions about V2V and V2I. Especially privacy concerns are important. For example, how can a car identify itself that it's a real car and later one this could be searchable if something bad happens, thus accountability needs to be assured. However, if there is no problem, the cars location shouldn't be readable to anyone. Although CCTV cameras are already on the roads and it can see the license plate, so V2I just makes it easier.

Is V2V or V2I more difficult to implement in terms of security?
The question is the same for both: Who can access the system? If I buy a car I can initiate V2V communication. If it's my own car I can do anything with it, if I can hack it, it will communicate with other cars the way I programmed it. With infrastructure at the beginning it will be harder. To hack a traffic light is harder, already in terms of accessibility, because I cannot buy a traffic light system. At the same time, we know that the infrastructure of a mobile network isn't impossible, so someone can install his own base station. With this aspect there isn't that much of difference between V2V and V2I, and I think both have problems.

15. Is there a difference in terms of security between the different types of automotive network communications protocols (LIN, CAN, MOST, FlexRay)?
I have experience with LIN, CAN, and FlexRay, and less with MOST, but MOST is an optical network, hence physically hard to access. If I cut the optical cable there is a problem. For LIN, CAN, and FlexRay it is very easy to connect and analyze the traffic. To be able to send LIN or CAN messages is also very easy if I can connect to the system. For FlexRay it is a bit more difficult because it isn't as trivial but it's definitely possible. Nowadays CAN is well known thus it's not an exclusive knowledge. FlexRay is a bit harder to access but it is a public standard, so everyone who want to manipulate these protocols they can learn and do whatever they want with it.

Would a new protocol solve this issue?
Automotive Ethernet is becoming widespread. It is a new standard, and although security wasn't the reason why, but it is harder to have the same easy access as CAN or LIN has. It is more difficult but not impossible. It is still possible to connect to the ethernet port, analyze it and then it is possible to understand what is happening. However, in the real world there are ways to be protected on the ethernet protocol thanks to the IT community. While on CAN with 8 byte we cannot do real cryptography, because each message is too small, but on ethernet it is not a problem, messages can be encrypted. In this sense it is a big improvement.
Yes. CAN is widespread and widely known, therefore most likely to be attacked. LIN is only used for relatively harmless equipment. FlexRay is more complex, therefore more difficult to manipulate. MOST uses an optical cable, which makes it more difficult to tamper.

16. Could the encryption of network communication protocol data improve security?
Yes, when encrypted it's better, it's undisputable, but it's needing to be done correctly. Because the messages being encrypted alone isn't secure. The whole system needs to be re-taught, redesigned, and tested. There can be non-trivial design faults with non-trivial implications. I heard one story, it is completely public, that the message was properly encrypted, but it turned out that the body of the message can be accessed from another place, and it had small unique data, thus easy to reverse engineer them.

Obviously, manufacturers are trying to make everything as cheap as possible, but they also want to make their cars secure. I, as a supplier, and the manufacturers too, they cannot say that to save 1 euro we take into account security, so I think they'll invest the required amount of money. It's another matter that encryption can be technically challenging or not possible. So, if there is a battery sensor, which is always on and checks the state of the battery even when the engine is turned off, in this case the consumption also needs to be considered. We cannot afford to drain the battery of the car to have encryption everywhere. Nonetheless, security needs to be done in a smart way, where the risk is big enough it needs appropriate attention. I believe manufacturers and the security community is aware of this.

17. All new cars sold in the EEA has an integrated E-call feature which requires a cellular connection, do you think this service is secure?
I’m not familiar with the details, but I see no safety issue. Some privacy issues have been raised. The fact that the car initiates a call when there is an accident, is not a problem. If the car can be contacted, so someone can call the car when there is no accident and can turn on the microphone, that is a big problem. But I assume that there is a solution to this, but I don't know how this works.

18. Would you like to add something?
I believe that the strict process-oriented approach used in the automotive industry has the potential to ensure automotive security on the long term. The IT industry could also learn from the automotive industry in this regard, as many of the security incidents would have been preventable by better processes.

Appendix B

Interview transcript B

2. What is your opinion on the current state of in vehicle IT security?

It's still an emerging market of course. I think that for automotive security in general the efforts started in 2015, after the Jeep Cherokee hack. Before that the automotive industry was not interested in security for vehicles even if they are using all the protocols like the CAN bus that was created in 1980s and so on. The major focus for manufacturers is to be time to market and they didn't consider so much the risk on cyber security because nobody before 2015 demonstrated a remote attack. After that happened the cyber security also in the automotive industry and the manufacturers improved. They started to take action on that. This is demonstrated also from the job advertisements online. You can see that Ford for example is looking for cyber security for automotive, Porsche I see some job advertisement about that and so on. I think they started to have some concern around the cyber security and how to address that. By the way there is also, from regulation perspective, that there are senators' initiatives that are taking in place. I don't know if you heard about senator EJ. Markey of Massachusetts who requested a report on the current state of connected cars. Most of the manufacturers didn't reply ad that is a demonstration about what is the feeling on the market. This is the most reliable information that we have on the market, because the automotive manufacturers don't want to reveal what they are doing. The lack or the security that they implement, because I still think that it is still immature, but they are doing some steps forward in that.

3. Are connected cars less or more secure than "offline" cars, why?

It's not a concept of which one is more secure or not, because there is a concept in information security that only a disconnected computer is more secure and isolated. But even for a disconnected computer by the network there are also attack like Tempest. This attack can capture the frequency of the screen and based on this you can get the text which is displayed to the user. So, it is not a matter of is it online or offline. Of course, if it is online the attack surface increasing and there are more risks. But I think that the only way to have a more secure product is to focus on secure software development lifecycle and analysis of the attack pattern. We are in a connected world, so you cannot imagine now that your car is offline. Because you have the key that you can open remotely your car. You have device aftermarket that you will put in your car, for example an insurance company to see how many miles you are doing and your driving style. The needs are evolving, and we cannot think about an offline car anymore, so I think that we cannot think about offline car.

4. Where do manufacturers spend a considerable amount of attention/time/money, and where should they spend more?

I can tell you that in general manufacturers they are spending a lot of time and money on human interaction with the device which can be a car, the infotainment system, and usability. I think they should spend more time also to consider the security and what are the risks, so understanding at least the attack surface and the risk of the device itself, and the potential harm to the end user. I think they still need to focus on that and based on that they need to pay attention about the attack surface like I said and more attention on the supply chain, and to better understand and formalize the risks. Based in the risks evaluate how to improve their processes.

5. How much attention/time/money do manufacturers spend on IT security in contrast with the previous question?
That is a good question because nobody is telling you that. The only data that are publicly available are the one from Massachusetts senator. I don't think that there is an answer on how much time or money they spend on. If I can suggest you, do you know BSIMM? It is a maturity model for security, and you can find a comparison between the maturity in different verticals. I don't remember if there is also automotive, but there is finance vs. healthcare. I remember that there were also manufacturers in general, I don't know if there is automotive. You can find some spider charts that will let you understand the difference between the verticals.

6. What is the biggest problem in automotive IoT security in 2019?
The biggest problem is that the manufacturers they don't invest so much in security so far, and the biggest problem of IoT security is that there is a lack of security. Do you remember the Nissan leaf hack? There was a mobile application to manage the climate system of the car, and as an authentication system between the app and the car there was the serial number of the car that you can find under the car. So, it is a weak authentication system, and with that application looking under the car you can put this information in your mobile application and you can change the climate of the car itself. It is a poor implementation of the mobile app that was connected to the car. There was other hack for the remote key that you can open the car with and there was a problem that you can clone the key, and so on. I think the manufacturers should spend more attention on the interaction that they have with the car. This demonstrates that they lack about the risk identification and the attack surface analysis.

7. How did the automotive IoT security change over the last five years?
For sure from the Jeep Cherokee hack in 2015, there was a little bit of more awareness, and again the initiative from the senator Markey demonstrated that there are some steps forward, and also companies like ford, Porsche they have job postings about cyber security. This demonstrated that there is more attention at least from some of the manufacturers. I don't know what the real maturity of the market is, and unfortunately these kinds of information I am not shared. I think it is improving but I don't know by how much. I did some work for big manufacturers, but it was more related to infotainment system. We found some issues, like DDOS attack, injection and so on. I can tell you about one manufacturer, they concerned with the interaction of the infotainment system with the CAN bus, but they told me that they have a kind of isolation firewall between the critical components in the system that prevent some malicious message to be sent to the ECU. So, there is some attention, but I cannot quantify it.

8. What are the weak points of connected cars?
Weak point of connected cars is the device after market and remote communication that they have. For example, a Tesla for autonomous driving you have camera, LIDAR, sensor. Imagine that one of the sensors you can manipulate, or you can freeze an image and so on. You can really have the life of the passenger. All the device you install on the car that is interactive with the external environment can be a potential threat. And all the wireless communication

that you have with the car in and out can be a very potential issue for the safety of the drivers itself. I think these are the main weakest points. One, the device aftermarket that you are putting in the car with the related risk. Second, the communication between the car and the environment with the sensor that they have and is becoming more sensitive with autonomous driving techniques that they are implementing Tesla and the others. Third, wireless communication, Bluetooth, ZigBee whatever.

9. What is the most likely attack vector on a connected car?
The device aftermarket will be easy because you can also have a rogue mobile application or rogue device that you can put in the car. Imagine that you are bringing your car to the mechanic and they have an old computer and they are connecting it to your car. Maybe there is a malware that can infect your car, or something like this. They can put a timer that after three days and you are above the speed of 120 the car stops on the highway. The OBD-II port is very sensitive. There are studies that we are making internally, so I can't share too much. And of course, external wireless communication.

10. What is the best defense to prevent hacking in general?
As you know, nothing is secure. Of course, the scope of cyber-security is to decrease and manage the risk. If a design is done in the right manner and the risk is managed in good manners the probability of that a bad event can happen is low. But as you know, in a connected car there are more than 100 million lines of code, so it's very complex. The investment that the manufacturer should do is to maintain the supply chain, and invest a bit more in secure software development, and monitor and managing the risk in a more formal way.

11. What is the best defense to prevent hacking via direct physical access?
One of the defenses that you can apply is to have a segregation between the critical component. That is the best security control that you can introduce, because you have an infotainment system that may be vulnerable when connected to the CAN bus and if you don't have segregation you can send messages through the infotainment to all the ECU that can be critical.
Is this segregation technique already in use?
This is not something new, this is one of the principles of cyber-security. Segregation, list privilege, so the components need to have only the privilege that they need for functioning. I saw only two manufacturers, and they were talking about data that we never passed but I think they are aware, and they are implementing it.

12. What is the best defense to prevent hacking via wireless access?
For sure you need to use secure protocols. For example, not using GPRS version 2, or WEP connection, replay attack protection. There are a lot of security controls that you can include, but of course everything is starting to from the analysis of the attack surface, and possible risks, and understanding if the security control that you implemented are enough and understanding if the security control that you put in place are strong enough. And of course the best defense that you can have managing the risk is also doing the penetration testing, and understanding what are the possible scenarios that could happen. Regular penetration testing is also the best defense.

13. What is the possible solution to mitigate security risks?
For mitigating security risks, you cannot measure what you cannot control, and you cannot control what you cannot measure. This means if you don't have a way to understand what is happening and what are the potential risks, you cannot prevent them. All starts with a risk based approach, you define the risks, and of course you also understand if the implementation is correct, all back to secure software development lifecycle and so on.

Should cyber security testing by a third party become obligatory to all manufacturers?
There are some actions taking place, for example in the Netherlands there is RDW to create some framework for automotive. To have the cars tested for security before they are allowed to enter the country. These entities like RDW are important for educating the manufacturers and the end-user. Because now the end-users are mostly focused on it works, it's an expectation that you buy something, and you expect that it works. Now the end-users don't think really about security, they think about security as an afterthought. What does it mean? They will car about security only if something wrong happened. Imagine that you are buying a baby camera for you, and there is someone who is an external malicious neighbor or someone that can enter the camera or speaks with the baby. After that event they will understand why it is important. So, it means it is often an afterthought. There should be more investment in educating the end-user and educating the manufacturer, and a central role is held by the accreditation body, and the entity like RDW that is approval authority for automotive in the Netherlands.

Is standardization a good thing and should it be enforced?
If you're enforced, you will do it. For example, for safety the manufacturers are enforced. If it is not enforced, they see security as a cost only. Having a regulation body to impose that will change the game. In the financial industry, the banks need to have and anti-fraud system. They know that they need to have it because it's the regulation, otherwise they cannot operate anymore. Financial industry is stronger in security just because of the regulation, and they are enforced. There is also a direct loss that they can quantify, like how much money they lose. Of course, if you are an automotive manufacturer, and there is a security risk. For example, imagine a tesla for autonomous driving, and there is a news on the paper saying that a hacker remotely controls a Tesla and killed 2 persons. Or there is a kind of terrorist attack in which they use a vulnerability of a Tesla. What would be loss for the company? They still need to consider that kind of effect.

14. Could vehicular communication systems like Vehicle-to-vehicle or vehicle-to-infrastructure communication poses security risks?
Of course. The more communication you have the more attack surface you have. V2I can be also a communication with the backend, with cloud, and so on. V2V means that you have sensors and these sensors are communicating with each other in other cars.

Is V2V or V2I more difficult to implement in terms of security?
I think that V2V is harder to secure, because it is a P2P communication. With V2I you manage the infrastructure, even when it is a cloud infrastructure, you know what the endpoint is. V2V will be a challenge because it's a P2P communication.

15. Is there a difference in terms of security between the different types of automotive network communications protocols (LIN, CAN, MOST, FlexRay)?
The difference between these protocols is how fast they are. The CAN might be insecure, but the automotive industry is still using that protocol because it is fast. If you include more security it means that you will pay the fact that the communication is fast, and in critical systems like cars you need to have velocity on that. I think that in terms of security they can pose the same risk.

Would a new protocol solve this issue?
We would have too many protocols, and we'll have the problem of heterogeneity, and it would be a problem for the market. I think that these should be standardized and should be centrally managed by ISO and so on, and then the automotive industry can implement them, and these will also help with interoperability. When you create something new it needs to be tested, but I think there is not only the ethernet communication is going on, but there are some companies like Argus that offers some kind of firewall, IPS, IDS, and so on that you can put in the care. There is a lot philosophy for that. Evaluating what is the best one I cannot tell because I don't know. You need to sit down understanding what the benefits are and what are the disadvantages for each. To do this you need to include the point of view

16. Could the encryption of network communication protocol data improve security?
Encryption is only one of the aspects. You can have encryption of all the communication, then you have a buffer of the application layer, and even if you have encryption is not enough. It means that encryption is a security control that you can use, but the fact that you are using a security control doesn't mean that you are secure. With encryption you will lose real time efficiency and so on, so you need to balance. But of course, the encryption is a primary security control that is used to secure the communication but there is something else called defense in depth that is also another security principal. It means you need have layers of defense. You need to understand how many layers you need to have in your solution to mitigate the possible risk.

17. All new cars sold in the EEA has an integrated E-call feature which requires a cellular connection, do you think this service is secure?
It depends what do you call secure. The fact that you have an E-call feature, you can misuse these kinds of systems anyway. Imagine that there are a lot of cars and you have a way to send and accept calls in the car. Imagine that there are a thousand signal of emergency calls. How can you distinguish what are the real ones and the fake ones created by a malicious user? The system needs to be secure. So now it is generic, it depends from the specific case and specific implementation and specific use. Because there are also mobile applications that interact with that functionality, which is a possible risk.

Which car would you buy now if you consider security?
There is no transparency, how can a normal user see that Tesla is more secure than a Leap? Leap is a manufacturer on the Chinese market and it is also cheaper. There is no market differentiator, to distinguish who is implementing security and who is not. UL is working on that to help users to make the final decision on the product. When you are buying a fridge, you know the efficiency by looking at the rating. You don't have this for security, and so what UL is doing is also to try to implement a system like that to have transparency to the end user.

Appendix C

Interview transcript C

2. What is your opinion on the current state of in vehicle IT security?
I think there is still a lot to achieve. So, for example the CAN bus is where I did my thesis on is a pretty old protocol, starting from the 90s. Which is still an industry standard even though it has a lot of security vulnerabilities and lacks a lot of security measures. I know there are some consortiums or groups of people working together to try to make another protocol industry standard, but I think it'll take a long time before that actually happens, but I think when they actually achieve to introduce the new protocol, for all the components to communicate together security will go up quite a bit. I think this is also where Tesla has a big advantage right now, because they create all their own components. So, it's easier for them to implement security as a whole than for a car manufacturer that buys components from different vendors and has to cooperate them together.

Do you this new protocol could be the solution, because we already have a lot of them and new one like Ethernet is appearing?
I really think that, especially ethernet protocol can help a lot. So, if all the producers of car components but also the integrator of the components have to speak this language, or to speak this protocol, it becomes far easier to secure the communication between these components. LIN and MOST are also quite old like CAN. FlexRay is newer but, I think it mainly focuses on media solutions, I'm not sure if it works well with high availability requirement of some components, like the gear train, and the breaks, and throttle. But I think especially the Ethernet protocol will be quite a big step forward.

3. Are connected cars less or more secure than "offline" cars, why?
I am not sure about the details to be honest, but I think connected cars come with his own threats, but also possibilities. Possibility to add a patch over the air for example. For old school cars you had to go to a vendor. But the interconnectivity also gives rise to possible threads. of course. Based on how manufacturers deal with the threats and how they use their possibilities it could be more secure, but I don't know all the details.

4. Where do manufacturers spend a considerable amount of attention/time/money, and where should they spend more?
I am not sure where they spend all their time right now. I guess they are aware by now of all the risks that exists. It's been researched enough for them to be aware what is possible, so I think that awareness is there. I am not sure if they already spent enough time/money on dealing with these issues. But if these research groups that I mentioned in the beginning, if they get a lot of support from these vendors, maybe they could speed up the process a bit.

5. How much attention time and money do manufacturers spend on I.T. security in contrast with the previous question.
Moving to connected cars the environment becomes big, it's not just an isolated car anymore. Cars are connected, its IT systems are connected, maybe even connected to infrastructure

when they start talking together. So, IT security together with IoT security, ICS security, all comes interconnected. I think they need a lot of time and attention/time/money they do need to spend to get it all secured.

6. What is the biggest problem in automotive IoT security in 2019?
I realize I am not too up to date on all the things happening right now.

7. How did the automotive IoT security change over the last five years?
I think a big one is the awareness around it. Probably you are aware of the things done by Charlie Miller and Chris Valasek, the car hacking researchers. You really saw a progression. On the first day they were able to hack something when they were actually plugged into it. Then they showed that it is possible to do it remotely, and together with all the other research happening it really went from this farfetched scenario that a researcher could do with very limited circumstances to actually executing on real cars. I think there a big change happened. People realize that it can actually be a big threat, and it can cost live of course, it's more dangerous than an IT vulnerability.

8. What are the weak points of connected cars?
It's the interconnectability. All these endpoints that you just connect to really old systems and really old protocols, systems that weren't developed with security in mind. They really increased the attack surface of a system that is not supposed to be connected. The entertainment system, that needs and internet connection for some reason, or the operating system that needs an intranet connection, or whatever, and these being connected to for example a CAN bus can create quite some risks. And also, the cars being connected to each other and to the infrastructure, if you can spoof any of these entities and send malicious messages I think you can create some disaster.

9. What is the most likely attack vector on a connected car?
I already answered in previous question. These external connections. Of course, it's way easier to hack something if you can do it wirelessly from home than if you actually have to be present around the car.

10. What is the best defense to prevent hacking in general?
It all starts with security by design. When you create software to have security, and it is deployed having proper monitoring in place to be able to detect when someone is being hacked, and knowing how to respond to it with proper incident & response? I think that is a really strong combination. Especially if you have a capable backup and restore program, and even something happens, but if you detect it quickly, you can get back to the default operating state if you can do the restoration quickly. I think it's a really broad thing, probably I left out all the things like bench management, antivirus, access control, all those are important, and they come back at the security by design part.

11. What is the best defense to prevent hacking via direct physical access?
When you have physical access. One thing that you'd like to see is the OBD-2 port really isolated from the critical part of the can network. So, what you often see in newer cars is that there is a gateway after the OBD port, so even if you plug in you can't really talk to the ECUs

that control the engine or the brakes or the gears. Only diagnostics messages can get out. I would say that's one. Another important, and quite obvious one is the immobilizer, that's been in keys for quite some time already. Preventing from someone that can drive away. In the end I think, with enough time and physical access you can always get what you want. But if you make it hard enough that someone can't do it while the car is parked somewhere is a good start. Using the CAN bus and the gateway is an important one.

12. What is the best defense to prevent hacking via wireless access?

For CAN bus it's the same, if you have your entertainment system that has a wireless connection you do want to separate it from the critical systems. So again, gateway kind of thing, or firewall, so basically network segmentation inside the car. Another thing that you see is for example with the keyless entry. These keys that you can just keep in your pocket and open the car and start the engine. Of course, these are vulnerable to relay attacks, you've probably seen examples of this when someone can just start the car in the driveway while your keys are inside next to the door. There could be really simple solutions, as keeping the keys in some sort of Faraday cage pouch, or simply going back to the old system where you actually had to press a button for something to happen. Or manufacturers could implement way fancier stuff like cryptographic binding or something to ensure the key is not too far away, but I don't think manufacturers will spend their money and resources on that. It also comes back to question 10, the more general question: proper detection. And maybe not a case by case basis, maybe not that in a car you have a detection mechanism that can flash a light when he is being hacked, I don't know what you really can do as a user from that, maybe pull over. But I think it's more important as a vendor to have a general overview of their fleet, if they're getting signals that something fishy might going on these networks, then they can investigate, and step in if it's necessary and prepare a patch so they can roll out.

14. Could vehicular communication systems like Vehicle-to-vehicle or vehicle-to-infrastructure communication pose security risks?

It definitely does pose security risks, you're opening up your car to even more sources that can communicate to it, that you don't know for sure if you can trust them or not. They are external parties they could be spoofed, or whatever. But they also pose opportunities, and I think that's important to realize that all these improvements that are being made, they are not just scary, but they can give a lot back. Not just in terms of traffic jam mitigation, or whatever, but also in terms of security if you average the knowledge if you monitor the thing as whole you can infer a lot more from that then just a single connected car.

Which communication system is harder to implement?

For both you need some industry standard of course, because you are talking about different vendors. If you talk V2V within one brand I guess that's the easiest, so all Volkswagens can talk together or something.

V2I you start cooperating governments, which tend to be even a bit slower than the companies, so I guess that will be the hardest thing to get them all online. The increased number of parties definitely adds a big lead time there.

15. Is there a difference in terms of security between the different types of automotive network communications protocols (LIN, CAN, MOST, FlexRay)?

I have looked into them in my thesis which ended two years ago, but if I remember correctly LIN is even a simpler version of CAN, for example for your windows to move it up and down. So, I guess that's the same as CAN or worse. CAN itself is really old, no security measures built in. The strong error detection which is nice in a car but security wise it's not. I am actually not sure if FlexRay has some things implemented. I think so, but it is quite limited. So, what you mentioned before, the automotive Ethernet, that could be the way to go.

16. Could the encryption of network communication protocol data improve security?
Yes, it could. If you look at the CAN bus, attacks that could happen are really simple basically, because it's just a plain text protocol, and you can add messages, remove messages, modify messages. All of this could be prevented by encryption. Encryption could definitely help. I am not sure if practical to roll out, because you have time sensitive applications, and you need real time application of course, and I am not sure if encryption adds too much overhead.

17. All new cars sold in the EEA has an integrated E-call feature which requires a cellular connection, do you think this service is secure?
Any additional external you add to the car does add to the attack surface of the car. I'm not sure about the details of how this is implemented. I'm not sure how it detects that an emergency happened, if it does have connection to the breaks or something that detects that something is not functioning properly than I definitely see risks. If it's a more separate service, I definitely see a very good safety implementation.

Should cars be tested and rated based on its security?
Of course, it sounds very nice, but I think the problem with these is that let's say you're shopping for a car, and you have a car that costs 5.000 and one which costs 10.000, and the 10.000 one has a stamp. Are you going to make your decision on this stamp? I don't know if the average user has enough awareness to make a decision based on this. Maybe it would be a good beginning to start with this and then to enforce it by law. So, manufacturers don't have a choice, they simple need to do it, so maybe it could be a beginning towards that.

From which brand would you buy a new car considering security?
I haven't done any research on this because, but I think Tesla model S is the one leading at the moment from what I've heard.

Appendix D

Interview transcript D

2. What is your opinion on the current state of in vehicle IT security?
Current state it really depends on the maturity level of the OEM. That would be the exact answer. Let's assume there are OEMs that has come to these spaces after being attacked. Probably you know the Jeep attack, and others that are sort of rushing to reach an accepted level of security within their vehicles in a totally changing environment where they moved from securing the perimeter, like a single car, head unit, or a single ECU within the car. Now they need to protect the embedded systems. There has been a big challenge for OEMs. And the result of this approach something that is not always measured as we expect. For sure, safety about privacy has place but I think we can do even more. That was why we are actually crafting an approach to assist OEMs in their connected vehicle security journey.

4. Where do manufacturers spend a considerable amount of attention/time/money, and where should they spend more?
At the moment they spend a lot on securing the single components, let's assume a typical connected vehicle ecosystem where you have mobile apps, head units, the vehicle itself. They spend a lot on securing single items, just the mobile application itself or the single head unit, but they are not spending well in protecting the end-to-end. The approach is not preventive but more a reactive approach to security, so they can spend more on protecting the end-to-end. That is not easy, but reachable so some OEMs are moving into that direction.

6. What is the biggest problem in automotive IoT security in 2019?
In my opinion the biggest is still ensuring the safety for the driver while features are growing at a very fast pace. The topic here is dealing with Tesla, or other top-notch players that are delivering new functions so business is more and more focused on the delivery of new functions to the vehicles like assisted driving, sort of autonomous driving. Lot of features that combined with connectivity to the vehicle itself and to new features is actually bringing more security risks to the ecosystem, and the challenge is actually ensuring a good level of security and coping with the spread of new functionalities asked by the business.

7. How did the automotive IoT security change over the last five years?
As I mentioned, the Jeep attack was really an event that changed the perception. We also had an environment before the Jeep attack where each OEM felt secure, so they didn't expect that someone could be able to turn off or brake the vehicle on the highway. The real topic is not the attack itself. You can imagine every OEM could be attacked at the time. They were not exploiting a single component, they exploited a network vulnerability then the head unit and then the segregation within the head unit and the CAN bus within the vehicle to launch and control the vehicle itself. They opened their eyes about having sort of new attack landscape and so the real point is how OEMs has changed their security posture to cope with the new threats. The trends that we have seen a lot is, first establishing the security functions, like vehicle security responsibility within the company, they have appointed a new roles and responsibilities within the company, so that was the first step that we've seen. Second, then the increased number of badges, I think about in product security I think 5 years ago we were

not even talking about product security. Now we have people working in embedded security, cloud security within OEMs. The third one that is still, and ongoing trend is about monitoring what it can from Vehicles. Let's assume an example, the data that vehicles are generating data while being operated needs to be analyzed, even to understand if there is an attack in place.

8. What are the weak points of connected cars?
The weak points are proportional to the features. Let's assume a not fully connected vehicle, so a vehicle that still lacks some new cool features, that vehicle is secure. When we talk about weaknesses of the vehicle it's always tied to the amount of technology that is within the vehicle. It's important to understand the approach and to understand how not only the OEMs but also the tier 1 and tier 2s are affected. If a tier 1 is putting security into design and into the product then the result is that there are less weaknesses. If you are leveraging or you are giving too much freedom to the Tier 1, then your vehicle as OEM is not secure. That is the key point, managing the lifecycle of the vehicle not just hardening, patching, or securing a single component.

9. What is the most likely attack vector on a connected car?
I would say two years ago that the most critical part could have been a remote attack, sort of jumping into the cellular connection of the vehicle, trying to temper with the connection, with the back-end, or trying to control the vehicle from a cellular network, and then gaining control. Nowadays, with the autonomous driving vehicles there are a lot of so-called machine to machine. It is very important to protect from proximity attacks, so you know 2020 the key point is to still have a secure communication even between vehicles, because now there is no interaction between men and vehicles, but the risks are there. Even that the V2V communication is still secure, it's required to monitor if someone is tampering or trying to tamper with the connection, otherwise you can lose control of the entire ecosystem. It's a matter of trust between the vehicles, so when we are talking about machine to machine it's not just having someone performing bad things on a mobile app, but probably someone that is spoofing a vehicle to send wrong information, for example we had a recent attack where someone has tampered with the lanes on the streets to have an autonomous vehicle to crash, so having the vehicle changing lane. But without actually having fully controlling the situation. This is just a sample where someone has modified something on the road and has gained the control on the vehicle. This is the new threat, so it is not just patching the server, or hardening the server, but actually leveraging with autonomous vehicle or Advanced driver-assistance systems are leveraging on external information. If you temper that external information, then you can control or modify the vehicle itself.

13. What is the possible solution to mitigate security risks?
First, the understanding the context, the vehicle you are protecting. For example, I used to talk with CISOs about protecting commercial vehicles, or commercial trucks, tractors. You need to understand the threat landscape, what are we protecting against. Once you understand your context, and your specific threat landscape it's important to protect not only the single components but focusing on the entire vehicle value chain. There is a concept that we developed in Accenture about the value chain. The value chain of connected vehicles starts from Tier 1 building, for example the head unit and until the final sale of the car, and still is part of the security of the car because it is involved in securing access to the information of the user or provisioning a secure service to the user. There is a set of activities that are not

only tied to a single component but to the end-to-end realization and delivery, and operation of the vehicle. Another key point is that OEMs are now facing is the monitoring of security when initiated by the vehicle. That's another point that is now speeding up the growth of a so called vehicle security operations centers. Companies are aware of the need for a security operations centers, so it's nothing new, but they are not aware of vehicle security operation centers. It is a new topic that we are addressing, we are answering some tenders. This is something that OEMs are coping with nowadays. Once you have these vehicle SOC in place, there is also a need for having a PSIRT (product security incident response team) that is even able to respond to incidents that vehicle SOC has detected. You're actually performing a set of activities related to contain and mitigate incidents. For incidents what we mean is a vehicle is being attacked, but not only, but also vulnerabilities that can impact the vehicle. There is a set of actions that every OEM should put in place to reach or increase the maturity level of security.

16. Could the encryption of network communication protocol data improve security?
I would say yes, and no. Because let's assume in an example that we have like TLS, we have a lot of security improvements in terms of network communication that can at least ensure confidentiality. Encryption means confidentiality in security, so no one break into that connection. The real point is not only encrypting data, that is for sure a best practice, but understanding even which data is really needed. It's important even to reduce the data to the set that is strictly needed, and another point is making sure that you are connecting to the right party. So there is a need of mutual mitigation, so it's not only establishing a ciphered connection but making sure that you're connected to the right party. Not a back-end server that is trying to be hacked on behalf of the real server which is a sort of spoofing.

Appendix E

Interview transcript E

2. What is your opinion on the current state of in vehicle IT security?
I don't think you can talk about I.T. security because I.T. security is something that's really for the IT Part of the information technology industry. It's more about that in the car you're not allowed to have false positives because safety is number one.

3. Are connected cars less or more secure than "offline" cars, why?
It's depending on how you want to phrase this. You know if it's all about safety, the answer could be answered yes or no because you know you can take an ODB port and do all kinds of stuff with the machinery. Or you can cut off the brakes cable or things like that. So depending on how you look at it, of course with the connected car you are creating another attack factor. So is it more safe? I don't think so. Is it more vulnerable? Yes. Because you're introducing more technology, more vulnerabilities because these technologies are being coded and these codes have flaws so that will be the same. Take an airplane, a Boeing, there are forty thousand errors in the plane. It depends on which angle you're going to look this. From a safety perspective that's key for the automotive industry. The autonomous car will be more safe but that's because all this technology and the fact that it can work with him, and what we are enabling, and the attack surface will be more. Of course it will be more challenging for hackers to see how they can penetrate from outside to the car. So yeah. Is it safer or is it the same as offline cars. I don't think so.

4. Where do manufacturers spend a considerable amount of attention/time/money, and where should they spend more?

They should spend more on standardization and they should spend more working together. I'm part of the automotive ISAC, which is very popular in the US and not really in Europe yet. We have to go down whole goals where we share experience and this agency also supports when they find firm abilities for the car manufacturers. You know everybody is hurrying up to get to the market, bring the business to the market, but you cannot jeopardize the safety of the drivers and the passengers. So still, there has been a lot of work still have to be done. They really need to spend more time on not only designing the vehicle but how to secure it.

5. How much attention time and money do manufacturers spend on I.T. security in contrast with the previous question.
I think not enough, because if you look to the setup for building a car. The industry really tries to build the car as cheap as possible. For example, if a sensor is one dollar you will not build security in for on the sensor that's worth hundred dollar. So, related to security they are not spending enough. Globally I don't know what the budgets are for that, but it's not enough. And what the industry is now looking for is: OK. what's the balance? And you will see that the big car manufacturers will do is they will try to outsource security for the vehicle because this connected vehicle is creating so much data you cannot upload that data always to the cloud because then the car manufacturer will go broke. So machine learning, A.I, those type of

intelligence are becoming more relevant and technology on bit level is getting more important.

6. What is the biggest problem in automotive IoT security in 2019?
I think the biggest challenge will be how to standardize. How can we standardize so everything will be much cheaper to secure the connected car.

7. How did the automotive IoT security change over the last five years?
That's very easy. We as customers are getting more demanding. Because we want to have quick access to the telemetry. So if I'm going from point A to B and there is a traffic jam I want to know how I can overcome this traffic jam. And I want to get that much faster with less fuel consumption. We are alerted upfront before I start my journey. Things like that. It wasn't thinkable 20 years ago for example. So it's making the journey more comfortable for the customer itself. And you can plan it much better now if you know I have a meeting in Brussels that will take one and a half hour then it's out of traffic congestion then you know how to do and plan it better.

8. What are the weak points of connected cars?
You know, till now everybody is talking very theoretically about connected cars and what their capabilities are. I think the weak point of the connected car is because it's so new, we don't know much about this and that everybody, every car manufacturer is implementing their own system. And they are not sharing, like for example in automotive ISAC you will see Mercedes is not sharing if they see some vulnerabilities with other competitors. And that's something this industry has to learn to share more.

9. What is the most likely attack vector on a connected car?
I think the most likely factor will be how I can penetrate the car and change settings or steal data, because the industry is not standing still. Let's take Porsche for example because we do a lot of work for Porsche so it's interesting that this Porsche car that will be rolled out in 2025 or somewhere. You have a standard horsepower, let's say 400 HP, so what if I can upgrade my horsepower by buying an app from Porsche and I want to take my car to the racetrack. So those type of functionalities you will be creating that. And that could be an attack factor because this app should be verified, it could be malicious code in everything. There are certain ways that this industry will move, and you will see these slow development of an appstore like concept for the cars.

10. What is the best defense to prevent hacking in general?
I think the best defense is isolate everything, so the cars will have around 200 ECUs, maybe more, so you need to have a security gateway where all these ECUs are connected to and you are only allowed to update the ECUs if you have the right credentials, the right keys. And it should be on bit level and not on messaging only.

11. What is the best defense to prevent hacking via direct physical access?
Oh that's difficult because you fall back on I.T. because when somebody really targets you they will get it. And that will happen also in this industry. And if somebody really wants to hurt you

they will find a weak spot. I think there is no best way yet, because it's so new, we have to find our ways into it.

12. What is the best defense to prevent hacking via wireless access?
What I would prefer is to set up a secure channel that can be SSL or could be VPN it's depending on how you are looking into it. This is the best way to do it.

13. What is the possible solution to mitigate security risks?
It's always on the edge to mitigate, so AI. and machine learning will help a lot. But still it has to create and digest a lot of data and so what you cannot do is for example, it’s depending on how the car is made so you must take right measurement that the car could not be tampered, and then that can be only be done if you really have a solid architecture.

14. Could vehicular communication systems like Vehicle-to-vehicle or vehicle-to-infrastructure communication pose security risks?
Of course it can. Imagine if we were able to penetrate the vehicle to vehicle communication and instead of communicating with the car in front of you let's communicate to 10 cars in front of you. We don't know yet what this will bring to the market because the car will communicate of course vehicle to vehicle but most interesting is vehicle to infrastructure because I'm not so worried about vehicle to vehicle security because I think that's something that will work out. I’m thinking more about vehicle to infrastructure because you have roads, you have traffic lights, so many things that is not controlled by the car itself. But it's getting information from the outside of the car and it's more depending how that infrastructure; a third-party infrastructure is secured. So thinking about that, and looking at the industry we have to think about the information that I'm getting from the third party is the integrity of that information the quality of the data, is that correct? And if somebody can manipulate that data you're getting the wrong information. And that's why I'm also with A.I. and stuff like that. You have two types of machine learning. One is supervised and one unsupervised. With supervised you know the outcome and unsupervised is that the machine is learning itself and just analyzing what the outcome should be. What happens if AI. is compromised? If you will fill the A.I. information with wrong data. What will the consequences be for it? The industry is not yet there. That's the biggest challenge, we've got a beautiful solution and I also believe in autonomous car level 5 even that it's very close by. But security wise we are not there yet. And the challenge will be more about which manufacturer will bring complete autonomous cars to the road saying hey we are secure enough.

15. Is there a difference in terms of security between the different types of automotive network communications protocols (LIN, CAN, MOST, FlexRay)?
Yeah. It is depending on how much data you have to work with, but you know, CAN bus traffic is one way traffic, just send messages and if some messages drop, it will try again. MOST and FlexRay are more focusing on multimedia. And we have to think about it more in a way, okay, will encryption work for example? I don't think so. And that's why you have to verify every message that you are sending on integrity and that you have to apply over all these protocols.

16. Could the encryption of network communication protocol data improve security?
Of course. Most cars don't use encryption for example. The CAN bus traffic you can temper it very easily. Encryption will help. But is it the holy grail? No. Because you will fall back.

Encryption will help you until a certain level. But what if somebody can penetrate if you look to the attack surface from the cloud towards the vehicle. And then again, an attack factor that the industry is not thinking about because they are so focusing on autonomous driving and car security. But what about the ecosystem? Because in the future it will be over the air update. So that cloud must be protected. And Cloud is a shared responsibility model because AWS and Google will protect you from infrastructure level, but all the thing above the infrastructure level are solutions that you have to take care of. You have to protect your firmware, you have to protect your data that you have in the cloud. There is no cloud provider that will take that responsibility. So, you have to take your own measurements, because these attacks surfaces are very important.

And why do you think manufacturers aren't using encryption?

Its very simple, encryption breaks a lot of things. Because all these cars have never been tested with encryptions. And encryption takes a load on the processing capacity. And remember, if you start a car it does certain checks. And if you put encryption into that it will take more time. That's because this car has all these brilliant ECUs. If you take a car who was 20 years old, you don't have that.

Can it be done, if wanted?

It’s not impossible. But the second question that you will have is: is the manufacturing having this business model that they can invest in the encryption if for all the ECUs and that's why AUTOSAR architecture is very important. The AUTOSAR is written by, I think one of the guys from Toyota. And it's very interesting to see how he talks about encryption architectures for the car.

17. All new cars sold in the EEA has an integrated E-call feature which requires a cellular connection, do you think this service is secure?

No. This service is not safe. It depends on how you look into this. So, when you set up the call or the channel, the channel is not encrypted, the channel is just open to the mobile network. For example, every call that you do with your mobile phone is that secure? No. So you need some way to encrypt. You've got the GTP tunneling protocol. But you can break them. There are still a lot of things to be done in this area.

And if they would use 4G for example for data transfer, would that be more or less secure?

So it will be the same for 4G or 5G. When you use narrow band IOT, those protocols itself are not secure. You have to find a way of securing that protocol, so it can be done with keys. It can also be done with fingerprinting technology, application identification so more on layer 7 for examples. Let’s take Facebook. Facebook has a lot of way of communications. Instead of doing it everything by IP ports, you do it based on application identification. For example, if you know that the application that I am gonna transfer from the car to the cloud or to the mobile operator if it's a voice call for example you fingerprint that I.D. So you know that this is a call. If somebody tries to temper and change coding or do something else, it will immediately reject that. So fingerprinting technology. In a simplified way of telling, I think that's the best way to go.

So nowadays cars are tested. For example, car crash test. But in the case of security testing, who should be the party doing it?
Hopefully not the manufacturer. Because you cannot eat your own dog food. So, organizations with testing environments should do this. You know like they have for testing on the CO2. So, there should be one organization. Or of course in each country depending how you see the one European organization was responsible for testing it on security.

Would you like to add something?
Of course. This is such a big theme that is coming up to for the automotive industry. It's new for the automotive industry. But if you look to aviation they already applying all these technologies like the auto pilot, landing systems, taking off systems, or stuff like that. So looking at the industries that are already being applied I think that we can get good lessons learned from it.

Why do you think the automotive sector is slower to adopt these new technologies like in aviation?
I think it has to do with money that you want to spend, but also services that you have to bring to the market. And the fleet management of thing. Remember they have huge fleet managements and there are more cars in the world than plates are. And there is a whole education system that's going on also for how you are going to repair these cars in the future. So that's why the adoption is more slowly because you have to serve a bigger, and more passengers. In an airplane you only have to take care of the passengers and communication system and there is less traffic than on ground. It is more complex, and the aftermarket is much bigger. You cannot throw it overboard and be successful. One company that is trying to do that is of course Tesla with its new concepts, with the batteries and stuff like that. But till now Tesla has seen challenges and Tesla doesn't want to be compared with the automotive industry as a car manufacturer. No, they tell themselves that they are a software company and not a car company. So those are shifts that have been seen and is going to be made. I was two months ago in Japan talking about autonomous cars with all the manufacturers and Toyota has opened his pattents for the hybrid model. So, everybody can share. This should be more common to the business. And for example, how many car manufacturers do we have, and how many plain manufacturers do we have. For passenger planes I can come up with Boeing, Airbus and maybe a few small ones, but that's it. But over here, the automotive industry is a much bigger market.

I only have one personal question left. From which brand would you buy a new car?
I would buy a German car. Any German car because I know how hard they are working on safety etc. And they are far ahead of the ballgame.

Appendix F

Interview transcript F

2. What is your opinion on the current state of in vehicle IT security?
The current state of IT security in vehicle appears to be in its early days because it seems to be just security concerns by IT guys. Manufacturers are not completely aware that they need to step up about this. They are still in their early age, because they don't see in-vehicle IT security as a competitive advantage. They are still seeing that they can adapt to when they are far away.

3. Are connected cars less or more secure than "offline" cars, why?
My answer would be yes, they are. Offline cars are more secure, but it depends on what we're talking about. If we are just talking about jumping into a car and drive it from A point to B point, yes you can say that it is more secure because its attack surface is not so wide as it could be with connected cars. The less points you can address in terms of security on an object the more secure it should be. Furthermore, you don't have any remote component so rationally it should be more secure than something connected.

4. Where do manufacturers spend a considerable amount of attention/time/money, and where should they spend more?
Car manufacturers focus is to make business, and they don't want to appear in the newspapers as being not safe, so they are more focused on safety and to protect the brand. What I know the best is the French market, here they are more focused on safety, what for me is wrong because safety is just common sense of doing business. If you want to have competitive advantage between your competitors you need to find out they way to make the car more autonomous, more contactless, and you need to focus on cyber-security.

5. How much attention/time/money do manufacturers spend on IT security in contrast with the previous question?
I would say they are getting more and more aware of cyber-security, so I would say they spend 5 times more on safety than on IT security.

6. What is the biggest problem in automotive IoT security in 2019?
When you are remotely accessing some component on your car, and let's say you are trying to ignite your engine remotely, you are giving access to a part of your car to someone who is not physically accessing your car. That is a way you can have the most important breach on your car because if someone can hack people who are trying to access your car remotely they can do anything with your car itself. For me, the remote attack chain they only way to perform a contactless attack and they are finding interest of all kind of trace agents.

7. How did the automotive IoT security change over the last five years?
It changed a lot, not only because of automotive industry but because of the booming of global IoT industry. They see that there is a market there, even if they don't know exactly how to take advantage of it. They know that there is a market there and they can jump into this market the better they can keep some position on the market and they can also work on all

over high term which are related to these markets. Interoperability, autonomous car etc. What they are looking for is not only to make better car to transfer a product-based industry to a platform-based industry, but they are wanting to have all the addition market. When I am talking about interoperability, if I have the capability when I am close to my house if I can put my light on because my light operator recognizes my car and know that I am close to my home. That's something that can be a big differentiator for users when they want to acquire a new car. It's also about making cars more autonomous. The more you have IT security in your car the more you have the chance to make it autonomous, and to disrupt the market/industry of vehicle.

8. What are the weak points of connected cars?

I would say remote services. It is a way to compromise a vehicle easier to trigger a cyber-attack on remote services. If you don't have the key to the car the only way to access it is by accessing remote services and use the ECUs. By nature, remote services are engaged into communication with various interfaces. You have WiFi, Bluetooth, cellular network. If you can hack these kinds of interfaces, you can access the car itself. For my point of view that is one of the most important point. The second one could be the remote code execution. The more you are using connected car with devices and IoT component the more you are using some IoT code in the firmware you are exposing the attack surface and making it wider because I can play with reverse engineering on your firmware because your car will be sooner or later will consist more byte than physical component. And if you can make some reverse engineering on the firmware or in the code that you are using to put it in your car or to make it accessible from a platform and I can be able to misuse it.

13. What is the possible solution to mitigate security risks?

It is also related to the way we as Accenture can drive automotive security, right? What I can say is that you need treat automotive with a cyber security concept. Not just to say that it is a specific industry you don't have the same process on it, but you need to have a global process on your security. It begins with the conception of the car itself, the way that you introduce some notion and some concept like privacy by design and how you can completely introduce security at the very beginning of your process, and the way you can put it your own APIs. Because we are also working on a global world and a global market, it is easy to be hacked by competitors and when they know exactly what you're bringing to the market they can know exactly how to hack it and how to give this information to hackers or however to ruin your reputation. The global software lifecycle for connected vehicles should be restricted and governed as a normal software lifecycle which needs a high level of security. And you also need to respect the standards and protocols. The biggest issue that we are facing nowadays on IoT market is the lack of standard and protocols. If you don't have some component or some tiers which make it possible to have some interoperability between proprietary standard and normalized standard it will be an issue. It is very important to be compliant with international standards only because when you are driving a car you can cross some borders, so you need to have this in your mind when you are conceiving a connected car. You also need to take care of cryptographic solution for connected vehicle because if you consider the car or embedded component unit as something accessible remotely you also need to take care of the way they can be used to get it. You need to introduce also some capabilities of cryptography or all these standards that are used to make it possible to authenticate the test unit you need to introduce them in your conception. Security should be something that you need to think about in an end to end perspective. From the conception of the car, with privacy by design, true written marketing aspect, your ID protection, and a way you conceive your firmware, your code etc. and the way you globally govern your industry chain.

Could standardization be a solution that each manufacturer should follow?
I'm convinced that manufacturers will never follow the standards, not completely at least. Because they will all want to protect their own advantage on the competition, and they know that when they make themselves compliant with the standard, people will make it possible to interact with them, and the biggest point they want to protect is the way they produce data in a way that they can manage and monetize this data. They know that every time they make themselves compliant with normalized standards, people and other competitors/companies can access data that they are producing and can use it to take more advantage on them. What they want to do is not only to bring some security to the connected car, but they also want all these new markets which are being opened because a car is connected. When you have a connected car, let's say I'm an insurance company, if I only know the way you use your car, I can propose you the most suitable insurance contract to you. This contract would be based on the data that the car is producing. Suppose that a car manufacturer makes it only accessible through standard or normalization. I can easily access the data without paying the car manufacturer. I'm not confident in fact that manufacturers will make it possible to be compliant. At the end of the day we will need some mediator to be the judge of piece. Someone between all this industry, car industry, insurance industry, to make it possible to translate proprietary standard or protocol universal.

14. Could vehicular communication systems like Vehicle-to-vehicle or vehicle-to-infrastructure communication pose security risks?
Yes, definitely. Let's suppose we talk about vehicle to vehicle communication system. When we talk about the same manufacturer, let's say you want to make a Peugeot communicate with a Peugeot. You need to make wireless communication between bot. You need to make them communicate together through some network protocol. If I can hack this network protocol, I can abusively get access to both cars. It's not a big deal because you can secure this kind of communication through some secure layer, like a secure socket layer, or a secure protocol that we have on the market. When it can go wrong is when you are making two cars from two different manufacturer together. You need some kind of translation of the protocol between both if they are not talking the same language, so you are making the attack surface even wider, so it can pose risks. And now the last point when you are making a vehicle communicate with an infrastructure it can also be an issue because you have to know exactly the framework. Your infrastructure is based, and you need to find out the best way to talk. What I am saying is that every time you need to make two components talk together you are introducing some risk in theme of security. This risk can be mitigated in such a way that when you brought some mediators in the middle of the communication.

Which one has more security problems?

I would say when you are making two vehicles from a different manufacturer communicate together I would say the risk is more or less the same as if you were making a vehicle communicate with the infrastructure because in both case you'll need some intermediation, and that is where you're making your attack surface wider.

15. Is there a difference in terms of security between the different types of automotive network communications protocols (LIN, CAN, MOST, FlexRay)?
I would say that between FlexRay and MOST is the greater differences.

16. Could the encryption of network communication protocol data improve security?
Absolutely. Every time I am talking about IoT security with people who are wanting to know more about IoT security and how they can jump into it without being afraid of abusive usage, what I say to them is that we are using encrypted communication networks for decades, so we can trust it make our communication safer. Definitely, my conviction is that one of the most convenient way to secure network communication between connected devices.

Why car manufacturers aren't using encryption?
Yes, it is an extra expense. They believe that they can achieve the same level of security without encrypting the network. Which is something wrong. The only project I did on connected object is the one with PSA on connected vehicle, and we convinced them to onboard PKI in their project so that they can secure the transaction between connected cars, users, and application resources. That is basically a matter of money, where they do not want to come to this decision, but I am convinced that at the end of the day they will all come to this because there is no way to run to. If you want to guarantee a good level of security in your transaction when you are using a connected device. That is one point which make them feel this way. I don't know if you know the difference between smart device and constrained device. Constrained devices are test devices that you have in daily usage and they don't have surface to introduce this kind of certificate and to make some encryption transaction. You know when you have a Fitbit for example, we call it constrained devices. In connected cars we have more than 128 MB where you can introduce some PKI component, etc. So, when you have a car manufacturer, they say, I am not obliged to make some asynchronous communication between my device, my car, and a service or application. They say that my surface is wide enough to make me interact with a server with certificate and I can just be without certificate. They say that they are not obliged to make a handshake from the two endpoints, they just want the server to have a certificate. This is a bad idea because it is a level of security that this option is offering to them is not secure enough to make users to be confident in what they are proposing. I am pretty confident that at the end of the day they will all come to the fact that encryption of network communication will highly improve security.

17. All new cars sold in the EEA has an integrated E-call feature which requires a cellular connection, do you think this service is secure?
I will have a philosophical answer, and not a technological one. For me when you are putting a SIM card in your car you are making it more vulnerable. I prefer a car without SIM, somehow to call emergency when an issue happened to me than having a SIM in my car, because it will

be the start point of my trouble. Once more it is not something very rational what I'm saying, this is just something for my own experience as user of a car.

Should cyber security testing by a third party become obligatory to all manufacturers?
Absolutely. Manufacturers should pay the highest attention on his production chain, and we should have a global protocol which need to be followed from end to end. We talk about privacy by design, we talk about IT protection that they need to care about before bringing a car to the market. And once a car is on the market or even before, they need to have a strict protocol, and give some kind of certification to the car manufacturer. Like a normal vendor, when it comes to IT and you bring a new software to the market, or when you bring a new hardware to the market, and it comes to security of people you have some certification that you need to respect. It's a bit of same thing for all connected device manufacturer because they are coming out of the traditional physical product market and they are jumping into a platform market. Being part of this market, they need to bring some guarantees to users so that users can know what kind of certificate the particular car has, and that the user's data is safe, and can be manipulated by the user, etc.

All this agreement that we are expecting from vendors when we are buying a software. We also need to expect this from car manufacturers.

18. Would you like to add something?
My biggest conviction is beyond connected car and IoT market. That is something that we are not taken as seriously as we should.

Appendix G

Interview transcript G

2. What is your opinion on the current state of in vehicle IT security?

It's really bad at the current state. It's not super bad, so let's say it's not that everybody could do it, but it has the same problems as networks. It has bugs, it has attack vectors, it has places where you can do it, if you have the right software, if you have the right key. The thing about being able to copy signals is something that we have to tackle. We need an extra authentication for example, not only signal or frequency that triggers the on and off on a door. If this were a network environment and you say, we authenticate by signal of a key and that gets captured. We need to mitigate that. How me mitigate that? For example, by using what everybody else has on his mobile is a biometric fingerprint authentication and there are other ways to be able to start a car without having to capture the frequencies in the air. Other thing is, yes it's great that we have everything connected, and we control everything from the remote like brakes, accelerating, stopping, sensors, alarm, lights, horns, it's all great but it wasn't architectured well. In cybersecurity we make sure we put borders there where needed and make sure that the access to these borders are more or less thought about what do I want to do. It's great that we have remote control for the brakes, but how will I access it and trough what application? If I'm in the system and through the brakes or do I need to be authenticated in the sub-system for me to use the remote. We make it too easy, if everything is open anyone have access. If I have access I'm the owner I can do anything. It's too easy because it's a 1 2 3 step for a hacker as well. We want to add 4, 5, and 6. In the meantime make the authenticated user still have that good experience in using the car and all its functions but make it extremely hard for hackers to go through these arrows and lanes that we have put in these network architectures to stop attacks. It's the old story as usual. Manufacturers have new gadgets, new tools, new functions and they want to push it as fast as possible to the consumer who has the money who will pay, and they need that money today not tomorrow. They'll figure out that there are bugs in the system anyway, and they will fix it, but with connected things we need to test it first, you need to put in some good security architecture, not only functional architecture, then we can enhance the state.

3. Are connected cars less or more secure than “offline” cars, why?

Less secure. Because, like I told you, at this point an offline car what can you do from the outside? Connected cars have options. If I have options as a hacker, it's less secure. If my car has no online connection or SIM card built in, what are they going to do. That's for me an easy question.

4. Where do manufacturers spend a considerable amount of attention/time/money, and where should they spend more?

They are pushing like any manufacturer with internet connection, pushing it drones, pushing it cars, fridges pushing it. The first smart connected fridge was hacked and used as a spam server. So, while you were drinking your milk, it was sending 1000 emails every minute. The attention should be on secure usage of their products instead of usage of their product. The word secure to any policy or goal or whatever they want and then you have a better secured product. I see it all the time, they don't have the security people at the beginning of the project. Let's say you want to build a drone. It goes with your app on your mobile phone and with your computer, etc. They don't evolve security people in that meeting, they get engineers, electrical people, GUI people, and they build a thing and they have a software package. Sometimes they call in the security people, hey we want a security check on this thing that we already built, architecture is in stone, everything is fixed. Sometimes security people can't even do anything about it. They can only say, yeah, we can do this to secure it a little bit more, and then here is your stamp, here is your product.

Can this be due to the lack of automotive IoT security people?
It's true, so what they need to do is to hire more people and involve them earlier in design process, and even before prototyping. If you involve security people in that process then you get a more secure product a 100% because if you are at architect level, then you are able to say: hey if we put this here instead of all together and one here, then it can be more secure by putting in more security measures and software. It has been done before, and we know the shift should be to more secure designing instead of secure auditing.

6. What is the biggest problem in automotive IoT security in 2019?
The biggest is that we are going so fast. Tesla is pushing automated driving from A to Z. You put in the address and you sleep. That's what they want to achieve, and they need to achieve it fast because Tesla's going down financially, and support is going down. It costs a lot of money to build these cars, they are not making any profit right now. This is an example to show how quick they need to push, they don't have the time to research things in the way they want or need to be. They'd rather have a bug, or a car crash, and this is like the hard truth, then wait three months and lose $5 billion. They need to push it out, they know there are bugs, but that's for them pure businesswise feedback even if it's fatal. I think that's a problem in human thinking, you need to make a product that is tested and safe, and you need an extra three months to do that. They are under a huge pressure to release, and not to test, and especially not in cybersecurity. All the other manufacturers have the same mentality.

7. How did the automotive IoT security change over the last five years?
They woke up, because as I told you it was first functionality only, no security. They first taught people are not smart enough to do that because they need their software, they need their source code to do that, that's what they said. Now they are awake and realize that there are people smarter than them and could hack their products, so they want to make sure they have more security in the end. They did involve the audit, they take security a little bit more seriously. On the other hand, if you say automotive IoT security in the end, they do actually take all of that feedback seriously. What they do is they make changes and talk about it and make sure that they are compliant. And they know it's going to be a disaster if 100 cars were taken over in the same time. It would be a big disaster for the world.
8. What are the weak points of connected cars?
The internet. It's the internet, it's authentication, it's making sure the right users using the right functional product and not the hackers. It's pure authentication, and how we enhance that authentication with biometrics like fingerprints, we have some smart things that warns if your car is suddenly connected to China, and I am not in China, some other systems would trigger hey, that's suspicious. Cars need to do that as well, putting more popups, and more stops, if my car took over I can say I don't want this. Where is the stop button to make it an offline car? You need something like that, let's say your computer suddenly started the mouse started to move alone. We are trained to pull out the internet. That's actually in our training.

So where do I pull out the internet from my car? If I wake up and I don't want internet in my car, I only want to drive offline. This is my offline button, and here we go. Me and the engine, and my radio on FM. Where is this possibility?

9. What is the most likely attack vector on a connected car?
I drive currently a BMW, it has a connected services and I can see where I am. This doesn't even need an attack. If people can follow the car, it's a silent attack. That would be not good because you can target. Having the same software as the car company and changing it a little bit, and crazy things can happen. You know obvious things like the controls, the brakes, the power, the fuel. You know BMW can put destination from the call center where I can call them and ask for a hotel, they can find it and push it to the car. They can change the navigation, they can make you drive on a specific route and jump on you. There are many things. In the end we think about the fatal situations, and this is where it can kill you. When you are driving 120 and let's do an emergency breaking right now. Everyone behind you will hit you and it would be massive. Let's do this not only with 1 car but 100 cars, at the same time, in the Netherlands in this area. 100 accident, mayhem. This is like the scary story, but it's possible. If I have access to one car I can have access to others.

10. What is the best defense to prevent hacking in general?
Authentication again. Smart authentication, and not passwords, but biometric authentication. It's something you are, and you have talked, and you know the pin. This combination of three things is good.

11. What is the best defense to prevent hacking via direct physical access?
The best alarm is the car alarm. Just have a very good car alarm. I have some cars where I can stand close to, and they will make a little sound. And make sure the user is notified when there is someone trying to enter the car. Make sure if you have a subscription that it calls the security services immediately.

12. What is the best defense to prevent hacking via wireless access?
That's all about authentication, and smart rules, and AI. Is it connecting from China and I am not in China, I just drove the car. And pure authentication rules, geographic rules, using biometry, and have extra limitations like how far a person should be to perform an action. If he's around and it's via internet it really needs some layers of authentication and checking. Is it you, checked through Google authenticator. The hacker will always miss something. He will not have your phone, he will not have your key. Maybe if I want to do something remote, my key should ask me to do something or my phone asks me to do something.

13. What is the possible solution to mitigate security risks?
Same things, authentication, security layers, smart rules, all of that.

14. Could vehicular communication systems like Vehicle-to-vehicle or vehicle-to-infrastructure communication pose security risks?
Absolutely. This is going to be applicable when we start to use connected driving. It's like automated driving, but also working with other cars on the highway. So fully automated driving, nobody drives with his hands anymore. Everything is sensors and autopilot. Then you'll have the risk where people are able to tweak the rules of engagement between the cars. Able to send signals to all the cars around you to stop so you can pass. Or you can send a distress signal to the cars, so they go to the right, so you can move on. These are things that I can think about and will going to be used because if nobody drives, there is going to be special software for police, ambulances, and fire trucks. Maybe you can copy or tweak that software and use it in your car. Use other software to jam or make other cars to stop. For example, you are driving

a Tesla on adaptive cruise control, if I'm in the car in front and I break, the Tesla breaks. This can cause an accident behind the Tesla. If you want to do harm with these sensors like in the military, you can build a little device, hang it on my car, and the other cars stop.

15. Is there a difference in terms of security between the different types of automotive network communications protocols (LIN, CAN, MOST, FlexRay)?
It comes again to how you put those things into the architecture and how you put an authentication layer behind them. These are nice functionalities, but again it's great to have them but you need that authentication built-in. I can imagine LIN and CAN too, or the enhanced versions of the first protocols with authentication, and with best practices as well in how to use it.

16. Could the encryption of network communication protocol data improve security?
Of course, without encryption it's not going to work. If you talk security, we'll always talk encryption. You don't need to encrypt everything. You need to encrypt the areas where we have outside communication, or communication between the user and the car. Inside the car, as long as there is a layer behind them, I don't think it's a problem. It's a must. Encryption in security is always the weakest layer if you don't have it, it's the entry point, you can see traffic, copy it, and replay it.

Why do you think manufacturers aren't doing it already?
When you build cars, and then secure, and do audits when the software has baked, and everything is all in, you are too late. It's getting the guys in the beginning and its needs to be encrypted, and then the developers can work, and then we have an encrypted product. So again, push security efforts to the beginning, and not to the end.

17. All new cars sold in the EEA has an integrated E-call feature which requires a cellular connection, do you think this service is secure?
I think it can be very secure. Because it's a mobile phone, and it's one way. It gives data only when you press it and it will call a verified number. Only if you play with that then you can do something, but normally I think it's safe. Basically, it's a one-line thing that can be secured easily.

Is it possible that someone calls the car and can listen through the microphone?
From the outside you shouldn't be able to do that because it's a one-way thing, it's a one-way traffic. It's me in a trench, I can't get out, I can't reach my phone, I push that emergency button, that's me calling the center which is verified, the number is hardcoded in that system, and they are able to help me, and that's it. I don't want them to call me. That would be unsafe, because that means someone else can call me. So, one way is the way, it's like a bacon.

18. What do you think about standardization like AUTOSAR, ISO, and others?
I don't know about them, and I haven't studied them but if they are security standards, like we use in ICS, and IT, best practices, architecture pushing security to the front, If they have these three things I am very happy. Because standards come from security people, they sit together from experts talk what they see, and learnt from past accidents, and that's always a good thing. Standards are a beautiful thing for our world because it gives us education and a line to put at the customer side and also the customer can embrace it and work on it. You have a mutual thing instead of me telling you what security is. And we agree on standards by experts and specifically for our industry.

Should cars be tested and rated based on it's security?
Always. I think since security certification, and compliance that's the only way to force manufacturers, and also other people to deliver products and vehicles that are tested in a way that it's not going to be obvious to hack. It needs some exception or some very unknown reason to be hacked and yes, I always think the way they push it right now just for money and for market share, that's contra, the other way around. We need to push them back and say: okay, not yet, we need to test it for security. And that's for your own benefits Mr. Vendor.

From which brand would you buy a new car considering security?
I want to buy a Tesla. I am not thinking about security at the moment, I just want to try the security when I am in, because I haven't try it I just test drove it. I don't hear a lot of things right now yet about Tesla, more about other things. I think Tesla at this moment is OK. I don't hear problems about users saying: hey someone is moving my car with the autopark feature. I haven't heard about those things yet, so I would feel safe inside a Tesla.

Appendix H

Interview transcript H

2. What is your opinion on the current state of in vehicle IT security?
For the cars on the road now, it's not great. We will see better security in the cars of tomorrow. But, due to the complexity of the systems, it will be very challenging to the get to the point that cars are just as secure as an iPhone. It will be a long time from now. Therefore, actors with a sufficiently large budget, will always be able to hack cars.

3. Are connected cars less or more secure than "offline" cars, why?
I do not think connected cars are more or less secure than "offline" cars. The risk however, for connected cars, is much higher. The loss or damage when a scalable threat materializes (like remote attacks do) is potentially much higher than a singular threat that may materialize on an "offline" car.

4. Where do manufacturers spend a considerable amount of attention/time/money, and where should they spend more?
There are different manufacturers active in the automotive industry and they spend their money differently. Some buy security expertise by buying a company, some set up their own security companies, some invest in their own personnel and other rely on their suppliers for security. Therefore, it is very hard to say something generic about what manufactures spend their money on.

5.How much attention/time/money do manufacturers spend on IT security in contrast with the previous question?
See previous answer.

6. What is the biggest problem in automotive IoT security in 2019?
The complexity of the systems implemented for a modern car prevents manufactuers from implementing (very) effective security measures.

7. How did the automotive IoT security change over the last five years?
There's definitely a drive to make security in modern cars more mature. Examples are the numerous initiatives like AUTOSAR, SAE J3061, ISO 21434, UNECE WP.29, etc.

8. What are the weak points of connected cars?
The interfaces that make allow it to be connected.

9. What is the most likely attack vector on a connected car?
Its wireless interfaces (e.g. wifi, Bluetooth, cellular, etc.) and the software that can be accessed through these interfaces.

10. What is the best defence to prevent hacking in general?
Focus on the biggest risks first. It will not possible to solve everything at the same time.

11. What is the best defence to prevent hacking via direct physical access?
This is especially difficult. Hardware security (e.g. secure boot, hardware crypto, etc.) will be required in order to withstand physical attackers. Then, you need to make sure that all the

interfaces exposed to a hacker with physical access are secure as well. The local attack surface is N orders larger than the remote attack surface.

13. What is the possible solution to mitigate security risks?

There will be no silver bullet. Security needs to the part of the development process of a product.

14. Could vehicular communication systems like Vehicle-to-vehicle or vehicle-to-infrastructure communication pose security risks?
It adds to the attack surface of a modern car. So yes.

15. Is there a difference in terms of security between the different types of automotive network communications protocols (LIN, CAN, MOST, FlexRay)?
From a software point of view it does not matter too much: attacker controlled data will end up at potentially exploitable software. Nonetheless, the physical characteristics of these interfaces impact security. For example, the interfaces that place nodes on a bus (i.e. CAN) impact security as any node can send (and receive) messages to any node on the bus.

16. Could the encryption of network communication protocol data improve security?
Definitely. Secure communications will definitely mitigate a few threats.

17. All new cars sold in the EEA has an integrated E-call feature which requires a cellular connection, do you think this service is safe?
It adds to the attack surface of a modern car. I do not know if it's safe.

18. Would you like to add something?
Cars can only be safe if they are secure.

Appendix I

Interview transcript I

2. What is your opinion on the current state of in vehicle IT security?
It pretty much varies across the brands, so obviously the more premium brands tend to invest more in security. After a bit of research, you can tell who does better things. Unfortunately, there is no guideline, so it is very hard to make sure where the car manufacturers actually are in term of security maturity. There is no standard when it comes to what features should they have already implemented. Everybody is going at their own pace. In general, we got to a point where automotive manufacturers cannot produce cars without cyber security in mind, however everything is really at the beginning, and unfortunately, we are doing 'bolt-on' security rather than security by design. So, we are still in the bolt-on phase.

3. Are connected cars less or more secure than "offline" cars, why?
If you buy a Porsche 911 from 1970 which will be all mechanical, obviously it will be much more secure, no doubt about that. The reason is simple, connected cars started to use radio wave features. Not just internet connectivity, but Bluetooth, remote key less entry, remote key fobs, digital radio, RDS, and so on. When the cars were purely mechanical, CAN bus was not the standard choice. In the transition when CAN bus, or LIN bus first appeared, obviously attacks were possible on the bus itself. At that time, the technology was so new that the tools which we have available right now were not available for like every guy on the street. Execution of any attack was very expensive, and it was not worth it to do it. No one really thought about that. The information was hard to get because internet did not exist really like we know it today.

4. Where do manufacturers spend a considerable amount of attention/time/money, and where should they spend more?
Currently it depends on the department. Engineering department they are trying to secure the on-boards side, everything which is in the vehicle. IT department, they are trying to secure everything between the vehicle and the back-end, and the back-end itself. The biggest problem is that usually these departments exist on top to each other. At the end of the day they have to talk to each-other. It's not like a standard, that's one of the investment which I think that needs to happen. Sort of make the security more streamlined, which is better between the engineering department and the IT department.
I would say that there is a trend to be both away from the software-based security to the embedded system, or hardware-based security. Which is costly however, there are specific use-cases where it can really resolve a lot of headaches. I think the key investment should be working with the researchers, or use some hardware-based security, which is gonna be much more difficult to attack then current software which we still rely on.

5. How much attention/time/money do manufacturers spend on IT security in contrast with the previous question?
There are two things, IT security and then engineering security. Very often the resources are misplaced. They are doing projects on securing the car data brokerage, which splits data about the location from driver and based on the approximate location, they might suggest gas stations or certain habits and so on. Obviously, some kind of security, because they need more anonymized data, not traceable back to the driver. So, I think that their priority is focusing on

gamification of connected vehicles, or providing some extra comfort to driver, like car data brokerage. They should really focus on securing the platform, or choosing the platform, an extensive platform, which they can use in the coming years, and use it like a framework. I would basically say that stop trying to go with the trend and try to clean your house first and secure the vehicle before moving to the next step with gamification or new features.

6. What is the biggest problem in automotive IoT security in 2019?
The biggest problem is really that the automotive car manufacturers do not really have the security requirements written anywhere for the tier 1 suppliers or for the suppliers in general. It is very hard for them to actually dictate what security features they would expect from their suppliers. In the end it results in receiving products which are not like fully thought through and in the end the car manufacturers have to put some bolt on security to make everything work as desired. The problem which is linked to that as well is because of the security requirements are not very well described, researchers and academia often start a research on something which is relevant for automotive, but they forgot to consider some of the automotive environment conditions, like power consumption, electromagnetic interference resistance, temperature ranges. At the end they create a research where they suggest certain direction which is not really viable for the automotive industry to go, because the technology is too fragile on the high or low end of temperatures, or it doesn't take well the huge temperature differences and so on. The third problem is the lack of framework, standard, or guideline which would really specify in an actionable way how a secure vehicle should look like, and what are the basic features that should be applied or that the vehicle should be compliant with.
AUTOSAR already exists and it's fine, the problem is that they still have the option to follow it or to not follow it. There is nothing which would enforce it like it is enforced with the safety regulations. For safety, you have a clear checklist, on which if you are not able to pass certain things the car simply cannot be commercially used. There are many that already exist, there is AUTOSAT, there is the National Highway traffic safety administration (NHTSA) in the US which also released some security guidelines, but everything is optional. There is nothing really that pushes you to adhere, and I think that's quite problematic.

Do you think the government should enforce it?
Better than government, because every time the government get involved it's much worse that it was. It needs a body like the one making the safety regulations, and they basically need to say: AUTOSAR has this so you need to take the architecture from AUTOSAR because it's proven, and you can base your framework on top of that. I think that some enforcement of security would really help the company, because very often they are quite lost about whether they should use this AUTOSAR because they think that, or someone told them that there is something better and so on. So, standardization, and better course of direction would help.

7. How did the automotive IoT security change over the last five years?
There was a significant pivot. If you take the infotainment system for instance, they moved from operating systems which were not designed primarily to automotive, to an operating system which is already designed for automotive applications. There are embedded system architectures that over the five years resolved quiet a lot of cyber security problems, but the biggest change is that somebody realize that the components needs to be automotive dedicated. I think that the pivoting to the purpose for automotive is quite interesting, and it's the biggest shift, which brings the biggest added value. All the connectivity stuff, like you can connect your car to the internet and you can have an access point, etc. I don't really consider

them as a breakthrough because that's only a matter of time, it's functionally easy to adopt, but they need to have a strong foundation. And the foundation is something that is actually changing quite drastically every day.

8. What are the weak points of connected cars?

The most afraid scenario is that you are going to be able to control the car remotely. The other concern is the privacy of the driver or drivers, and obviously data protection. Things will get collected, not necessarily with the full awareness of the consequences for the users, and so on. It might be the problem of these three things. Privacy, cyber security, and data.

9. What is the most likely attack vector on a connected car?

The easiest attack is always the cheapest. If you break the window of the car, or if you tow it somewhere and disassemble it for parts, that's obviously the easiest part. We have to a conclusion that when you have an attacker who wants to gain financial benefits from a car, you need to make sure that if he disassembles the cars into different pieces, that the parts that he wants to sell on the black market will not work. You can guarantee that the thief will not have the appetite to steal the car. So that can help you get rid of the thieves. When you have a cyber security attacker, the easiest access is through the back-end. Online services, web applications, infrastructure. It's much easier and more accessible to use infrastructure and web application penetration testing then to teach an attacker on how to desolder a chip from the motherboard, reverse engineer it, recompile it, put it back in, solder it in with the correct checksum. The most likely vector currently how you can exploit fleet cars is through the back-end. Back-end of whatever source, back-end used for data aggregation, or for firmware over the air update is quite important. But if you have a skilled attacker with physical access to the car, he can just plug his tools, like oscilloscope, and can reverse engineer the CAN bus and so on. Even though this is easy, I don't considerate the easiest, straightforward vector that majority of attackers without physical access can think of.

10. What is the best defense to prevent hacking in general?

Right now, some of the things that are really annoying when you are trying to hack into cars, is obviously encryption on the communication bus inside the car. You're unable to replay, you're unable to spoof messages. That's one of the most annoying factors when it comes to on board security. Additional annoying factor for a hacker is that companies are getting pretty good in securing the debugging access of the motherboard and system on chip devices. Meaning that before the car leaves the factory close all the jtag ports, any other debugging interfaces, and they make sure that without getting the car back to the factory, or without triggering some function that only 2 or 3 dealerships are advised to make. You are essentially unable to make modification to the car. These are pretty good steps and detouring steps on the on-board side. A side that have a secure boot, and secured integrity of the operating system on the infotainment unit, so it gets much harder to replace the unit, or change the booting sequence to force it to boot it to a different state. For the off-board part, it's very critical to make the application and infrastructure security hygiene correctly. An example, if you would have a transport channel with TCP/IP for your firmware the air update platform properly secured with TLS 1.3 for the future. It's not really going to resolve your problem when the web application which you host or run has default admin-admin credentials across all the customer base, and where you can for example extract the firmware and upload your own without anybody noticing. Resulting in you pushing the poisoned firmware back into the car. From the off-board to on-board integration I think that really the key task is to make foundations secure.

11. What is the best defense to prevent hacking via direct physical access?

What is happening right now is when you're connected to the OBD port under the steering wheel, you have a secure gateway which is essentially a device in the car sitting on the bus and inside the firewalls, so it prevents certain messages to travel to certain regions. That's one thing, then every ECU currently has some sort of internal logic that for instance when it knows or when it's relevant for him that the car is doing more than 5 km/h it is essentially going to be disable any debug access, so you are not able to issue any debugging command for example. I am not considering physical access that you're unable to get to the wires, I mean you can always throw a brick onto the window, get in, cut the wires and get access. So I'm really talking about how you protect the wires from like cyber security perspective, or how you protect the leaf components. The next trend, because it is already quite invasive, is detecting solution. There are many firms out there like Arilou, Argus, Enigmatos which are focusing on creating something they call hardware fingerprinting where using analogue ways and specific physical phenomenon which they see on the wire, they are able to determine which component is actually has that differentiating physical phenomenon. Based on that they are able to build a map, and determine with the help of the user obviously, what connection is valid and what components are valid and so on. If there is a topology change or if there is something suspicious, let's say a new analogue signature of device will appear, most likely there is an anomaly or that you plugged in your own tools like a raspberry pi, or whatever. These are the hardware fingerprinting, and then obviously with being able to detect in the future you should be able to prevent something. But this is very far away.

12. What is the best defense to prevent hacking via wireless access?

Via wireless access it is slightly more difficult. Because of the replay attack possibilities, interference, you can even cause a lot of havoc with the Denial of Service attack. In general when you're talking about the functional spec, you can for instance use bounding protocols, meaning you are measuring certain distance of a receiver or transceiver and it's going to help you measure at the same time when or at a similar time when someone tries to replay the attack, sort of record what your key-fob is sending and try to replay it. It's basically not going to work, because the combination of the signature and the physical phenomenon is not valid. Another option might be establishing like pool based physical unclonable function-based keys, where each key would really have a unique and unclonable chip, or small device which will make it irreplaceable. All the security can be built on top of that. Also, there is a lot of technologies and approaches where we don't really have a reliable security solution like GPS. You are always getting not only the location but also the time, and there are really no fixes to that. The only fix could be to correlate GPS data from the sensor data in the car directly to really get the sense of what is happening with the car, and maybe warn the user that his GPS connection is being tempered because the value from your powertrain indicates that your car is moving while your navigation map still shows that you're not moving anywhere.

14. Could vehicular communication systems like Vehicle-to-vehicle or vehicle-to-infrastructure communication pose security risks?

Definitely yes, not only to the vehicle themselves but vice-versa to the infrastructure itself. The concept of the dedicated vehicle area networks they are called VANETs. It's like in very early stages, so the V2X, V2V as well. I think we always again adopt where we started with this discussion meaning there will probably be some physical unclonable function. So, you don't essentially need to do these types of work anymore manually.

15. Is there a difference in terms of security between the different types of automotive network communications protocols (LIN, CAN, MOST, FlexRay)?

By design none of them has any security, so they are insecure. Out of these that you named, FlexRay is arguable the most secure because it is most the most difficult to execute replay attacks. Because of all the timing and needs for the token to be able to speak etc...

16. Could the encryption of network communication protocol data improve security?
To some extent, meaning that if you're able to ensure that the private keys are stored somewhere securely then yes. The problem is that then you are going to face small sensors and actuators where actually they have a lack of computing power for these operations. Actually, it makes a big difference, where it comes to when or if the companies want to go down this route or not.

17. All new cars sold in the EEA has an integrated E-call feature which requires a cellular connection, do you think this service is safe?
I think so. We did some tests and there is nothing which would be dodgy.

18. Would you like to add something?
Maybe one thing is, I am going back to AUTOSAR about the open source or closed source topic. I think that it really makes sense to start using open products for vehicles in general. You can make use of for example Automotive Grade Linux called AGL, which is currently being developed, and gets traction and understanding from more and more car manufacturers. Simply because some of the code source of real-time operating systems like QNX or Harman. They were never originally intended to be made for automotive, and you can recognize that the security of the design is bolt-on. Manufacturers would prefer something where the security is built from scratch and which can be scrutinized by bounty programs, where more people can participate and so on. Which is true for the AGl automotive grade Linux.

Should an agency / government regulate connected car security standards, testing etc?
Primarily the car manufacturers themselves, and specialized firms as well. And they should also consult a lot with researchers, about new attack vectors, and to stay ahead from the attackers. We discussed that probably the good way to secure the car itself is to secure the on-boards and we don't want to make the cars impossible to exploit. We want to make the exploits so expensive that it will become much more economical to buy a new car or buy spare parts. This is what car manufacturers should do. Many of them are doing it. Some of them are starting with it. We basically it the cyber-security garage same way as you have garages for the muscle cars where they are measuring the performance, tuning engines. Each of the manufacturer should have a similar garage which would be dedicated to cyber-security. Some of the premium brands have it and smaller firms are getting into it. The consultancies like Accenture, should have the same facility to stay competent and be able to offer it to car manufacturers. Obviously, the car manufacturers they should have more consulting firms to do the security testing because the more eyes the more you can see. They also need to find a partner or ideally partners that are not only going to be with them during the security testing engagements during the final product but being with them during the development of a new release of a car. Very often car manufacturers are overwhelmed by their own processes and for that basically they don't really have the attention to the details. So, it is very good to hire someone who is not just working on automotive but on medical, telecommunication, aeronautics, or other industries who can bring various angles and different resolutions to the same problems. Because that in the end is what changes the perception and can make the cars more secure.

What kind of car would you buy considering its security?

If I would consider security I would consider a Daimler car. Because it is widely known that they spend a lot of time, and a lot of resources on security.

Appendix J

Interview transcript J

2. What is your opinion on the current state of in vehicle IT security?

While the Functional Safety is well developed in the automotive field we see a lack in the general Security knowledge and mentality, best explanation to this is that the functional safety standard ISO26262 has been around for years while the Automotive Security Standard is still not released ISO21434. We do have standards like J3061 and some important projects like HEAVENS and EVITA.

3. Are connected cars less or more secure than "offline" cars, why?

Suppliers often waste a lot of time in fixing security flaws in their security concepts at the end of the project, these mistakes can be fixed if they spend considerable time performing TARA and clarifying all security requirements at the start of the project.

4. Where do manufacturers spend a considerable amount of attention/time/money, and where should they spend more?

Suppliers should definitely spend more money time and effort in educating their employees about automotive security.

7 & 7. How did the automotive IoT security change over the last five years? What are the weak points of connected cars?

Automotive IOT evolved a lot over the last few years as CAR to X communication is available in almost all modern cars, this offered a lot of new weak interfaces (LTE, WIFI, switches ..) that can be a target for attacks.

Appendix K

Survey questions

1. What is your age?
   a. Under 18
   b. 18 – 30
   c. 31 – 45
   d. 46 – 60
   e. Above 60
2. What is your gender?
   a. Male
   b. Female
   c. Other
   d. Prefer not to say
3. What's your education level?
   a. Primary education
   b. High school graduate
   c. Bachelor's degree
   d. Master's degree
   e. PhD degree
4. Which industry are you working in or studying for?
   a. Agro-Industries
   b. Energy and Utilities
   c. Manufacturing
   d. Services
   e. Construction
   f. Public Sector
   g. Communications
   h. Other industry
   i. Retired
5. Do you own/lease a car?
   a. Yes, it has connected features
   b. Yes, without connected features
   c. No
6. Do you think currently sold cars are continuously connected to the internet?
   a. Yes
   b. Maybe
   c. No
7. Do you think that a continuous internet connection would raise or lower the level of car security?
   a. Raise
   b. Lower

   c. No change

8. Are you familiar with the possibility of hacking connected cars?
   a. Extremely familiar
   b. Very familiar
   c. Moderately familiar
   d. Slightly familiar
   e. Not familiar at all
9. Knowing connected cars can be vulnerable to hacking, would you still buy one?
   a. Yes
   b. Yes, but with precaution
   c. No
10. Would you prefer to buy a connected car or an offline car?
    a. Connected car
    b. Offline car