Automotive Cyber Security

Threat modeling of the AUTOSAR standard

Master's thesis in Computer Systems and Networks

ADI KARAHASANOVIC

Department of Computer Science and Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY
UNIVERSITY OF GOTHENBURG
Gothenburg, Sweden 2016

Master's thesis 2016

Automotive Cyber Security

Threat modeling of the AUTOSAR standard

ADI KARAHASANOVIC

Department of Computer Science and Engineering
Division of Computer Systems and Networks
Chalmers University of Technology
University of Gothenburg
Gothenburg, Sweden 2016

Automotive Cyber Security
Threat modeling of the AUTOSAR standard
ADI KARAHASANOVIC

Supervisor: Magnus Almgren, Department of Computer Science and Engineering
Examiner: Erland Jonsson, Department of Computer Science and Engineering

Master's Thesis 2016
Department of Computer Science and Engineering
Division of Computer Systems and Networks
Chalmers University of Technology and University of Gothenburg
SE-412 96 Gothenburg, Sweden
Telephone +46 31 772 1000

Cover: Image of a connected car with a transparent net made out of padlocks representing a security mechanism.[76]

Gothenburg, Sweden 2016

Automotive Cyber Security
Threat modeling of the AUTOSAR standard
ADI KARAHASANOVIC
Department of Computer Science and Engineering
Chalmers University of Technology and University of Gothenburg

Abstract

We live in a world that is getting more interconnected by each day and we are witnessing a global change where all the devices in our surroundings are becoming "smart" and connected to the Internet. The automotive industry is also a part of this change. Today's vehicles have more than 150 small computers (ECUs) inside them creating an in-vehicle network, which controls the vehicle functions similar to the fly-by-wire concept in aviation. These vehicles have multiple connection points to the Internet to offer their users a variety of on-line services.

As every device that connects to the Internet gets exposed to various on-line threats, so does the connected vehicle. This is why it is becoming increasingly relevant to address the cyber-security issues in the automotive industry. AUTOSAR is the de-facto standard for the Automotive embedded software today and 80% of global production is based on this standard. This thesis first investigates currently employed security mechanisms in the AUTOSAR after which it shows how the threat modeling process is adapted and adjusted in order to be applied to the connected car and the AUTOSAR standard. The result of this process provided a list of potential security vulnerabilities of the connected car and the AUTOSAR standard. The overall contribution to the automotive industry is achieved by providing two threat modeling processes that are specifically adapted for this domain and can be applied to upcoming releases of the AUTOSAR platform as well as the connected car itself.

Keywords: AUTOSAR, connected car, threat model, security, STRIDE, TARA.

Acknowledgements

First I would like to express my sincere gratitude to my university supervisor, associate professor Magnus Almgren, for his continuous support and guidance throughout this thesis. I would also like to express gratitude to my supervisor at Combitech, Pierre Kleberger, for giving me the opportunity to do this thesis and providing me with his invaluable support and knowledge. Besides my supervisor in Combitech I would also like to thank my other colleagues that have also contributed to my work, especially Ulf Cornelisson, Jimmy Haeggström and Jonas Lindholm.

A significant part of this thesis was made possible because of the equipment and the support provided by the Arccore company and their staff, especially I would like to thank Lukas Suter and Michael Lundell. And last but not least, I would like to thank Cristiano Corradini from the NCC Group and Timothy Casey from Intel Security for their valuable support and the knowledge they shared with me.

Adi Karahasanovic, Gothenburg, November 2016

Contents

List of Figures

List of Tables

1
Introduction

The world is getting more interconnected for every day that passes. The devices we use in our daily life are now "smart" devices connected to the Internet and may be controlled remotely from anywhere in the world. Smart homes, smart grids, smart appliances (e.g. smart refrigerators, smart washing machines, smart air-conditioning) are just the beginning and even the vehicles we use are becoming "smart". Most of the new cars are connected to the Internet in order to provide a more diverse experience for the end-user. Vehicles today have more than 100 million lines of code which is considerably larger than an F-35 fighter jet or a Boeing 787 passenger plane [98]. Just recently we have witnessed a historic event when the Tesla company launched their new Model 3 and received more than 325 000 orders in just one week [116]. This model has very sophisticated software, an auto-pilot option and various connection points to the Internet.

As the production of these types of cars increases, we will witness a big change in the automotive industry. One key issue that is and will be very important in the future is the cyber-security of these cars. The chief technology officer at Veracode, Chris Wysopal explains [118]:

> *"Exposing a car to the Internet makes it vulnerable to cyber-attacks due to poorly written software, which could render the car unstable or dangerous"*

There have already been a number of successful cyber-attacks on connected vehicles such as the attacks on Jeep Cherokee [20], Tesla S model [121], Nissan electric car [119] and Chevrolet Corvette [120]. The attack that seemingly got the most attention was the Jeep Cherokee attack, because this was the first remote attack on a vehicle. As such, it was a wake-up call for the entire automotive industry to pay more attention to securing these vehicles from online threats. Before this attack happened the main argument from the automotive industry on why the cyber-security of the cars was not a priority, was that any attack required physical access to the car itself. This is why the remote attack performed on the Jeep Cherokee had such a big impact on the automotive industry and its approach to cyber-security.

The goal of this thesis is to better understand the security mechanisms in the software architecture of the connected car. In particular, we study AUTOSAR (AUTomotive Open System Architecture), which is the name of the system standard that is used by both the car manufacturers and the electronic equipment suppliers [6]. The

purpose of this standard is to decrease the complexity of the automotive electronics architectures, enable companies to work together on improving this standard, while also allowing them to compete on implementations. AUTOSAR is used to create a standardised operating system (interface) for embedded controllers (ECUs) to enable developers to design software independently of the actual hardware supplier. As it has become a de facto standard in the vehicle industry, it is important to investigate it in detail from a security perspective.

One of the main parts of the vehicles is the internal vehicle network. This network connects all the Electronic Control Units (ECUs) in the car and each ECU is responsible for a different car function. When companies use AUTOSAR, they can develop software much faster without knowing the ECU details, on which the software will run.

The research on security vulnerabilities of this standard is increasing as the automotive industry is becoming more aware of the risk from on-line threats. The problem is that the new vehicles for the upcoming 2-3 years are practically "done" so any research that indicates potential vulnerabilities today may not be implemented in the vehicles before 2020. Part of the software can be additionally upgraded through service centers but the applications are all based on the AUTOSAR standard and the operating system of the vehicle is developed according to the AUTOSAR specification. Even if we manage to update the operating system, each application that was running on the old version would need to be updated in order to work on the new version of the operating system. Another concern is the data that the vehicles contains and that is needed for the proper function of the vehicle. Even updating from Windows 7 to Windows 10 can be very difficult if you want to keep all your applications and data running smoothly, but performing this on a vehicle that is not even designed to have this as an option, is nearly impossible. The computer industry is much more advanced than the automotive industry in this sense which is why this type of update is still not recommended for vehicles.

A comprehensive cyber-security evaluation of this standard is very much needed, which is why this thesis presents a threat model of this standard. The purpose of the threat modeling process is to evaluate the AUTOSAR standard from the security perspective and possibly give suggestions as to what could be done to make the standard more secure.

Before starting this process, the current threat modeling methods are adapted and adjusted in order to apply them to the connected car and the AUTOSAR standard. The created threat modeling process can be used in future releases of AUTOSAR to ensure a continued high security level of the architecture. All the vulnerabilities discovered are documented and categorized. This information will be valuable in order to see which parts of the AUTOSAR architecture are potentially vulnerable and need more attention, as well as to protect the applications running on AUTOSAR based systems.

1.1 Aim of work

The aim of this thesis is to first adapt and then apply different threat modeling methods to the connected car and the underlying AUTOSAR standard as well as evaluate their efficiency. After the initial research, we chose two methods and adapted them to be applicable to the automotive industry. As a consequence of this process, the thesis provides two threat modeling methods that can be further used and applied to different systems in the automotive industry. The information gained from this thesis and the results of the threat modelling process will hopefully contribute to the improvement of cyber-security of connected vehicles.

1.2 Timeline

The thesis is constructed in the following steps:

STEP 1: Research

The main areas of research are related to connected car technologies, AUTOSAR standard, threat modeling techniques and security vulnerabilities of connected vehicles. Most of the research is focused on the AUTOSAR standard and the security mechanisms specified in the latest 4.2 release.

STEP 2: Test environment for the AUTOSAR standard

In this step, a test environment for AUTOSAR is setup. This test environment is used to perform some of the security test cases.

STEP 3: Threat model of the Connected car and AUTOSAR

This step is completed by examining scientific literature of previous attacks [102] as well as discussions with and interviews of experts (thesis partner Combitech). Access to the Vehicle ICT Arena is provided [122] in order to talk to other experts in the field, exchange ideas and gain new knowledge about the AUTOSAR platform. All major companies from Sweden are members of this Arena such as Volvo AB, Ericsson, Mitsubishi Electric, Cybercom, Delphi, Viktoria Swedish ICT.

Threat modeling techniques are adjusted and adapted so they can be applied to the connected car and the AUTOSAR standard. Specific test cases are created and each test case reflects a realistic threat that is discovered during the research phase of the thesis.

STEP 4: Results, discussion and conclusion

After the threat modeling process is finished, the results are presented and discussed. The thesis finishes with a conclusion summarizing the results of the threat modeling process and stating the contribution of the thesis to the automotive industry.

1.3 Thesis partner

The thesis work was conducted together with the supervision and support from Combitech. They describe themselves as found in [26]: *Combitech is a Nordic technical consultancy company that combines technology, environment and security. The company, which is an independent company within the defence and security group Saab AB, has around 1800 employees in 20 locations across Sweden, as well as offices in Norway and Finland. Their consultants have expertise in information security, systems safety, logistics, systems integration, systems development, robust communications, technical product information and mechanical engineering. Combitech's customers are companies with a need for reliable security solutions, authorities responsible for the protection of societal flows and players in aerospace, defence, telecommunications and all industrial segments.*

1.4 Limitations

The focus of this thesis is on the following parts:

- Research into the existing security mechanism in AUTOSAR
- Adapting a threat modelling process to the connected car and the AUTOSAR
- Documenting potential security vulnerabilities discovered

Any work or information that goes beyond the three points above will not be included in this Master thesis. The report has all the relevant information concerning the topic and excludes any unnecessary information that can lead to confusion.

1.5 Combitech AB limitations

The work in this thesis was conducted inside the Combitech AB company, because of which some of the sensitive and confidential information that was gathered during the thesis is left out of this report. This information could include some sensitive data that concerns the security vulnerabilities that are discovered during the threat modelling process, or some detailed information about the AUTOSAR architecture. This does not by any means reduce the quality and the usefulness of this report but rather prevents any misuse of the information presented here.

The sensitive data is filtered out of the report in accordance with the *Combitech AB non-disclosure agreement*. This thesis report is publicly available according to *Chalmers Agreement on Electronic Publishing in Chalmers Publication Library (CPL)* [89].

1.6 Thesis outline

This thesis is structured as follows:

- **Chapter 1** - The introduction chapter provides information about the motivation and goals of this thesis. It presents a short time-line of the thesis work and also states some limitations in the thesis project along with non-disclosure agreement (NDA) with Combitech AB.

- **Chapter 2** - The second chapter gives all the relevant background information. It describes the connected car concept and all the external entities that communicate with the car. The chapter also gives a brief history of cyber-attacks on the vehicles, and states some major concerns when it comes to vehicles security.

- **Chapter 3** - The related work chapter gives information about the sources that were used during the research stage of this thesis as well as descriptions of papers that have a similar subject as this thesis report.

- **Chapter 4** - In this chapter, an overview of AUTOSAR is presented along with the security protocols implemented in release 4.2.

- **Chapter 5** - This chapter describes existing threat modeling techniques, tools and methods.

- **Chapter 6** - After having examined the existing threat modeling methods, I selected two of them for further research, namely TARA and STRIDE. This chapter describes how I adjusted and adapted the TARA method in order for it to be applicable to the automotive industry, and more specifically to the Connected car concept.

- **Chapter 7** - This chapter describes how I modified and applied the STRIDE method to a software application that is based on the AUTOSAR standard. I used a threat modeling tool from Microsoft and a special template that was designed for the automotive industry. Additionally, I created a simulation of a small CAN network, which I used to test some of the threats found by the STRIDE method.

- **Chapter 8** - The eighth chapter summarizes the results of the threat modeling process. It provides a discussion section about the interpretation of the results and limitations of the methods.

2
Background

2.1 The Connected car

A vehicle with connection points to outside external networks, including the Internet, is the concept of the next-generation vehicles called the Connected Car. According to the Business Insider report, there will be 380 million connected cars on the road by the year 2021 [53]. These vehicles have multiple connections to the Internet and to other external networks with a common goal of improving the driving experience.

Each car consists of 100-150 ECUs (Electronic Control Units) which are small computers that are networked together and control most of the vehicle functions. Each ECU has a number of sensors and actuators attached to them. The ECUs and the internal vehicle network replace the mechanical connections with electrical systems and slowly transform the car to work on drive-by-wire technology. Some of these new systems are IPA (Intelligent Parking Assistance), BSW (Blind Spot Warning), LDWS (Lane Departure Warning System), LKS (Lane Keeping System), and they all form part of the ADAS (Advanced Driver Assistance Systems). Table 2.1 shows some of the major changes in the automotive industry [88].

Table 2.1: Changes in the automotive industry

Current automotive DNA	**New automotive DNA**
Powered by petroleum	Powered by electricity and hydrogen
Powered by internal combustion engine	Powered by electric motors
Controlled mechanically	Controlled electronically
Stand-alone	Connected
Total dependence on the driver	Semi/Full autonomous driving
No Internet connection	3G/4G, Wi-Fi, Bluetooth
Human operated	Driver-less

Today's vehicles are equipped with a number of new technologies and features that were not possible without an Internet connection. Passengers now have the option to receive service information and traffic reports through the vehicle's dedicated cellular connection. They also have the option to connect their smart-phone to the vehicle over a Bluetooth or Wi-Fi connection and use the smart-phone's Internet connection to enable some of the new features of the vehicle's entertainment center. This center enables web browsing, access to social networks, streaming of on-line content, and many other services depending on the vehicle type and manufacturer.

In the very near future vehicles will communicate with each other (V2V) and with the infrastructure around them (V2I). The idea is to reduce accidents and decrease the gas consumption by letting vehicles have more control. They will determine the speed limit, and have an established connection to the Internet and outside networks in order to collect information on traffic and road conditions – and these are just some of the major features of these technologies.

Vehicle-to-Vehicle (V2V) technology enables cars to wirelessly communicate with each other and even maintain temporary networks among themselves in order to prevent accidents and avoid traffic hazards [51]. As shown in Figure 2.1, cars will have a certain network field around them, and every car that comes in the range of that field can connect to that car in order to exchange information. This information can be related to traffic safety and security, keeping a safe distance between the two cars for preventing accidents or any other data that is meaningful to the vehicles. This technology is challenging because of its distributed nature and to implement V2V connection the car manufacturers need to agree on communication technologies and protocols that will be used. Otherwise without the mutual agreement between car manufacturers, only the cars of the same brand would be able to communicate with each other [115].

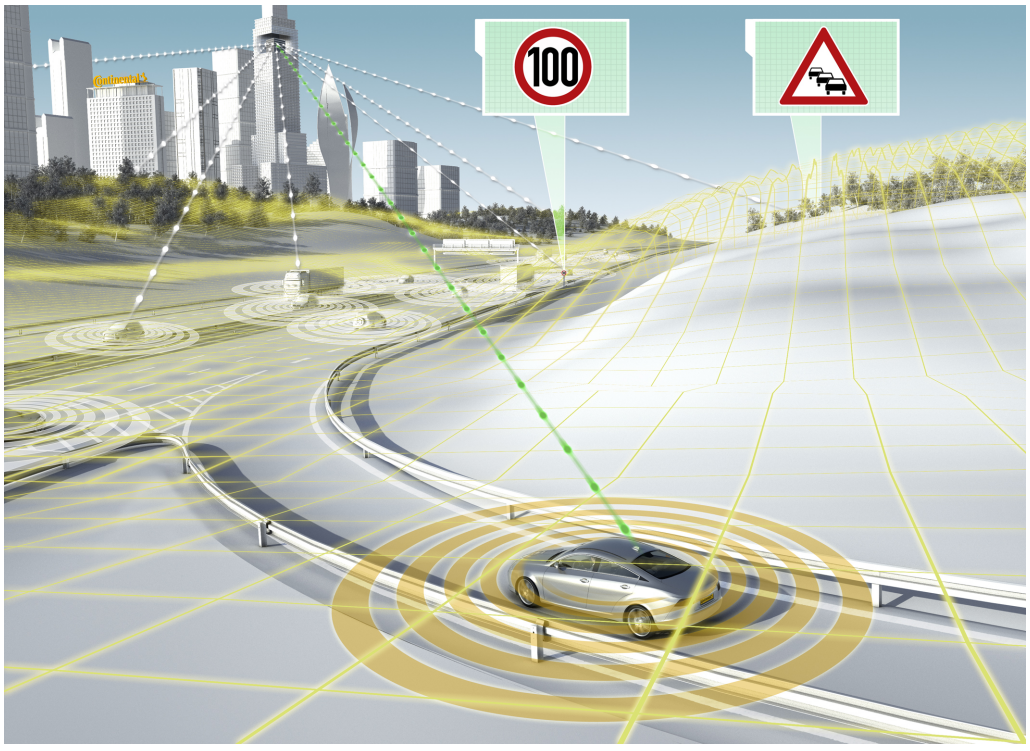

Figure 2.1: Vehicles communicate with everything in their surroundings [80]

Vehicle-to-Infrastructure (V2I) are technologies, as shown in Figure 2.1 and Figure 2.3, in which the car communicates with the environment around it, including road signs, highways, traffic lights while also receiving up-to-date information from Traffic Info centers on possible traffic jams and accidents. By collecting the

information on traffic and road conditions the vehicles can work together to reduce the traffic jams and avoid any possible accidents. In the near future when most of the vehicles will be connected cars, the traffic can be regulated by one central authority by giving suggestions to all vehicles on the best route and speed, enabling an environment without traffic jams, accidents and with less fuel consumption [115].

There is already a CAR2CAR communication consortium of European car manufacturers, equipment suppliers and other research institutions that has a common goal of enabling this technology. All major players from the European automotive industry are part of this consortium [27].

2.2 Automotive networks

As the number of electrical components in vehicles increases [71], the need for a good network that will connect these parts becomes more important. Different electrical components have different functions and as such need different types of connectivity.

Today we have four main types of automotive networking:

- **LIN (Local Interconnect Network)** - This network type provides a cost-effective solution for connecting switches, intelligent actuators, temperature or rain sensors, small motors, lamps, sun roof or heating control. It has the smallest bandwidth of all four networks which is one of the reasons why it is used in non-critical functions of the vehicle system.
- **CAN (Controller Area Network)** - The most widely used automotive network protocol. It is a single centralized network bus where all the data inside the vehicle is broadcast. This network type can be divided into two categories depending on the nature of the traffic: real-time control in power-train (SAE Class C) and body control (SAE Class B). It is used in engine timing controls, anti-lock braking systems, electronic throttle control etc.
- **Flex-Ray** - Main purpose of this network type is to support the new drive-by-wire systems such as steer-by-wire and brake-by-wire, that require good error management along with high transmission rates.
- **MOST (Media Oriented Systems Transport)** - Has the largest bandwidth of all networks and it is mainly used for audio, video, navigation and telecommunications systems. It is most suitable for real-time audio and video transmission applications.

Each of these networks has different attributes and application areas. Table 2.2 shows the main differences between them.

Table 2.2: Overview of automotive networks [71]

	LIN	CAN	Flex-Ray	MOST
Application	Low-level communication systems	Soft real-time systems	Hard real-time systems (X-by-wire)	Multimedia, telematics
Control	Single-master	Multi-master	Multi-master	Timing master
Bus access	Polling	CSMA/CA	TDMA/FTDMA	TDM/CSMA
Bandwidth	19.6 kBit/s	500 kBit/s	10 Mbit/s	24.8 Mbit/s
Data bytes per frame	0 to 8	0 to 8	0 to 254	0 to 60
Redundant channel	Not supported	Not supported	Two channels	Not supported
Physical layer	Electrical (single wire)	Electrical (twisted pair)	Optical, electrical	Mainly optical

Figure 2.2 shows the internal structure of the in-vehicle networks and how they are organised in smaller sub-networks. Each sub-network is based on a different network technology depending on the requirements of the systems connected to that specific network. For example, the head unit is responsible for the audio and video transmission which requires a faster bandwidth, therefore it uses the MOST network type.

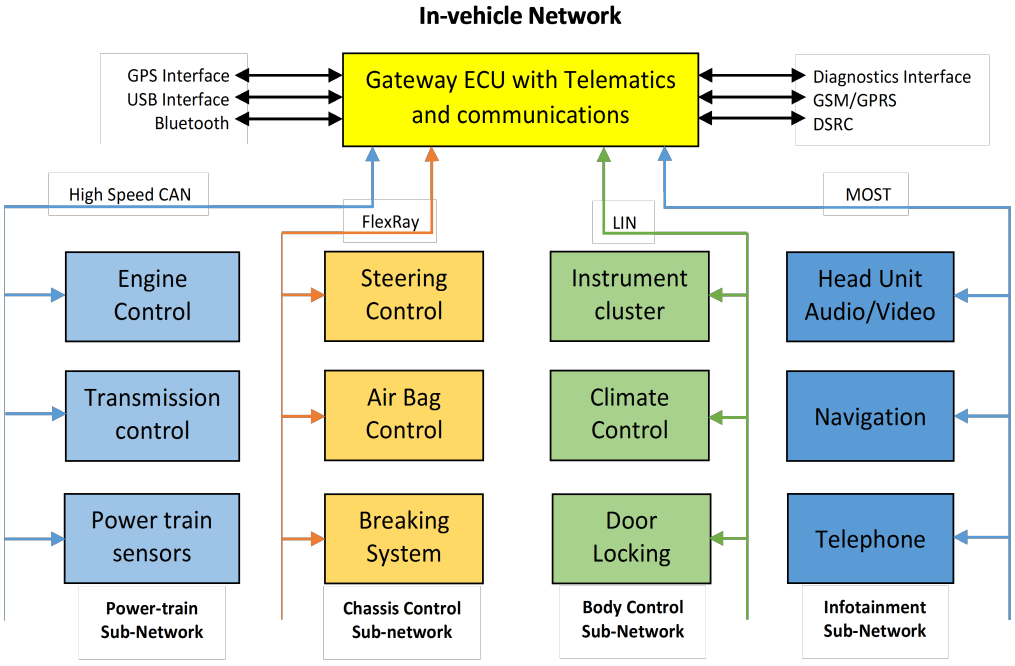

Figure 2.2: Overview of internal vehicle sub-networks [103]

2.3 Security concerns

As cars are getting more interconnected with other vehicles and the environment around them, the security threats will continue to increase. Before the concept of a connected car was introduced, the automotive industry did not pay much attention to cyber-security because the attackers required physical access to perform an attack.

Today we have cars with multiple connection points to outside networks including a connection to the Internet. In addition to the LTE and WiFi connections, Figure 2.3 shows all the additional services that the connected car will have in the future. Car2Cloud technology represents all internal services available because of the existence of Internet connections.

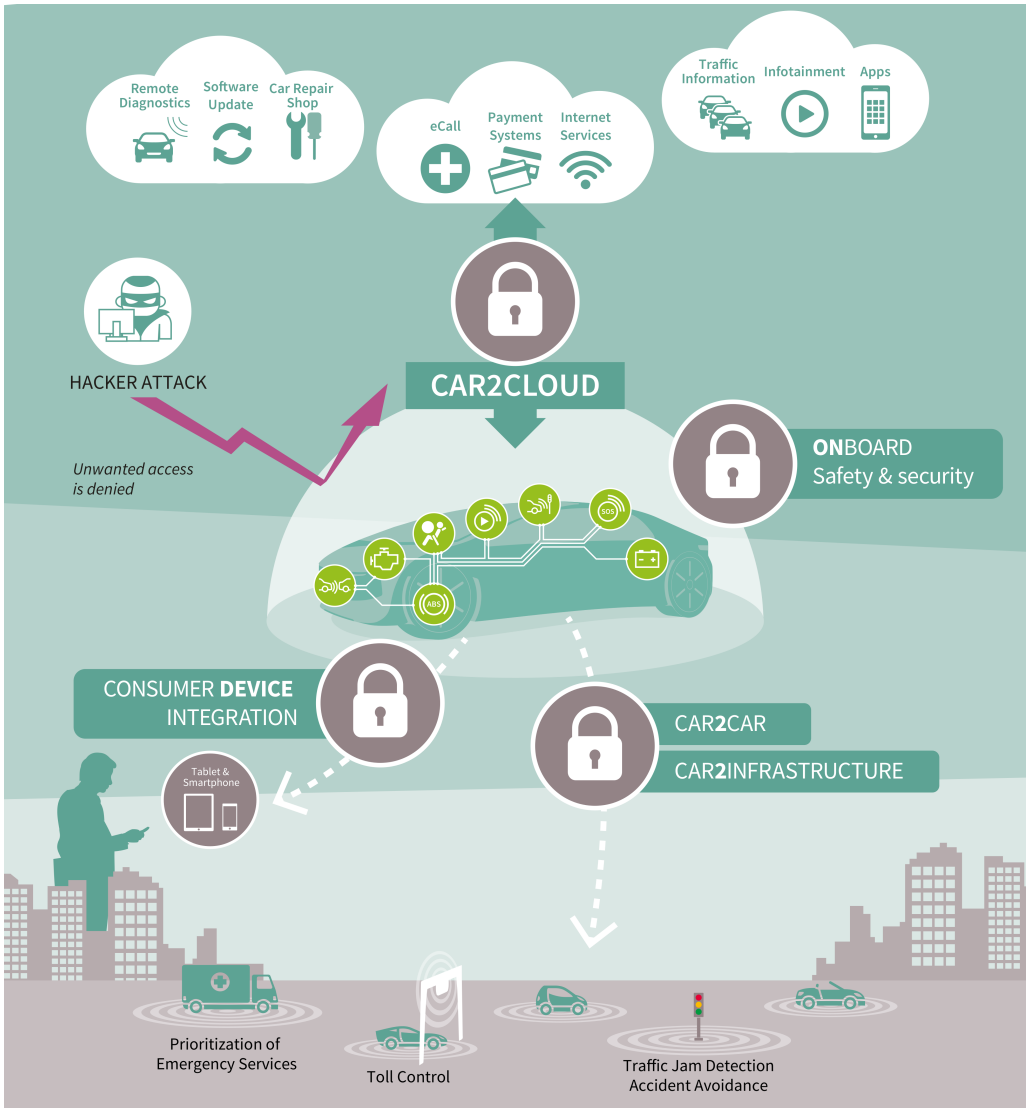

Figure 2.3: The connected car concept [108]

Figure 2.4 illustrates the 15 most vulnerable points of a connected car according to the Intel security report from 2015 [124]. Each of these 15 points actually represents an advanced feature of the connected car. Most of these features are implemented through dedicated ECUs that are in charge of those specific functions. The ECUs are interconnected through the internal vehicle network called CAN (Controller Area Network). If any of these features gets compromised, the entire internal network is potentially in danger since these ECUs are interconnected, and depending on the attacker's expertise some of the critical systems can be controlled.

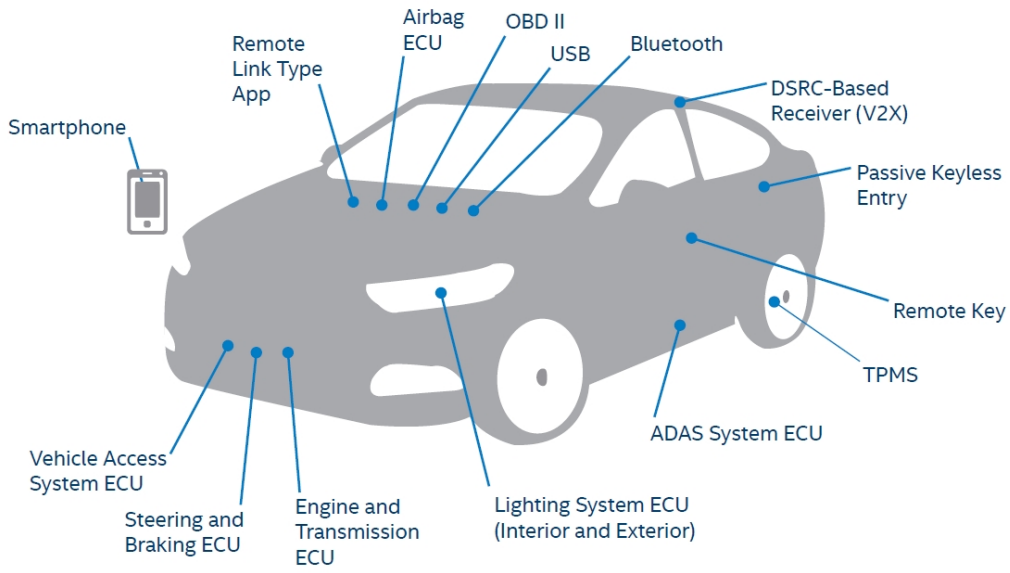

Figure 2.4: The 15 weakest points of a connected car according to Intel [124]

The four main difficulties in securing the connected car are in the following areas:

- **Over-the-air updates (OTA)** - The connected cars are very similar to computers, as they have a very complex software architecture and a variety of applications to enable some of the new enhanced features. As time goes by, this software needs to be updated with new bug-fixes or security patches to prevent discovered vulnerabilities. These updates are challenging for the automotive industry because some updates could be very critical and potentially dangerous for the safety of the driver and passengers if not installed on time. If the car cannot be updated due to the vehicle not always being on-line, whose responsibility will it be if outdated software causes an accident? At the time of writing this thesis, only Tesla has remote updates enabled while others require a visit to the service center [65, 16].

- **Low computational power** - Because of the long vehicle life-cycle and the environment conditions such as humidity, vibration and temperature, the computational power of vehicles is low. This is to the attackers advantage because they can leverage the power of stronger computers. Moreover, as the vehicle gets older, the more advanced technologies will be developed comparing to the car's production year, making it even more easy to exploit [16].

- **Difficult to monitor** - It is difficult to monitor the status of the automotive electronics by a certified authority, as the car is not always connected to the Internet [16].

- **Cost** - One of the major difficulties is, of course, the costs of making all the vehicle software secure. Companies would need to employ more people and they would need to change their entire development process in order to incorporate security from the very beginning.

- **No Safety without Security** - Just one infected car on the road represents a potential hazard for all the surrounding vehicles, and each new security vulnerability exposes new safety issues e.g. if security mechanisms fail to ensure the integrity of messages sent by the braking system [16].

As cyber-security becomes a more important attribute of the vehicles, so will the car manufacturers have to employ more security experts in this field. The new car manufacturer, Tesla, already has a team of security experts reviewing Tesla's software and hardware designs, making sure there are no security flaws. One thing that all car manufacturers have in common is that they use AUTOSAR as the platform for most of the vehicle's ECUs, which is why it was chosen for the threat modeling process in this thesis. More detailed information about the AUTOSAR standard and the security mechanisms that it employs, will be given in the next chapter.

From the scientific literature, e.g. Martin Bohner et al. [67], we can see how the design of software architectures such as AUTOSAR has a big influence on the overall cyber-security of vehicles. It demonstrates how tightly interconnected safety and security are in the automotive industry, and that we cannot have safety without high quality security mechanisms. Since security threats are changing dynamically it is much more difficult to design security mechanisms that will ensure the integrity of the system throughout the whole life-cycle. Creating a threat model will give more information on the current threats on the system and provide more details and recommendations for improving the security of the entire vehicle system. There are typically three approaches to threat modeling: attacker-centric, software-centric and asset centric [109]. Each of them is based on a different security perspective and combined together will provide an extensive analysis of the AUTOSAR standard. Chapter 5 will give more details about different threat modeling methods that are divided between the three approaches to threat modeling.

2.4 History of cyber-attacks on vehicles

The research on automotive cyber-security became more focused and open in 2003 when the Embedded Security in Cars (ESCAR) Conference was founded. In the beginning the research in this area did not arouse much media attention and was not considered important by the consumers. But in the last few years cyber-security of vehicles got a lot more attention, mainly because of some very significant attacks that were published and discovered by researchers. This section gives a brief overview on the most recent and most interesting vulnerabilities that were discovered. Table 2.3 shows a summary of these attacks while a short description is given in the following sections.

Table 2.3: Overview of cyber-attacks on vehicles

Vehicle OEM	Type of attack	Severity	Section
Jeep Cherokee	Cellular network - Entertainment system	High	2.4.1
GM Chevy Impala	Physical access – Buffer overflow	Low	2.4.2
BMW	Spoofed Wi-Fi hotspot	High	2.4.3
Corvette	OBD dongle exploited	Medium	2.4.4
Tesla S model	Physical access – Trojan	Low	2.4.5
Nissan LEAF	Wireless attack – Mobile app	Medium	2.4.6
Tesla All models	Wireless attack – Wi-Fi	High	2.4.7

2.4.1 Jeep Cherokee

The turning point for the entire automotive industry was the, now famous, **Jeep Cherokee** attack in 2015, when two security researchers remotely accessed a car on the highway and gained control over its functions, including the critical ones such as the steering wheel, brakes etc. They were able to do this because of a vulnerability in the car's entertainment system that used a cellular connection in order to provide access to Internet and other services. Uconnect is the name of the entertainment system that uses the Sprint cellular network to connect to the Internet. The Uconnect entertainment system had a specific D-Bus port (6667), known as the Diagnostic Bus, that was open for connections and consequently vulnerable. In normal conditions this port should not be open for external connections, but only used for internal communication between different processes. A targeted attack was possible if the IP-address was known, otherwise a port scan of port 6667 across IP ranges 21.0.0.0/8 and 25.0.0.0/8 would give a response from all the vulnerable vehicles across the country. Just by communicating with this port the attacker could get GPS information, VIN number etc. 1.4 million cars were affected by this vulnerability [20].

2.4.2 General Motors

What the public was not much aware of at this point was that a very similar attack was discovered long before the Jeep Cherokee attack, but on this occasion it was not made public. Researchers at the University of California at San Diego and the University of Washington that discovered the vulnerability chose to just show the exact exploit to the GM company and in the public announcement they did not reveal the make and the model of the vehicle itself (**General Motors' 2009 Chevy Impala**). Because of this, the attack did not get a lot of media coverage compared to the Jeep Cherokee attack. The interesting part is that the initial attack that allowed the researchers access to the system was a specifically designed mp3 file, which, when played to the in-car call system, granted access to the car's system and most of its critical functions. The mp3 file triggered a vulnerability in the car's computer, known as the buffer overflow [78].

2.4.3 BMW

Since the Jeep Cherokee attack and up until now, there have been a number of discovered security vulnerabilities in cars of some of the major OEMs. The **BMW's** ConnectedDrive service was discovered to have a security flaw that could allow malicious users to remotely unlock the car. More than 2.2 million cars were exposed to this vulnerability. Researchers created a fake cellular network, using a portable cellular base station in the proximity of the car. This enabled the car's internal SIM-based cellular connection to connect to this network instead of the real network, enabling the remote unlock attack. The car was tricked into communicating with a spoofed BMW server instead of the real one. The attack was possible because the connection was not encrypted. The patch that was later on published added the HTTPS encryption to the connection between the car and the outside BMWs servers [38].

2.4.4 Corvette

Another recent attack targeted a dongle that is installed into the car's OBD port, which is used by insurance companies to track driver behavior in order to reduce insurance cost by identifying "safe" drivers. In the **Corvette** model that the researchers used, they were able to apply the brakes remotely by exploiting a vulnerability in the dongle. And this was all done by sending a very specific text message to the dongle connected to the OBD port inside the car. In other vehicles that have more features, even more functions could be controlled using this method [120].

2.4.5 Tesla S model

In 2015, Kevin Mahaffey from the mobile security company Lookout and Marc Rogers from DDoS mitigation service CloudFlare unveiled a way to attack the **Tesla S** model and also to gain remote access to its features. In this case, the researchers first only had physical access to the car, but after installing the Trojan into the system they could acquire remote access. The flaw was quickly fixed by Tesla [121].

2.4.6 Nissan LEAF

One of the most recent security issues with a connected car concerns the **Nissan LEAFs** Electric car, one of the best selling electric cars in the world. Researcher Troy Hunt discovered a vulnerability in the Nissan Companion App, used in the smart-phone for providing access to some of the car's functions including remote access. The researcher set-up an interesting experiment where he performed a remote attack from his location in Australia to a car located in the UK. He was able to remotely turn on/off the air conditioning, seat heating and also access the car's GPS history. Although not dangerous, the attack still provides a clear example of how the security of a connected car is still not taken seriously [119].

2.4.7 Tesla all models

The last known security issue with a connected car, to this date, is with the Tesla vehicles. Researchers from the Chinese firm Tencent discovered a flaw in the Wi-Fi connection of the Tesla S model that allowed the researchers to remotely access the driving system and even activate the brakes from a remote location.

The initial flaw that allowed them further access to the vehicle's internal CAN network, was discovered in the Tesla's web browser, based on the open source browser framework WebKit. By exploiting this flaw they were able to run malicious code on the browser, when a specifically designed web site was visited. In order to present this attack, they created their own hot-spot named Tesla Guest, which is a common name for a hot-spot at Tesla dealership stores, and set-up the password to be the same one as in the Tesla shop. This ensured that a Tesla vehicle would auto-connect to their hot-spot and automatically load the malicious web site. Two additional vulnerabilities allowed the attackers to gain control: a flaw in the Linux operating system, and another flaw that allowed them to overwrite the firmware of the gateway system separating the head unit from the internal CAN network. After this attack was publicized, Tesla released a security patch within 10 days. The patch was rather extensive and introduced a new security control known as code signing, which prevented any firmware updates unless they were digitally singed by a cryptographic key that only Tesla possesses [79].

All the research and the vulnerabilities discovered in these examples were made in a controlled environment and had no negative impact, nor did they cause any harm. Up to now, there have been no publicly known cyber-attacks on vehicles that were meant to cause harm to people or the OEMs reputation, but this does not mean it will not happen in the future.

2.5 Summary

This chapter provides the most relevant information concerning the connected car concept and security issues that the automotive industry will have to consider when constructing the software for these cars. It should be more than obvious that the security of vehicles has to be a priority when designing automotive software because safety of the passengers can be threatened. All the new features of the vehicles today are very tempting for users to use and enjoy but in order to safely implement them and ensure passenger safety, vehicle manufacturers have to make security a priority, especially in the future when autonomous driving becomes a reality.

3
Related work

This section gives an overview of the literature related to the topic of this thesis. It is divided into six sections depending on the type of document involved. Most of the papers related to the topic refer to security analysis and risk assessment of the connected car concept. Since 80% of vehicle production is based on the AUTOSAR standard, we can assume that these papers are closely related to the subject of this thesis.

Only two papers, previous thesis reports from Chalmers, are similar to the topic of this thesis and deal with threat modeling of the AUTOSAR standard and the vehicles based on this standard. More details on these and other papers are given in the following sections while the main difference between these papers and the thesis at hand is given in chapter 3.7.

3.1 Books

When it comes to threat modeling, one book that can not be avoided is the one written by Adam Shostak [109]. This book has a very extensive description of all the threat modeling methods along with examples and guides on how to apply each of them. The author is well known in the security community and is considered as one of the top experts in threat modeling methods. Because of this, the book was used as a starting point in the research and also as a main reference in this thesis.

Another book about threat modeling was written by Tony Uceda Velez and Marco M. Morana [82] and published in 2015. Both authors have an extensive background in security, Marco Morana is a director of Minded Security while Tony Velez is the CEO of VerSprite. The book gives some more recent information about threat modeling process but also a more detailed description of the asset centric approach called PASTA. The book was used as an extension to the one written by Adam Shostak.

The author managed to find only two books in which the main topic was automotive cyber-security. The first one, written in 2005, "Embedded Security in Cars - Securing Current and Future Automotive IT Applications" [60] comes from the University of Bochum, Germany. This is probably one of the first books that gives a comprehensive description of the role that cyber security has in the automotive industry. The book was one of the starting points to get the sense of the area of automotive security in order to understand all the aspects and concerns.

The second book was published in 2009 [73], and was written by one of the same authors of the previous book, Dr.-Ing. Marko Wolf, a professor at the University of Bochum with an extensive background in the automotive industry and security. The book gives an overview of potential threats to vehicles, analysis of the attack methods and provides recommendations on secure engineering design that should improve the overall security of vehicles. The book was used to get a better understanding of automotive security.

3.2 Automotive cyber-security guidelines

The cyber-security area of the automotive industry has become a very important aspect in this industry which is why, today, we have three different security guidelines that the manufacturers in the automotive industry should follow in order to make their vehicles more secure. It is important to mention these guidelines as they are closely related to the topic of this thesis and represent a major contribution to the automotive industry when it comes to security.

The first guideline that was published in 2011, is from the EVITA project [35] (E-Safety Vehicle Intrusion Protected Applications). This project was co-funded by the European Commission. The goal was to design an architecture for vehicle networks that would prevent any tampering with the security-relevant components inside the vehicles and also protect any sensitive data from being compromised from an outside attack.

Just two years after the published results of the EVITA project, an information promotion agency (IPA) based in Japan, released a document with a similar goal as the one from the EVITA project. The document titled "Approaches for Vehicle Information Security" [57] represents potential threats to vehicles along with security measures that need to be implemented in order to mitigate these threats.

After these two guidelines were released from the **EU** and the **Asia** agency, the next step was to have an **international** guidebook on security requirements for vehicles. This guidebook was published in January 2016 by the Society of American Engineers (SAE) [87]. This guidebook gives straightforward recommendations on how cyber-security should be designed in the cyber-physical vehicle systems from the initial concept phase to the final decommissioning phase.

The last two papers that are worth mentioning in this section are in the "Automotive security Best Practices" category. One paper comes from Intel Security [124] while the other one is written by the NHTSA (National Highway Traffic Safety Administration Agency) [90]. In the reports, both companies give their opinion on how the automotive industry should approach the cyber-security issues of vehicles and they also give recommendations on which security mechanisms should be implemented.

3.3 Threat analysis

This section presents papers that deal with threat analysis and risk assessments with the connected car as the target. Each paper has a different approach to this process which is why it is important to present these papers and show the difference between their approach and the approach taken in this thesis. The papers were used to get a better understanding of the work that has already been done in the area of automotive cyber security.

In 2010, researchers Roesner et al. from the University of California and the University of Washington published one of the first papers analysing the security of a modern vehicle [59]. They conducted a series of experiments and road tests on a modern vehicle, and found that it was possible to manipulate the vehicle by injecting false messages on the CAN network. They never disclosed the type of car they used for the test and their research did not get much attention because the attacker needed physical access in order to perform this type of attack.

The next year, in 2011, the same researchers Roesner et al. published a new paper to address the low media attention to the previous paper. In this paper [102] the researchers analysed the external attack surface of a modern vehicle and they managed to exploit some of the connection points such as the Bluetooth function and the vehicle's cellular connection used for the telematics system. But again the research, even though groundbreaking, did not get enough media attention because the team did not release the information about the methods they used and they never disclosed the type of vehicle they tested.

The paper by Wolf et al. [74] from 2012, was one of the first ones that gave a new risk analysis method that was tailored to the needs of the automotive industry. The method considers two factors, potential damage and the probability of a successful cyber attack. The goal of the method is to avoid over securing or under securing different parts of the vehicle which in return would decrease costs.

In 2012, researchers Mohamad et al. from the Eindhoven University of Technology and Wolf et al. from the Malaysia University of Technology provided a taxonomy [64] of security and privacy in the connected vehicle. The taxonomy classifies the existing threats to the connected car along with the solutions that mitigate these threats. The paper was used to get a better insight into the threat landscape and different security mechanism that could be implemented in the connected car.

Researchers Ibarra et al. from the MIRA Ltd company that deals with vehicle engineering, in 2013, tried to form a threat analysis method [31] that would be used in parallel with the already established method for functional safety analysis. The method would be an extension to the safety analysis method based on the ISO 26262, but the problem was that the definition of hazard in the ISO 26262 standard was much narrower than the one needed for the cyber security threats. The conclusion was that further work was needed in order to synchronise safety and security.

The U.S. National Highway Traffic Safety Administration (NHTSA) released a report [19] in 2014 in which they described a composite modeling approach of cyber security threats to the connected vehicles. The company created threat models and threat reports of different types of possible threats to vehicles along with a list of potential cyber attacks.

A security expert, Slawomir Jasek from the company SecuRing, wrote a paper [105] on the attack surfaces of the connected car. In the paper he clearly outlines all the vulnerable areas of the car that could be potentially exploited by an attacker. The most vulnerable ones, according to the paper, are the connection points to the outside networks such as Wi-Fi connection, bluetooth, cellular connection etc.

Another paper that presents a new method for security analysis of vehicle was proposed by Mundhenk et al. [93] The described method uses Continuous-Time Markov chains (CTMC) to model the architecture at system-level, afterwords the model is analyzed for confidentiality, integrity and availability by using probabilistic model checking. The method was shown as successful in finding vulnerabilities in the architecture which were not found by analysis done on component or sub-system level.

One more attempt to combine safety and security risk analysis was done by Machera et al. [41]. The authors combined the automotive HARA (hazard analysis and risk assessment) with the security domain threat modeling STRIDE. The resulting method was named SAHARA (Safety-Aware Hazard Analysis and Risk Assessment). This method is used to determine the impact of security threats to the safety concepts in the vehicle at system level. The method is useful for assessing remote attacks and attacks affecting entire vehicle fleets, because it determines the damage potential and affected users.

In a recent paper, Islam et al. [81] gave some more information about the process of risk assessment for the automotive embedded systems. Authors state four security objectives: safety, financial, operational, and privacy and legislation – also referred to as impact levels. The authors combine the threat analysis with risk assessment in order to determine a security level that indicates what level of protection a certain part of the system needs. It also provides information about the counter measures that need to be implemented to avoid unreasonable risk.

3.4 Work by security consultants in industry

Chris Valasek and Charlie Miller are probably the two most noted names when it comes to automotive cyber security. They were the duo that made the entire automotive industry question their security mechanisms when they published a detailed paper on how they remotely attacked a Jeep Cherokee and managed to gain control over its critical functions [20]. This was not the only paper the security duo published. Earlier they examined the attack surfaces of a number of vehicles, stated the information about each attack surface and concluded which car is the most vulnerable one and which one is the most secure [25]. Another paper they wrote [23] stated

information about different methods that can be used on two types of car models with detailed manuals and tools for performing these attacks.

In order to make this research available to more security experts they also wrote a paper about testing an individual ECU that people can buy cheaply online and then use it to test some of the methods from the papers mentioned previously. The paper concluded with an instruction on how to attach the ECU to a go-cart and test it while the vehicle is in motion [24].

3.5 Documented vulnerabilities

This section gives a brief description of different research papers that revealed real vulnerabilities of different vehicles. It demonstrates the importance of this thesis by providing evidence from the research community about the significances of vehicle cyber security.

The first natural place to start with vulnerabilities would be the RFID immobilizers that are used by car keys to lock/unlock the car. A paper by Richardson [4] gives examples of five different types of attacks that can allow the attacker to gain access to the car and drive it away, without any physical damage to the car.

A paper by Enev et al. [68] demonstrates how a driver's privacy could be violated if someone could get access to the information transferred over the internal CAN network. The paper demonstrates that by analysing driving behavior data from the vehicle, that was collected by different vehicle sensors, authors were able to identify almost every driver with amazing accuracy.

More examples on how privacy can be violated by acquiring data from vehicles was given in a paper by Hoppe et al. [113]. By attacking the ECU gateway an attacker can gain access to the inside CAN network and perform sniffing attacks that would allow them to listen and capture all the packets exchanged on the internal CAN network.

"Security and privacy in automotive on-board networks" is a PhD dissertation by Hendrik Schweppe [46] that gives extensive information about the security and privacy issues of the connected car. It gives a very detailed view on this area compared to previous papers in this section.

Telematic units of modern vehicles have already shown some vulnerabilities even though car manufacturers are trying to make them more secure. Even the cars without the telematics unit can be upgraded with aftermarket telematic units that connect to the car via the OBD port. The paper by Foster et al. [47] examines the security implications of these devices and concludes that it is not hard for an attacker to remotely compromise these devices and gain access to critical functions.

The vehicle's TPMS (Tire Pressure Monitoring System) sensors communicate over a wireless network giving input to the vehicle about the tire pressure. A paper by Roufa et al. [48] examined the TPMS sensors and determined that it is possible to track drivers by eavesdropping on the TPMS sensors because each car transmits a specific ID number along with the tire pressure information. The ID is different for every car and can be used to identify a specific car. Another vulnerability that they found is the spoofing of sensor messages, which in return sends false data to the vehicle, making the car instrument show false data to the driver, such as warning messages about low tire pressure when in fact the pressure is normal.

3.6 Previous Master theses

During the literature survey, multiple previous master theses have been found that deal with the automotive cyber security [61, 58, 110, 100]. Each of them has a different approach but the main idea of presenting possible threats and vulnerabilities of the connected car is something that each thesis has discussed. Only two master theses have dealt with the AUTOSAR standard and performed threat modeling.

The first one, written by Ha et al. [1], is about the communication flow in the AUTOSAR standard that includes the security module SecOC. The authors created DFDs for the information flow with the security module along with making a small implementation of the CSM module. The DFDs were used to apply two different types of the STRIDE method. Even though they performed threat modeling of part of the AUTOSAR standard, the thesis is still very different from the one described in this report. The thesis in this report is carrying out threat modeling of a software application that is based on the AUTOSAR standard, the Interior Light application. The DFDs used for the threat modeling are different and the SecOC module is not used. Another difference is the existence of an implementation of the Interior Light application on which some of the threats found during the STRIDE threat modeling process were validated.

The second thesis, written by Hasslund et al. [55], did not used any DFD diagrams nor did they use the STRIDE method. They used an evaluation hardware board similar to the one used in this thesis but again they implemented a different part of the AUTOSAR on which they performed the tests. The focus of their AUTOSAR implementation and testing was the Diagnostics Module of the AUTOSAR architecture, which is different to the Interior Light software component used in this thesis.

3.7 Summary

As seen throughout this chapter, there is a substantial increase in the research concerning security in the automotive industry. This trend will keep rising as the automotive industry is going through major changes and security is a big part of that change. The main topics of all the papers in this chapter is the attack surface, vulnerabilities, attack methods and different techniques that can be used in order to assess the risks that come with the connected car. AUTOSAR is the main automotive standard and covers over 80% of vehicles as stated in the introduction chapter which is why it is important to address the security issues of this standard. Only two papers were found that deal with security issues of the AUTOSAR standard and this is why it is important to extend this research because if the security of this standard improves - the security of all vehicles that use it will also improve!

The main focus of this thesis is on two points, which are not addressed in any other paper as far as the author knows.

- First, the thesis applies an attacker-centric approach to the connected car which has not been done before. Threat agents, methods, motivations, needed skills and other information are all summarized in the thesis based on the literature survey and an extensive consultation with the experts from the field.

- Second, the thesis performs a STRIDE threat modeling method on one limited part of the AUTOSAR standard using the Microsoft Threat modeling tool. There are two important distinctions here compared to similar work: the template used in the MS threat modeling tool was created by experts in the NCC Group company, and one threat from each category of the STRIDE method was tested on a real system simulated by the hardware board containing the implementation of the AUTOSAR application.

4

Overview of the AUTOSAR standard

AUTOSAR (Automotive Open System Architecture) was founded in 2003, and today it is the de facto standard for automotive OEMs and their suppliers. The goal was to develop an architecture, independent of the underlying ECU hardware, that the automotive industry can use in order to reduce the increasing complexity of software in modern vehicles [28]. AUTOSAR makes an abstract layer of the underlying hardware, so that the applications written on-top of AUTOSAR are independent from the actual supplier of the ECU hardware. Volvo Group was the first commercial vehicle manufacturer that adopted AUTOSAR [54].

This architecture provides a uniform standard that the automotive industry can use, while leaving room for competitive development of innovative applications and functionality [28]. The benefit of using the AUTOSAR standard is the reduction of time it takes to develop new applications by reusing the application interfaces and AUTOSAR's core functions. AUTOSAR prepares a standardized template and work flow when developing automotive applications and ensures re-usability and reliability [62].

4.1 AUTOSAR organizational structure

The AUTOSAR partnership has a three tier organizational structure that consists of:

- Core partners
- Premium partners and Development partners
- Associate partners

Figure 4.1 shows the internal structure of the AUTOSAR partnership with the logos of the major member companies. The organization has over 200 partners worldwide. Only the core partners have the organizational and administrative control, while all partners use the AUTOSAR standard and contribute to its further development. The usage of AUTOSAR is not limited to just the automotive industry but can also be used in marine, railway power-train, agriculture/forest machinery, construction/mining machinery, compressors or pumps and power generators. However, it is not +used in the aviation industry [7].

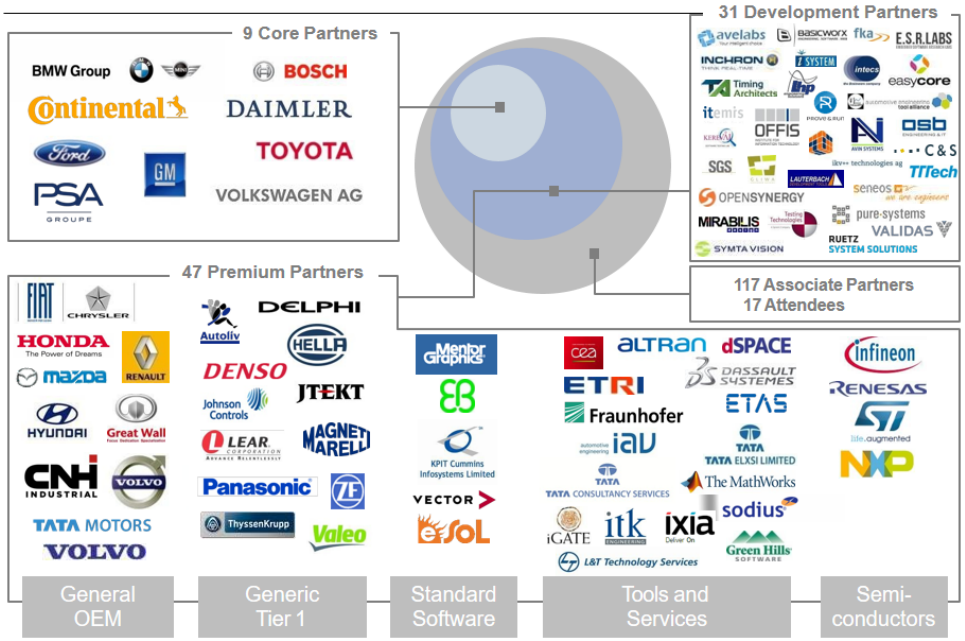

Figure 4.1: Overview of the AUTOSAR partnership program [6]

4.2 Software architecture

The AUTOSAR standard documentation guides companies and the automotive industry in designing and implementing software in their vehicles. By adopting the AUTOSAR standard, companies can develop software solutions that are independent of the hardware they are running on, and this software can run on any ECU in the vehicle. This is the reason why the AUTOSAR platform is also called a hardware-independent architecture. Figure 4.2 shows the difference in the vehicle software architecture when the AUTOSAR standard is adopted.

Besides defining the architecture and the interfaces, this standard also defines a design flow that specifies how software should be mapped to the ECUs during the development cycle. This process ensures that all the companies use the same approach for implementing this standard into their vehicles. The high configurability of the AUTOSAR implementation allows it to be adjusted to the specific needs of each company and guides the application software that each company is developing for their specific vehicles. This is one of the main goals of this standard, to use the knowledge and experience of every member company in order to improve and further develop the standard on one hand, while on the other hand allow each company to develop its own software applications and configure the AUTOSAR implementation to their own needs. This allows companies to “Cooperate on standards, compete on implementation” which is the official AUTOSAR motto [72, 7].

AUTOSAR provides detailed specification for:

- Software Architecture
- Software Development Methodology
- Standardized Application Interfaces (APIs) [6]

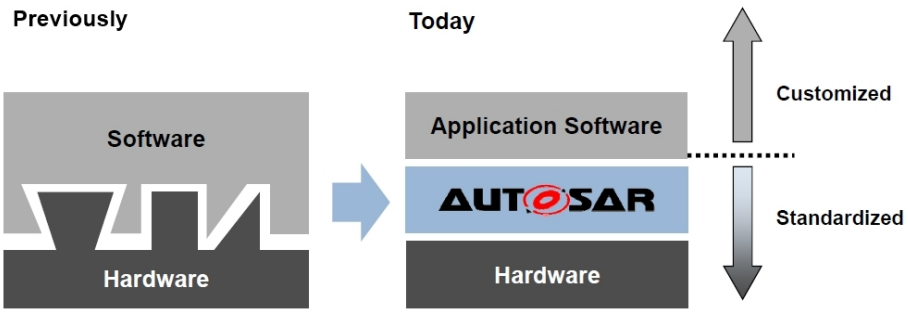

Figure 4.2: AUTOSAR hardware-independent architecture [6]

Figure 4.3 shows the three-layered architecture of the AUTOSAR standard: Application layer, Run-time Environment (RTE) layer and the Basic Software (BSW) layer that consist of four sub-layers. Each of the sub-layers offers different services as illustrated in Figure 4.4. The highest layer is the **Application layer** which contains the software components (SWCs). AUTOSAR application (e.g.ABS or the seat heating control) consist of several SWCs which provide the core functions that are used by the AUTOSAR application. The AUTOSAR SWC is an atomic piece of software that can not be divided and is located on one ECU. The SWCs used in this thesis are sensor and actuator SWCs.

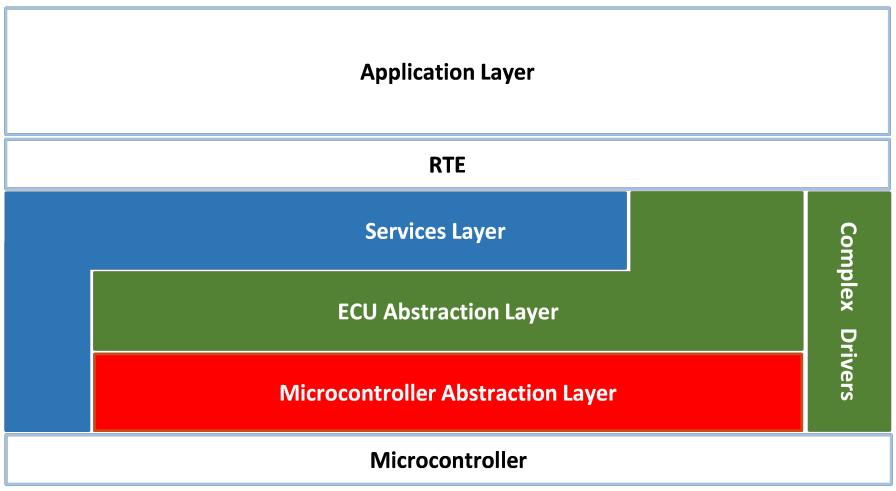

Figure 4.3: The layered AUTOSAR architecture [6]

The sensor SWC reads the state of the sensor and provides that data to other components or the AUTOSAR application, while the actuator SWC sets the state of an actuator located on that ECU. SWCs are ECU dependent while the AUTOSAR

application is not dependent on one ECU. The interaction between the AUTOSAR application and the AUTOSAR SWCs is achieved through the RTE layer [63].

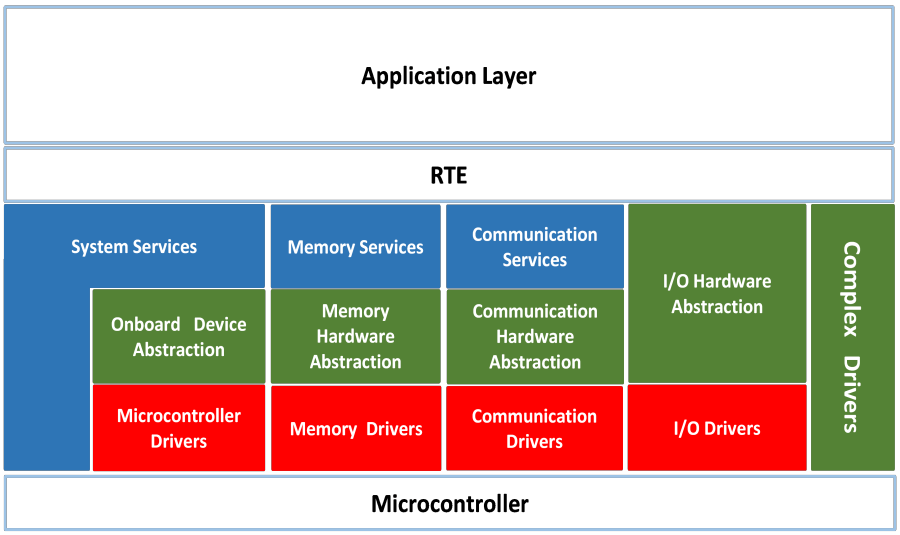

Figure 4.4: Each sub-layer of the BSW layer offers different services [6]

The **Run-time environment (RTE) layer** provides communication ability between the SWCs and the Basic Software Layer. Because of this layer SWCs can be used on different ECUs, independent of the ECU vendor. This layer is ECU specific because the specification of the ECU determines the correct access to the right communication channel [15, 7].

Basic Software layer (Figure 4.3) consist of [15, 7]:

- **Services layer** - This is the highest layer and provides basic services for applications, RTE and BSW modules. It offers operating system functions i.e. communication services, memory services, diagnostic services, ECU state management and logical and temporal program flow monitoring. The layer also contains the main security mechanism of the AUTOSAR standard: CSM cryptographic module and the SecOC security module, which are explained in more detail in section 4.3.
- **ECU Abstraction layer** - This layer responds to the functions of the applications and interacts with the drivers of the micro-controller abstraction layer. It provides an Application Programming Interface to devices regardless of their location (internal/external micro-controller) including external devices. This layer makes the higher layers independent of the ECU layout.
- **Micro-controller Abstraction layer** - This layer contains drivers for direct access to the micro-controller and internal parameters. It makes higher layers independent of the micro-controller.
- **Complex Drivers layer** - The layer provides the ability to integrate special purpose functions such as drivers for devices that are not specified with the AUTOSAR standard. This layer accesses the micro-controller directly.

Figure 4.5 illustrates a more detailed view of the AUTOSAR software architecture including the paths of internal communication between different layers and internal services. One new concept shown in Figure 4.5 is the AUTOSAR Virtual Functional Bus (VFB), which defines a communication framework between SWCs. VFB abstracts the communication away from the hardware in such a way that it does not matter if two communicating SWCs are on the same ECU or on different ECUs [123].

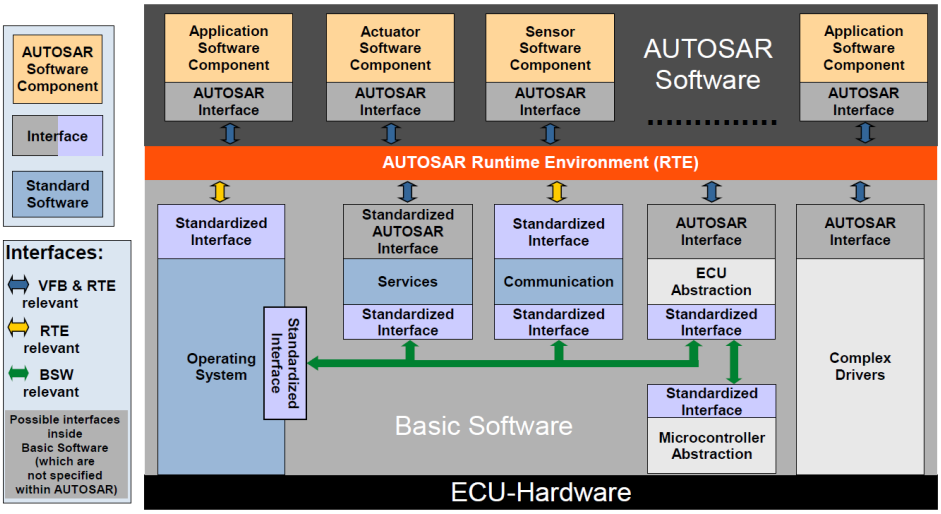

Figure 4.5: AUTOSAR software architecture - Components and Interfaces [6]

4.3 Security features

The AUTOSAR standard defines important security mechanisms that are used by the SWCs and other software modules implemented into the vehicle system. It further specifies interfaces and procedures for ensuring secure on-board communication while the rest of the security mechanisms and implementations are left for the OEMs to decide on. OEMs choose the cryptographic algorithms and encryption techniques that they want to implement and use in the vehicle system [8]. The three main security mechanism in the AUTOSAR are:

- **CSM** - Crypto Service Manager
- **CAL** - Crypto Abstraction Library
- **SecOC** - Secure On-Board Communication

4.3.1 CSM and CAL

AUTOSAR specifies two crypto modules. The first one is the **Crypto Service Manager (CSM)** which is located in the Service layer of the BSW and provides services for higher level applications. CSM allows for different applications to use the same service to access different cryptographic primitives (cryptographic algorithms). One application may need access to an MD5 digest while another application needs to compute a SHA1 digest. This service of the CSM module can be accessed only locally inside that ECU, while any access between different ECUs needs to be specified

and implemented as a separate mechanism, as this is not defined by AUTOSAR [8].

The second crypto module is the **Crypto Abstraction Layer (CAL)** which is a static library with a very similar function as the CSM. The library is used to provide cryptographic functionality directly by bypassing the run-time environment (RTE). CAL provides C-functions that can be called directly from other software modules such as BSW, Software components (SWCs) or even the Complex Drivers layer. The services of the CAL depend on the underlying cryptographic algorithms and are always executed as a call to a function. Because CAL is a library, it is not related to any of the layers in the AUTOSAR architecture [8].

Neither CSM nor CAL define any actual cryptographic algorithms, instead this is specified by the implementers based on their choice or the customer needs. Because the OEMs choose the cryptographic algorithms to be implemented, it is very important that their security staff are experienced and know which algorithms are secure to use. Both modules provide an input parameter used to select a certain cryptographic algorithm that was requested by a software component or a module. The following cryptographic functions may be implemented by the CSM or CAL [8]:

- Hash calculations
- Generation and verification of message authentication codes (MAC)
- Random number generation
- Encryption and decryption using symmetrical algorithms
- Encryption and decryption using asymmetrical algorithms
- Generation and verification of digital signatures
- Key management operations

As Figure 4.6 shows, these two crypto modules are subdivided into two layers: **Interface layer** and **Implementation layer**.

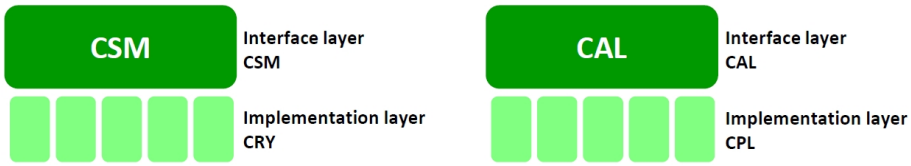

Figure 4.6: Two layers of crypto modules [6]

The interface layer is completely standardized by the AUTOSAR while the cryptographic algorithms in the implementation layer are defined by the implementer. The CSM implementation layer is called **Cryptographic Primitives Module (CRY)** while the implementation layer for CAL is called **Cryptographic Primitives Library (CPL)**. These two modules are used to implement cryptographic algorithms (routines) that will be used by software components (SWCs) in the application layer and modules in the BSW layer. The cryptographic algorithms are implemented using a software library (CSM and CAL) or a cryptographic hardware module (only

CSM). Both, CSM and CAL, have to be configured with information about the names of the cryptographic algorithms in the implementation layer (CRY and CPL) and the maximum sizes of keys of the corresponding CRY/CPL module [8].

Table 3.1 shows the main differences between these two modules. Even though they have similar functionality, CSM is a service while CAL is a library, and they use different communication mechanisms. The existence of both modules is because of historical reasons, as stated in the AUTOSAR documentation.

Table 4.1: Differences between CAL and CSM

	CAL	CSM
Services	25	26
Implementation	Library	System service module
Behaviour	Synchronous	Synchronous / Asynchronous
API	*Cal_< Service >(cfgId,ContextBuffer,...)*	*Csm_< Service >(cfgId,...)*
Context buffer	Provided by application	Buffer has to be provided by CRY
Crypto	CPL (Crypto Primitive Library)	CRY (Cryptographic library)
Re-entrance	Re-entrant	Non re-entrant
Usage	Following functions have to be called: ➢ (Csm/Cal)_<service>Start ➢ (Csm/Cal)_<service>Update (at least one time) ➢ (Csm/Cal)_<service>Finish	

4.3.2 Secure On-board Communication (SecOC)

The SecOC module provides an authentication mechanism for critical data. It is used in all ECUs that require secure communication. This module is specified for the first time in Release 4.2 of the AUTOSAR standard specification. The module provides a security mechanism that is easy to implement into the existing communication technology, is not resource-heavy, and as such can be used for legacy systems as well [6].

The specification of the module mostly relies on the assumption that symmetric authentication approaches will be used with Message Authentication Code (MAC), but it also supports asymmetric authentication approaches. The symmetric authentication approach is faster and less complex, and achieves the same level of security but with smaller authentication keys compared to the asymmetric approach.

Figure 4.7 shows that the SecOC module is integrated on the same level as the Protocol Data Unit Router (PduR). On the configuration in Figure 4.7 the PduR is responsible for the routing of the security related I-PDUs (Information-Protocol Data Unit) to and from the SecOC module. This module then adds or processes the security relevant information of the I-PDU, and reports the results to the PduR [7].

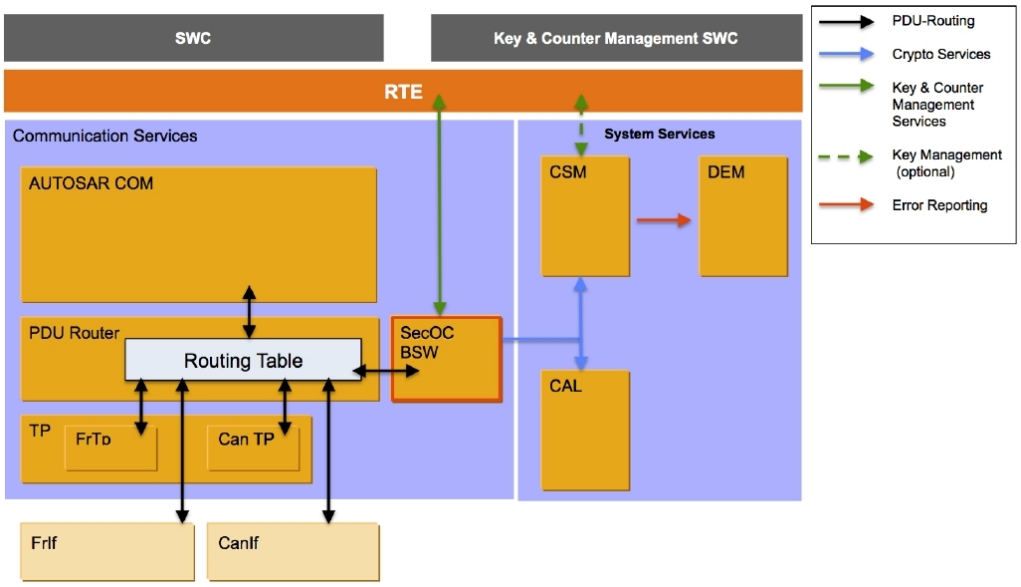

Figure 4.7: Integration of the SecOC basic software module [7]

Figure 4.8 shows the structure of a Secured I-PDU that contains: Authentic I-PDU, freshness values and the authenticator. Authentic I-PDU is an AUTOSAR I-PDU that requires protection against manipulation and replay attacks. The freshness value and the authenticator ensure the integrity and authenticity of the information.

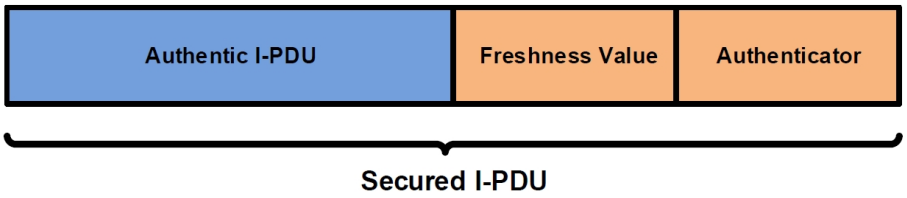

Figure 4.8: The contents of the secured I-PDU [7]

This security module protects against injection, alteration and replay of secure I-PDUs. It uses cryptographic algorithms of the CSM or the CAL module and interacts with the RTE layer in order to allow key and counter management. It provides the functionality for verifying the authenticity and freshness of the PDU based communication between different ECUs inside the vehicle. The authentication and integrity protection ensures that the information sent over the in-vehicular network comes from the right ECU and that the information itself is correct [7].

4.4 The AUTOSAR Security Work Package

In November 2014, the AUTOSAR Security Work Package was started, involving all the security experts from the automotive industry including vehicle manufacturers, suppliers, software stack vendors and semiconductor vendors.

The purpose of this work is to address the increasing security concerns in the automotive industry that mainly involve the connected car concept and the security vulnerabilities that might arise. The cooperation of more experts will produce high quality security measures that can be incorporated in the AUTOSAR standard. It is also cost effective and improves the interoperability between different ECU manufacturers. The costs are decreased because the companies are not working separately on the solution. Instead they work together and share the knowledge which allows them to find the right solution faster and with less effort [72].

4.5 Future of AUTOSAR

The main future product of the AUTOSAR organization is the release of the AUTOSAR Adaptive platform planned for the beginning of 2017 [104]. This will be the first implementation of the AUTOSAR standard and will be developed by the AUTOSAR partners. Until now, the AUTOSAR standard was based on extensive specification documents that each partner used to make their own implementation of the software, but with the Adaptive platform each partner will have software that is already implemented and licensed to all AUTOSAR partners.

With the upcoming new Adaptive platform concept the AUTOSAR organization wants to respond to the new requirements for the future vehicles that includes increased connectivity, autonomous driving and a more dynamic architecture that will interact with other vehicles and the environment surrounding it. The communication in the Adaptive platform will be based on IP/Ethernet technology.

The initial release will contain very basic functions without any security modules implemented and each new release will expand this software with new features and modules. It will be based on C++ programming language. Some of the planned security features are user management, file encryption and crypto-hardware. The Adaptive platform does not substitute the Classic platform, instead it just adds additional functionality and decreases development cycles.

4.6 Summary

AUTOSAR has great potential and most of the vehicles today use it as a basis for their software architecture. This means that if the AUTOSAR organization incorporates good security mechanisms and practices in their standard then all the vehicles that use it will in return have those security mechanisms in their software architecture. If we add to this the specific security mechanisms that each company adds to their vehicles, we are looking at very secure vehicles with very low risk of being exploited by malicious attackers. This is why it is important to emphasize the current security modules in AUTOSAR, but also to test the standard and see what type of security improvements can and should be made.

5
Threat modeling techniques

The process of threat modeling is important because it performs a security analysis of the system. It identifies which assets of the system are interesting to an attacker, identifies the ways that an attack could be carried out along with the motivation behind such an attack. It shows the system designers which parts of the system are vulnerable and suggests which counter-measures to implement. It is also a process of risk assessment that shows the risk level of different system parts along with the impact that an intrusion would have on the system. These are the reasons why threat modeling of the AUTOSAR standard is important to perform, because it will show which parts of the system, based on the AUTOSAR standard, are vulnerable and will consequently need more attention in further AUTOSAR releases. As described in previous chapters, cyber-security of connected vehicles has recently become a very important aspect in the automotive industry and with AUTOSAR being the most commonly used standard, it is only natural to be the first one in the line for a security review and improvement process. When it comes to the threat modeling process there are three main approaches [13, 107, 69, 56]:

- **Attacker-centric**
- **Software-centric**
- **Asset-centric**

More details on these approaches will be given in the following sections along with example methods for each approach. The example methods were chosen based on the current state of the art and an extensive literature survey. There are, of course, other methods that can be used, but the most commonly used and the most reliable ones are stated in this thesis.

After analyzing these methods and evaluating their applicability to the automotive industry, in the next chapter, they will be modified and adapted in order to apply them to the connected car and the AUTOSAR standard.

5.1 Attacker-centric approach

The attacker-centric approach focuses on the attacker, their motivation, goals and how these might be achieved. This approach is not that commonly used which is why there are not many methods that implement it. The main examples are: Intel's TARA [70], Cyber Kill Chain [94] and the OODA Loop [21].

5.1.1 Intel's TARA (Threat Agent Risk Assessment)

Intel's method for threat modeling prioritizes specific areas that are critical for the system and most vulnerable to attacks. This ensures that the security staff targets the most exposed areas and efficiently applies its resources to increase their security level. More specifically, the TARA method identifies which threat agents are the most dangerous ones, what kind of action they want to perform and the most likely techniques they will use to accomplish their goal. This information is then cross-referenced with the known vulnerabilities and controls in order to determine the most exposed areas. This process can be seen in Figure 5.1 [70].

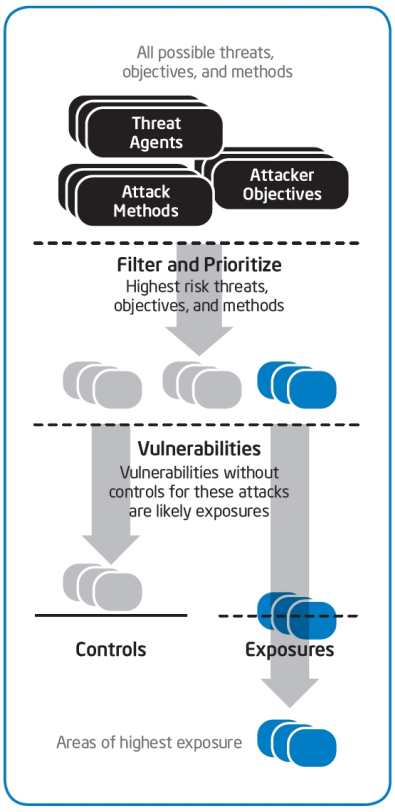

Figure 5.1: Narrowing down the field of attacks [70]

The main goal of this method is to determine the most likely attack vectors in order to apply an optimal security strategy which would ensure efficient use of resources and reduce costs. Most security solutions are offering a universal fix for all vulnerabilities while the TARA method defines a security strategy that focuses its attention just on the areas that pose the highest level of overall risk [70].

TARA is the first step of Intel's *Defense in-depth information security strategy*. This strategy has a layered approach to security and has several different security controls in position. The existence of more than one security control provides redundancy in case one of the security controls is breached or fails.

"Threat agents are attackers who represent a security risk of loss, and they are classified by characteristics including skills, capabilities, resources, intent, and access" as stated in Intel's white paper [70].

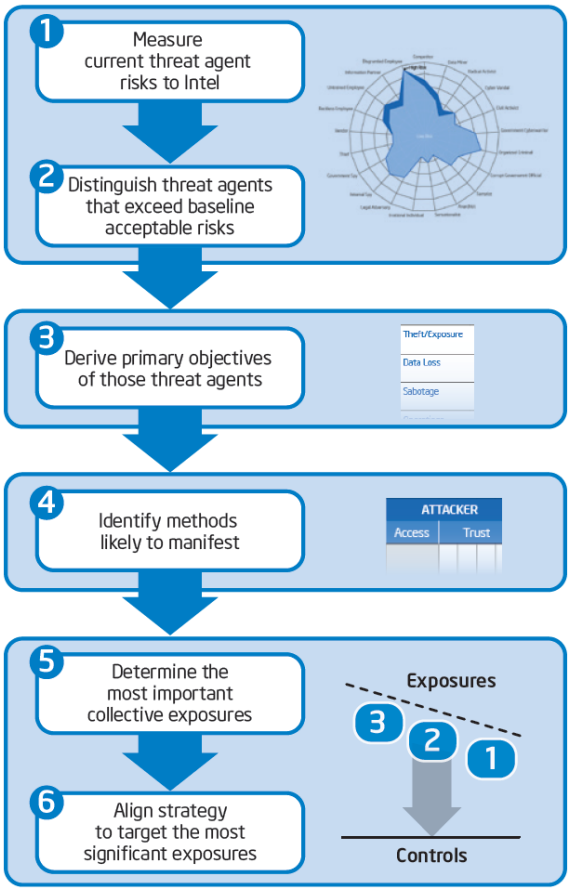

Figure 5.2: The TARA process in detail [70]

TARA method relies on three main components in order to reach the intended goal:

- **Threat Agents Library (TAL)** - is a unique standardized library that contains 22 threat agent types along with nine common threat agent attributes.
- **Common Exposure Library (CEL)** - contains known security vulnerabilities and exposures.
- **Methods and Objectives Library (MOL)** - contains a list of known threat agents objectives along with a most likely method they will use to accomplish their objective.

Figure 5.2 shows the six steps of the threat modeling process by using the TARA method. The final outcome of this process reveals which parts of the system are the most exposed. The security experts can use this information to adapt their security strategy in order to focus on the critical parts of the system and allocate security resources efficiently, avoiding over-securing parts of the system with lower exposure.

5.1.2 Cyber Kill Chain

The Cyber Kill Chain method was established by Lockheed Martin, which is an American global aerospace, defense, security and advanced technologies company. It focuses on the steps that an attacker has to take in order to perform an attack on the target system and achieve his/her goal. Every step has a specific goal that needs to be reached in order to move on to the next step. By looking at each step of an attack, companies can prepare their defense in a more efficient way by concentrating on the relevant assets in their systems. The name of this method points to a chain of seven steps needed in order for an attacker to penetrate the system and export the information he/she needs [94].

These are the 7 steps of the Cyber Kill Chain:

- **Reconnaissance** - Research, identification and selection of the target.
- **Weaponization** - Creation of a malicious package to be sent to the target.
- **Delivery** - The malicious package is delivered to the target by e-mail or other means, and this represents just one of many intrusion techniques the attacker can use.
- **Exploitation** - Refers to the actual execution of the malicious package on the target system.
- **Installation** - Refers to installing a Backdoor Trojan or similar which would grant remote access to the target machine over a longer period of time.
- **Command and Control** - Establishing an outside connection or a channel by which the attacker can gain "command and control" over the target machine from a remote location.
- **Actions on objectives** - This is the final step of the attack which can take months to successfully perform. The attacker performs actions that would accomplish his/her initial goal [94].

By using this method security experts can get into the attacker's head, and concentrate on the assets that are truly at risk. The company needs to analyse the chains of attack that happened previously and draw meaningful conclusions which would improve their response to the next intrusion attempt. If the security strategy of the company is based on this method and if the method is implemented correctly, the company can be one step ahead of any attacker that tries to penetrate their system [94].

5.1.3 OODA Loop

This threat modeling technique was developed by the U.S. Air Force and was initially intended for decision-making in air-combat situations. It did not take long until its application to business and strategy was shown to be useful as well. The main idea of the technique is to make decisions based on real-time information that is fresh and updated constantly. The technique is rather dynamic and involves real-time monitoring of the necessary inputs for fresh information, resulting in a decision-making process that changes and adapts according to the received input [21].

There are four main stages of this technique:

- **Observe** – Find as many relevant sources as possible and collect fresh and updated information from them.
- **Orient** – Analyze the collected information and update the current strategy based on this assessment.
- **Decide** – Make a decision based on information from the two previous stages.
- **Act** – Execute the decision.

The OODA loop is performed over and over again in order to always be ahead of the "enemy". The speed at which this loop is performed by a company or an individual is the main advantage that one has against the competition (adversary). Every time we go through the loop, the results of our decisions are analyzed, and based on them, future decisions are taken in the next loop with different results.

5.2 Asset-centric approach

The asset-centric approach starts from the asset that is entrusted to the system at hand, such as a collection of sensitive personal information i.e. GPS history. The approach focuses on the final target of an attack which is usually some important information about the system or data stored on the internal memory.

This approach is more commonly used than the attacker-centric approach. All the methods that are based on this approach require a lot more time and resources than the methods from other approaches. The most reliable and comprehensive examples of this type of methodology are [82, 114, 52]: PASTA, OCTAVE and ETSI's TVRA.

5.2.1 PASTA

PASTA (Process for Attack Simulation and Threat Analysis) is an asset or risk centric approach to threat modeling that has some significant advantages compared to other threat modeling methods. It was developed by the director of Minded Security, Marco Morana, and the CEO of VerSprite, Tony Uceda Velez [82].

The method achieves technical sophistication and accuracy, while also providing important information about the risk reduction and security strategy of the company. This ensures that the results of this method can be used not just by the technical staff of the company, but also by management, in order to see the impact on business and implement an appropriate strategy for securing their systems. The method is performed in seven stages (Figure 5.3) and each stage has a different task that needs to be performed before moving to the next stage [82].

The main goals and values of this method are [82]:

- Allows cost and time savings
- Integrates with the SDLC
- Better understanding of most likely attack sources
- Better communication between security groups inside the company
- Increases the maturity of the organization in software security

Figure 5.3: 7 stages of PASTA [82]

5.2.2 OCTAVE Allegro

OCTAVE Allegro (Operationally Critical Threat, Asset and Vulnerability Evaluation) is a method first introduced in 2007 by the CERT Survivable Enterprise Management team. The main focus of this method is on the information assets. The main security requirements for information assets are confidentiality, integrity and availability (CIA) and these requirements live with the asset throughout its life cycle. The method examines the ways the information asset is stored, transferred, used, processed and how it is exposed to threats and vulnerabilities [33].

The OCTAVE Allegro is performed in eight steps which are divided into four phases as can be seen in Figure 5.4. In the first phase, the company develops risk measurement criteria consistent with organizational drivers that are strongly linked to the strategic goals of the company.

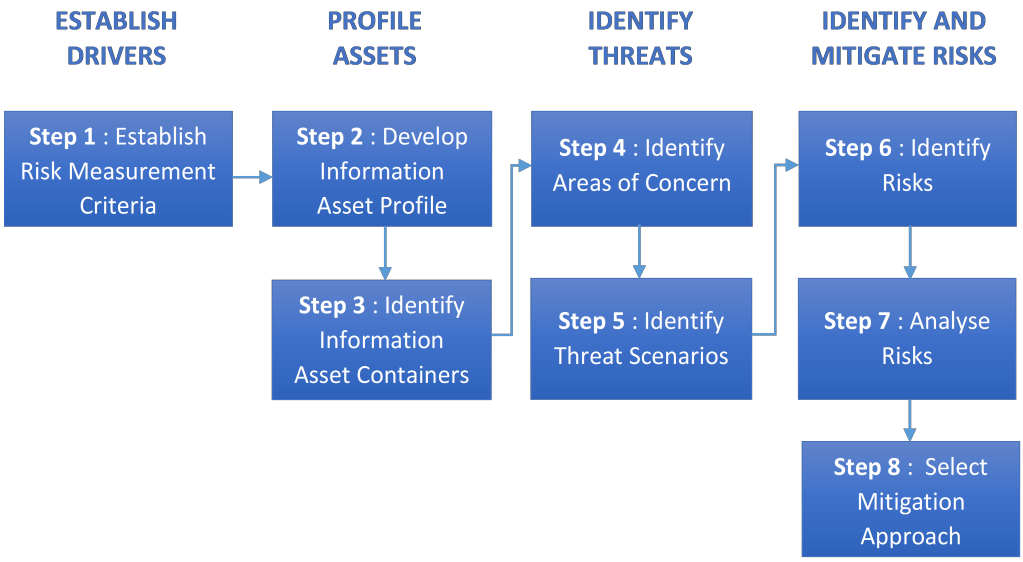

Figure 5.4: OCTAVE Allegro road-map [33]

The next phase, Profile assets, is used to identify and profile the assets that are the target of the risk assessment. The containers of these assets are also identified in this phase. In the third phase, threats to the identified containers with respective assets are found and documented. While most methods use threat trees to identify threats, the OCTAVE Allegro uses threat scenario questionnaires instead, in order to avoid the confusion that can arise with complex threat trees. The final stage identifies the risk to the assets based on the threat identification from the previous step. In this stage, mitigation strategies are developed to deal with the identified risk.

5.2.3 ETSI's TVRA

The European Telecommunication Standardization Institute (ETSI) developed a threat modeling technique named TVRA which stands for Threats, Vulnerabilities and Risks Analyses. The method models a system consisting of assets which can be physical, human or logical. The process further identifies all the assets of the system, potential vulnerabilities of these assets and the threats that could potentially exploit them. In the beginning all assets of the system are considered to have a weakness, as an initial assumption.

The method needs to make sure that all assets perform their function even if under attack from a malicious user. The method identifies the vulnerabilities, isolates them and selects appropriate countermeasures to mitigate these vulnerabilities. It also assesses the impact of an attack to a particular asset of the system.

The result of the TVRA method is a quantified measure of risk that each asset of the system represents along with appropriate security requirements that will counter these risks and make the system more secure [50, 49].

The TVRA method is performed in seven steps [49]:

- Identify security objectives
- Identify security requirements
- Produce an inventory of system assets
- Classify system vulnerabilities and threats
- Quantify the likelihood and impact of an attack
- Determine the risks involved
- Specify detailed security requirements - countermeasures

5.3 Software-centric approach

The software-centric approach starts from the system design and then goes through the model of the system, looking for types of attacks against each element of the model. The approach is mostly used for threat modeling of networks and computer systems and it has become a de-facto standard in this field. It uses data-flow diagrams (DFD), use case diagrams, or component diagrams to illustrate the system and its components. This is the most commonly used approach to threat modeling and the two main examples come from Microsoft: STRIDE [83] and DREAD [92].

5.3.1 STRIDE

STRIDE is a well known threat modeling method developed in 1999 by Microsoft's employees Loren Kohnfelder and Praerit Garg. The method is intended to help software engineers and developers to identify potential threats and attacks that their system may be exposed to.

STRIDE is short for [92]:

- **Spoofing** - refers to faking the identity of a person or an object. It can be impersonating someone else, sending e-mails or network packets with "spoofed" origin address etc. The most common types are spoofing of the process, file, machine, person or a role.
- **Tampering** - means that someone intentionally changes the contents of a packet/file in order to cause the system to perform illegal operations. Malicious users can tamper with files, memory, network etc.
- **Repudiation** - is stating that you did not perform a certain action nor are responsible for the results of that action. Repudiation can be honest or deceptive. This type of threat is closely associated with the logging system because without this system it is hard to determine when and by whom a certain action was performed. Examples of this threat type is repudiating an action or attacking the logs.
- **Information disclosure** - refers to getting access to information that a person is not authorized for. It can be against a process, data store or a data flow.
- **Denial of service** - is a very common attack that prevents the system from operating normally by occupying its resources with fake requests, which block all other genuine requests to the system's resources. It can be against a process, data store or a data flow.

- **Elevation of privilege** - refers to performing an action that you are not authorized to do. This can be done by corrupting a process or by getting past authorization checks.

There are four types of this method: STRIDE-per-Element, STRIDE-per-Interaction, DESIST (Dispute, Elevation of privilege, Spoofing, Information disclosure, Service denial, Tampering) and Elevation of privilege game.

It is common to use the Microsoft Threat modeling tool when applying the STRIDE method. This tool automatically detects vulnerabilities from the six STRIDE categories. The only input needed for the tool is a data flow diagram of the system being analysed. Table 5.1 shows which security protocols are violated by each threat from STRIDE categories.

Table 5.1: STRIDE threat categorise vs security protocol violated

STRIDE	**Security protocol violated**
Spoofing	Authentication
Tampering	Integrity
Repudiation	Non-repudiation
Information disclosure	Confidentiality
Denial of service	Availability
Elevation of privileges	Authorization

5.3.2 DREAD

This method was developed by Microsoft and it is used to calculate the risk level of different threats to the system. It divides the risk into five categories and by performing the method it identifies the areas of concern.

DREAD stands for [92]:

- **Damage Potential** - defines the level of damage an attack can have on the system or part of the system.
- **Reproducibility** - determines how easy it is to reproduce the attack. If the attack can be performed over and over again, it represents a significant risk.
- **Exploitability** - how easy it is to perform an attack on the system or how much effort it takes to execute a successful attack.
- **Affected Users** - the number of users that a potential attack would affect. The more users get affected, the higher the risk is.
- **Discoverability** - how easy it is to find a vulnerability in the targeted system.

DREAD is a categorization scheme that quantifies, compares and prioritizes the amount of risk that each evaluated threat represents [22]. This method has a scale of 1-10, for each category listed above, and when that number is determined it is then calculated in the formula:

Risk DREAD = (DAMAGE + REPRODUCIBILITY + EXPLOITABILITY + AFFECTED USERS + DISCOVERABILITY) / 5

The result of this formula is a general risk value (assessment) of the system at hand. The number is always between 1 and 10, with the higher the number the higher the risk. The DREAD method is fairly subjective and can lead to misleading results in many cases, which is why the Microsoft SDL Team does no longer recommend its use as of 2010.

5.4 Threat modeling mechanisms

This section will give some more information about different mechanisms and tools that are used during the threat modeling process. Data flow diagrams (DFD) and attack trees are used to graphically illustrate parts of the threat modeling process. On the other side threat modeling tools represent a software solution with complete templates that can speed up some of the threat modeling process.

5.4.1 Data Flow Diagrams

DFD (Data Flow Diagrams) drawings and interconnection drawings illustrate different parts of the system. They show the data flow and the trust boundaries between different components in the system as in the example on Figure 5.5. The diagram illustrates what type of data will be on the input/output, the origin and the destination of data along with information on where the data will be stored. This is very helpful during the threat modeling process as the Microsoft Threat modeling tool can automatically find certain vulnerabilities just by computing these DFD drawings [18, 125].

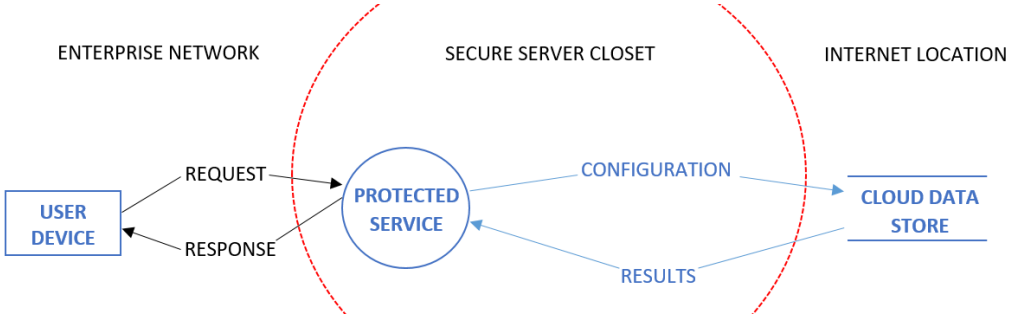

Figure 5.5: Example of a data flow diagram

Figure 5.6 shows the most common elements of a data flow diagram. The first element represents a process that changes the input data in some way, such as some type of computation, data sorting etc. The External interactor represents an outside entity that communicates with the system and receives/sends information to the system in question. The data store is in charge of storing the data used in the process. Data flow arrows show the flow of data between different entities in and outside the system. The trust boundaries separate the different parts of the system

such as the inside processes from the outside entities and illustrate data moving from low to high trust areas [66].

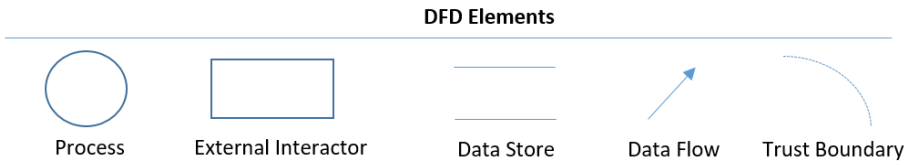

Figure 5.6: Common elements of a data flow diagram

5.4.2 Attack Trees

Attack trees are diagrams that are used to illustrate a certain attack on an asset/-target. The attack on the system is represented with a tree structure where the root node is the goal of the attack and the leaf nodes represent different ways how the attack can be accomplished. The leaf nodes further branch into child nodes which represent conditions that need to be fulfilled in order to make the parent node true. In other words, if the condition is true then the described action by the parent node can be performed. The attack is complete when the root node is satisfied. An example of an attack tree is shown in Figure 5.7.

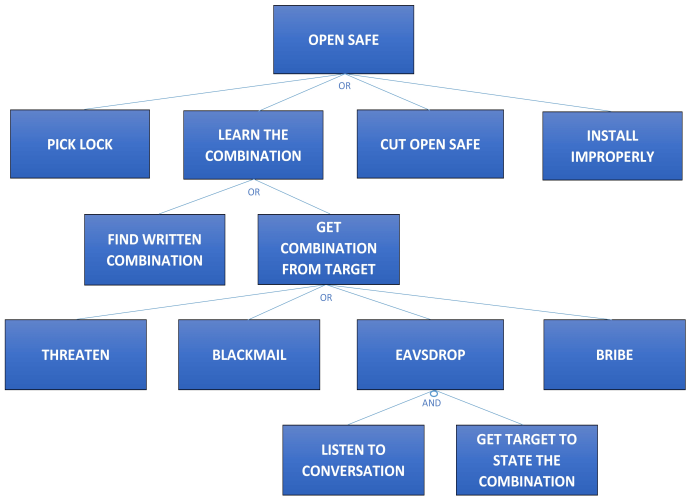

Figure 5.7: Example of an attack tree for breaking into a bank safe [11]

5.4.3 Threat modeling tools

As stated previously, the purpose of the threat modeling tools is to automate some parts of the threat modeling process and to provide generic templates that can be adapted to the system being modeled.

The **Microsoft Threat Modeling tool** is one of the most commonly used and provides guidance in creating and analyzing threat models. It is designed for developers and not just security experts, enabling them to communicate the security design of the system, analyse the system for vulnerabilities and suggest a mitigation strategy.

Using this tool developers and security experts can design the system by creating Data Flow Diagrams (DFDs) for different parts and components of the system. After creating the DFDs they can use a built-in threat library, which is based on the Microsoft's STRIDE threat model, to let the tool automatically analyse the DFDs in order to detect all the threats to the system. The result of this analysis is a list of all discovered vulnerabilities with detailed descriptions of the threats, along with recommended mitigation techniques to neutralise these threats. Besides this, there is also an option to document the impact that each threat has on the system coupled with the steps that will be taken to address this threat. This is where the developers and security experts can explicitly state which security mechanism will be implemented to prevent the vulnerability to be exploited. In general, this tool helps find threats during the design phase of software development. This tool is free and can be downloaded directly from the Microsoft web page [10].

MyAppSecurity ThreatModeler is another threat modeling tool with the same function as the Microsoft tool but with a different methodology and functional design. It is the first commercially available threat modeling tool. One of the main differences is that this tool uses Process Flow Diagrams (PFDs) instead of the DFDs that the Microsoft tool uses. The tool uses its own Centralized Threat Library that is frequently updated and synchronized with reliable industry sources (e.g. CAPEC, WASC-TC, OWASP). The risk analysis is performed by the Intelligent Threat Engine which automatically detects threats to the system, categorizes them by the risk level and specifies appropriate security controls to mitigate them [84].

PFDs (Process Flow Diagrams) are specifically created for threat modeling to illustrate how the user interacts with different features of the system. The diagram shows the relationship between the major components of the system and decomposes the system into various use cases that are interconnected by communication protocols [126].

5.5 Summary

The threat modeling methods, mechanisms and tools introduced in this chapter are some of the most commonly used by security experts. It is important to have a good understanding of the available methods in order to choose the one that is adequate enough to apply to the connected car and the AUTOSAR standard. For the purpose of threat modeling conducted in this thesis, the author has chosen two threat modeling methods: TARA and STRIDE. In order to apply the STRIDE method successfully, two threat modeling mechanisms will be used: Data flow diagrams and Microsoft threat modeling tool.

6

Threat modeling of the Connected Car

After conducting an extensive literature survey it was concluded that methods from the attacker-centric approach were not used very often. Intel Security tried to make a change in this field and invented a new method that considered the attacker as the main focus. The method is called Threat Agent Risk Assessment (TARA), and it is based on descriptions of threat agents and their appropriate attributes such as motivation, objective, skill, resources, attack methods and attack surface. The method is not time-consuming and the knowledge required, and input information can be accessed which is one of the reasons why it was chosen for the threat modeling in this case. It is also very adaptable and can be applied to various industries such as the health-care industry [29] or as in our case, the automotive industry. Attacker-centric threat modeling in the automotive industry had thus far never been conducted, to the best of our knowledge, and this can be seen as a gap in the research which is filled with this thesis. The STRIDE method will be discussed in chapter 7.

6.1 TARA

The Threat Agent Risk Assessment (TARA) method is based on three libraries from which the security experts can draw conclusions on what assets of the company that need to be better protected. Once developed, these libraries can be updated and used in all future instances of the TARA method and can show how the threat level of different threat agents changes over time as well as how different assets become more targeted than before.

- **Threat Agent Library (TAL)** - lists all relevant threat agents and their corresponding attributes.
- **Methods and Objectives Library (MOL)** - lists methods that each threat agent might employ along with a corresponding impact level.
- **Common Exposure Library (CEL)** - lists areas of the greatest exposure and vulnerability.

These libraries are developed internally inside a company by their security experts team. They are based on incident reports, breach reports, security measures and other confidential information that is required to create the libraries.

By using the information from the libraries, security experts can determine which threat agent attributes are needed in order for a threat agent to pose a threat to the company and its assets. The information is also used to list the methods that are most frequently used to attack these assets along with a list of the most exposed areas.

Each of the exposed areas is described with the level of exposure, current security control that protects the area concerned and the recommended security control for this area. The difference between the current and the recommended security control shows which of them needs a new or improved security measure. By combining the information from all three libraries, security experts can determine which areas are most likely to be attacked with what method and by which threat agent.

6.2 Adaptations

In order to adapt and apply the TARA method to the automotive industry and the connected car, certain modifications were made to the method. The method in its original form is intended to be conducted internally inside one single car manufacturer company. The main reason for this is the sensitivity and confidentiality of the information that is needed in order to perform the method successfully. The other reason is the knowledge and the experience of the security experts that work for that specific car manufacturer company. These factors are very important in order to get accurate and reliable results.

For the purpose of this thesis the author had access to just one of these two factors; the security experts from the automotive industry. The other factor was not accessible because of its sensitive nature but it was partially replaced by an extensive literature survey related to automotive cyber security and recent cyber attacks on vehicles. The domain experts were not available for a group meeting which is why an on-line survey was created to gather the opinions of each expert. Individual sessions with some of the experts were also conducted.

Because of these reasons the main benefit of the results gained in this thesis can be seen as providing a first point of reference for companies in the automotive industry for all future work in this field. The three libraries created by the TARA method can be further used and developed by any car manufacturer company and as such would decrease the time involved and give all the relevant information that security experts need in order to conduct the TARA method internally. It is a way to present this method to the automotive industry and show how it can be a useful tool for their experts in improving the security of the connected car.

The structure of the three libraries that the TARA method is based on, had to be changed to fit the needs of the automotive industry. Most of the changes were related to the context of these libraries, more details to follow.

6.2.1 TAL Library

This library lists the names of all the threat agents that are relevant to the automotive industry along with their corresponding attributes. The following changes were made compared to the original TAL library provided by Intel Security.

- Ten threat agent profiles were removed from the original TAL library and eight new profiles were added instead. The new threat agents that were added are: Outward sympathizer, Hacktivist, Cyber vandal, Online social hacker, Script kiddies, Organized crime, Cyber terrorist and Car thief. The new agent profiles were based on three sources [29, 86, 111] along with research and consultation with domain experts.
- The outcome attribute was also modified, two parameters were removed and four new were added that include: Reputation damage, Material damage, Harm to the passengers and "15 minutes of fame".
- Attributes that are assigned to threat agents were also slightly modified for some of the threat agents included from the original TAL library. For example, the skills and resources level for the Sensationalist threat agent were raised to a higher level than at the start.

6.2.2 MOL Library

This library provides information about threat agent objectives, likely methods they might use and the impact that their actions would have on the automotive company and the assets in the connected car. The following changes were made:

- The sections "Acts" and "Limits" were removed and replaced with five different attack methods that are used in the automotive industry. The "Limits" section can be found in the TAL library.
- The parameters of the "Impact" attribute were replaced with new impact levels that are relevant to the automotive industry and the connected car.

6.2.3 CEL Library

The CEL library does not have a standardized format because it contains confidential information which is why this particular library is never publicly available to any specific company. The CEL library created in this thesis is customized to the needs of the automotive industry and more detailed information can be found in section 6.7.3.

6.3 Methodology and tools

In order to conduct the TARA method the author of this thesis used the information gained from extensive research and the results of an on-line survey. The survey was completed by security experts and more details are given in the next section. The method was conducted with support of domain experts and a project manager from Intel Security in charge for the TARA method. The TARA method is performed

in six steps, the goal of which is to find the critical exposures of the connected car. The following sections describe how each of these steps was conducted in this thesis.

1. Measure current threat agent risks

By using the on-line survey that was completed by security experts, the method determined the threat levels of different threat agents. These threat levels are related to risks that the agents represent in the IT world and to different IT services in general. The TARA method refers to this risk level as the *Default risk*.

2. Distinguish threat agents with elevated risk level

This step was also conducted by using the on-line survey that determined which threat agents have an elevated risk level when it comes to the connected car as the main target. The TARA method refers to this risk level as the *Project risk*.

3. Derive primary objectives of those threat agents

By using the survey results and with the support of domain experts, primary motivations and goals of each threat agent was determined and stated in the MOL library.

4. Identify methods likely to manifest

Based on extensive research of previous cyber attacks on vehicles and with the support of domain experts, it was concluded that all attacks on vehicles can be classified into five attack methods. Additionally, five different impact levels were also identified that were mainly based on motivations and objectives.

5. Determine the most important collective exposures

The CEL library was created with support of domain experts, the information gained from the on-line survey, and extensive research in the field of automotive cyber security. The created CEL library relates to the entire automotive industry and not just one specific company; it contains a list of the most exposed areas of the connected car ranked by the level of exposure.

6. Align strategy to target the most significant exposures

The results of this method can be further used by car manufacturer companies to align their security strategy and focus their resources to the areas of greatest concern.

The survey methodology

The survey was distributed to security experts experienced within the automotive cyber-security sector along with experts working for two major car manufacturer companies. It consisted of eight questions important for conducting the TARA method.

The first two questions were to determine the level of threat that each threat agent represents, first in general for different IT services and afterwords just in the specific case of the connected car as the target.

The other six questions were related to motivation, resources, skill level, attack surfaces, objectives and preferred methods of attack. These are all different attributes of threat agents that are later listed in the TARA libraries. The respondents chose different parameters for each of the attributes that in their opinion were the most relevant ones. These parameters are stated and explained later in this chapter. The parameters with the biggest "hit-rate" indicated which threat agents need to be further considered in regard to the connected car. For example, if the minimum skill level was determined to be "operational" then all the threat agents with a lower skill level were not taken in further consideration.

The survey was distributed to people with experience within IT security, embedded security and automotive cyber security. One part of the experts that completed the survey work for two major car manufacturers. In total 12 people completed the survey. A copy of the survey questions is included in Appendix A.1.

6.4 Threat Agents

The names of threat agents were taken from the TARA methodology and the European Union Agency For Network and Information Security (ENISA) report on threats [86]. Descriptions are adapted in order to relate to the automotive industry and some threat agent names were also changed (new names are marked). Examples of actions that each threat agent might take are given from the perspective of targeting the connected car.

Figure 6.1: Anonymous Hacktivist Group

Hacktivist* - Highly motivated, but non-violent people that support some cause that they think is the right one and promote freedom of expression. This can involve stealing electronic business data that in return causes a variety of disruptions in the

targeted company. An example in the automotive industry could be a group of people that believe autonomous vehicles will cause loss of jobs, so they could try to steal some internal reports of issues that a targeted company could have in regard to their autonomous vehicles. Afterwords they can publish this information to attract public attention and promote their cause of not supporting autonomous vehicles.

Competitor - A business rival who competes with the company concerned by stealing IP or business data. One common example is corporate espionage. This could be someone that works as an outside-contract employee of a car manufacturing company, and who steals confidential data from the competitor companies. This data could involve crash-test reports, bug reports, security breach reports, PII (Personal Identifiable Information) data from the vehicles etc. All the information that a competing company can benefit from is a potential target of this threat agent.

Cyber Vandal* - More known as the "Black hat hacker" is someone who finds excitement from breaching various systems and destroying property. Motivation behind this threat agent is mainly personal gain. It is unpredictable what this agent might do to harm the connected car, but an action like crashing multiple cars at once by breaching their systems could be one of them. The purpose would not be to harm people but to show to the cyber underground community the level of skill they posses, or it could just be for sheer personal entertainment.

Data Miner - Professional data collector specialized in different methods and techniques for stealing and analyzing IP, business data and PII. One major threat to automotive industry would be to steal vehicle data such as GPS data, driving behavior data, personal phone book information, VIN numbers, social media information from the entertainment center etc. Afterwords they could sell this information on the black market or use it for their own personal agenda.

Online Social Hacker* - Experts in social engineering which allows them to analyze and understand the behavior and psychology of social targets. The agent violates the privacy of potential victims, e.g. Spear Phishing. With the introduction of the connected car concept, our vehicle is getting more and more features of a standard computer. The in-vehicle entertainment center offers access to web browsing, social media web sites, e-mail accounts etc. The attacker can use this information to send customized e-mails or messages over social media, pretending to be your vehicle manufacturer or your vehicle insurance agency, and asking for some personal information which is later exploited for personal gain. This e-mail/message could ask the victim e.g. to provide a credit card number for paying insurance premiums or to make a payment to your car manufacturer for some new software update.

Script Kiddies* - Young individuals with low skill level that use the information available on the Internet to launch a cyber-attack. Their main motivation is curiosity and excitement. Guides on creating malware and ransom-ware are easily accessible on-line. Today there are a variety of tools available on-line that people can use to capture packets on the vehicle CAN network, replay these packets or

create their own packets and send them to the network. One of these tools is used in the thesis and will be discussed in the next chapter. There are even manuals [20] and books [22] on how to attack vehicles and if any individual has a strong motive and the desire, they could formulate an attack. People can, for example, test these attacks on their own vehicles for later use on the victim vehicle of the same brand.

Government Cyber-warrior - A state-sponsored agent with major resources that can be used to initiate disruption on a national scale and cause harm to organizations, infrastructure and even physical harm to people through network/computing disruption, malware etc. If the agent could penetrate into the vehicle system remotely, it would allow them access to the entire vehicle control system. Potential scenarios include attacks on individual vehicles that cause them to have a traffic accident with potential deadly consequences or even attacks on a bigger scale where a group of cars is attacked in order to cause multiple traffic accidents.

Organized Crime* - Characterized by having significant resources and a variety of ways to accomplish their goals. When it comes to the automotive industry, it is well-known that the main action that this agent caries out is car theft. With the extended connectivity of new vehicles the variety of methods used to steal a car will surely increase. Depending on the skills required this agent could even use cyber attacks on vehicles to target individuals and cause traffic accidents with deadly consequences.

Radical Activist - Has similar motivation as the Hacktivist threat agent but the means that this agent would use to accomplish a goal goes way beyond the Hacktivist. A radical activist could potentially cause property destruction and physical business disruption to get to their goal. They could, for example, cause traffic accidents of autonomous vehicles just to try to convince people to believe that these vehicles are not safe.

Sensationalist - The usual profile describes a person who wishes to attract public attention by employing any method for notoriety just to get their "15 minutes of fame". In the case of automotive industry, this profile will be extended to also include researchers whose results got so much attention that made them famous. The best example is the team of two researchers Miller and Valasek [20], however their intent was maybe not to get famous or cause reputation damage to the Jeep Cherokee but this certainly was the outcome of their actions. Since their attack in 2015, there were a number of new attacks which resulted in a similar outcome, which is why it is important to include them in this agent profile.

Cyber Terrorist* - People who use violence to support personal beliefs and sociopolitical goals. This can include any type of violence, property destruction or physical business disruption. The future of autonomous driving and connected cars could be a tempting field for this type of threat agent as they could perform remote attacks on groups of vehicles or even buses in order to cause deadly traffic accidents. Nevertheless, in order to perform a successful attack on vehicles they would need

a lot more knowledge and skills than this agent group usually has, which is why it probably does not pose a big threat to the connected car at the moment. In the future when autonomous driving becomes a reality this threat agent could potentially become a bigger threat.

Car Thief* - An individual or a group of individuals working together with a simple profit motive. Car thieves can work alone or as an organized group of highly skilled individuals with just one goal and that is car-jacking. Cars will have more and more connection points to outside networks allowing the car thieves to create new attack vectors and new methods of stealing vehicles. The most interesting attack surface for this threat agent are the Key Fobs and Immobilizers.

Insider threat agents

Government Spy - A person funded by the government who has extensive resources compared to other threat agents. The agent works against the government of other countries and has no personal motivation but rather works as a covert employee of some intelligence agency. One potential scenario could be to spy on new technologies in the automotive industry and then report on these to the government agency they work for.

Internal Spy - The individual works as a trusted insider with extensive access to company resources and business data. The insider has access to confidential information that can be sold to the highest bidder on the black market or to a competitor company. In the automotive industry an insider could sell a company's technology secrets and other information to competitor companies.

Information Partner - This involves someone with whom the car manufacturer company has knowingly shared sensitive information (company confidential) which was caused by poor privacy protection mechanisms inside the company. A potential scenario could be a car manufacturer that allows applications installed on the entertainment center to collect information about driving habits, GPS data etc.

Disgruntled Employee - An unsatisfied current or former employee with enough knowledge or access to the company systems that allows the agent to cause harm to the company by abusing employee privileges for cyber or physical disruption. This person could leak confidential information about the company's new technology or even give information about the security flows of the vehicles on on-line forums just to cause harm to the targeted company. Motivation behind it is mainly personal satisfaction such as revenge for something they believe was unfair from their employer or former company.

Reckless Employee - Current employee that in order to increase their work efficiency bypasses some security mechanisms, but does not intend any harm to the company. Examples of the agent's actions could include misuse of authorizations or harmless shortcuts. These actions could potentially lead to a leakage of confidential

information or expose an attack surface to the attacker that would otherwise be protected. As laptops issued by the agent's company usually have a lot of safeguards and security mechanisms that often cause problems and delays for employees, they could want to bypass these by using their own personal computer to do some part of the work. Personal computers usually have lower protection mechanisms leading to greater exposure to cyber attacks - this could allow the attacker easier access to confidential information.

Untrained Employee - Current employee that unknowingly misuses the company's system or protection mechanisms, such as some unforeseen mistakes or "pushed wrong button".

Outward Sympathizer - A person that uses their company's resources to perform attacks on other people or companies, without the permission of their own company and with harmless intent to the company itself. Someone working for some car manufacturer could have insight information on how to perform a successful attack on the vehicle of that brand, and they can then use this information to pursue someone for their personal goals.

6.5 Threat agent attributes

TARA methodology defines different attributes that identify the specific characteristics of each threat agent. The following is the list of these attributes with a short explanation. All the original attributes from the TARA method were used and only the "Outcome" attribute was modified. The attributes are described in more details in the further subsections.

Intent - Describes whether the agent's intent is to cause harm or not. Two parameters are described for this attribute: Non-hostile and Hostile. The agent with non-hostile intent does not want to cause harm, but his actions accidentally lead to a harmful situation in regard to their company.

Access - Describes what type of access the agent has to the target. Access can be internal, representing an insider threat agent, or external, that represents an agent that has no access to internal data or resources.

Outcome - The final outcome of the agent's actions is given by this attribute. The possible outcomes are: acquisition/theft, business advantage, material damage to the vehicle, physical harm to the drivers/passengers, reputation damage, technical advantage and "15 minutes of fame".

Resources - What type of resources the agent has access to is described by this attribute. Possible type of resources are: individual, club, contest, team, organization and government.

Skills - The level of skills that the agent has is described by this parameter. It can be: none, minimal, operational or adept.

Motivations - This is a newly introduced attribute that explains the motivation behind an action conducted by each of the threat agents.

Visibility - Describes the extent to which the agent wants to hide or reveal their identity. The parameters of this attribute are: overt, covert, clandestine or "don't care".

Limits - With this attribute the TARA methodology describes the extent to which the agent would go in order to accomplish their goals. Parameters for this attribute are: code of conduct, legal, extra-legal (minor), extra-legal (major).

Objective - Describes the primary action the agent will take in order to achieve their goal. Parameters are: copy, deny, damage, destroy, injure, take or "don't care".

6.5.1 Motivations

The motivation is an important attribute of threat agents because it tells us what human drives are involved and what the main reason is for their actions [112]. The motivation usually has two meanings, cause and drive. The cause means the underlying reason for some harmful or unintentional action, which could be some specific situation or an emotional reason. The cause is the primary parameter used to describe the motivation, but the drive is also important because it defines a certain level of intensity or interest a threat agent might have.

Figure 6.2: Different motivations of threat agents [112]

The main reasons behind the motivation parameter are:

- Knowing the threat agent's motivation can give us information about the target or the asset that agent is most likely to focus on.
- If the security experts know the threat agent's intent, they can focus their often limited resources on the most likely attack vectors for any asset.

- Motivation shapes the intensity of the attack because the attackers usually act in a way that reflects their emotional or circumstational state.
- The motivation also helps to better describe the threat scenarios in a less technical language. The motivation describes a more detailed story.

The threat modeling process in this thesis describes two motivational aspects, defining motivation and personal motivators for individuals. The first one is the most descriptive and describes the threat agent group in the best way and is the primary cause of their actions. The second one is focused on motivators for individuals that work alone or as part of a organization. The main reasons and drives for these individuals are described by this aspect. The mappings of motivations can be seen in Table 6.1.

Table 6.1: Motivations of different threat agents

	AGENT LABEL	DEFINING MOTIVATION	PERSONAL MOTIVATION
EXTERNAL	Hacktivist	✓ Ideology	✓ Ideology
	Competitor	✓ Organizational Gain	✓ Personal Financial Gain
	Cyber Vandal	✓ Dominance	✓ Dominance
	Data Miner	✓ Organizational Gain	✓ Personal Financial Gain
	Online Social Hacker	✓ Personal Financial Gain	✓ Personal Financial Gain
	Script Kiddies	✓ Personal Satisfaction	✓ Personal Financial Gain ✓ Personal Satisfaction
	Government Cyber-warrior	✓ Dominance	✓ Ideology ✓ Personal Financial Gain ✓ Personal Satisfaction
	Organized Crime	✓ Organizational Gain	✓ Personal Financial Gain ✓ Coercion
	Radical Activist	✓ Ideology	✓ Ideology
	Sensationalist	✓ Notoriety	✓ Personal Satisfaction
	Cyber Terrorist	✓ Ideology	✓ Ideology
	Car Thief	✓ Personal Financial Gain	✓ Personal Financial Gain ✓ Personal Satisfaction
	Information Partner	✓ Organizational Gain	✓ Personal Financial Gain
INSIDER	Government Spy	✓ Ideology	✓ Ideology ✓ Personal Financial Gain ✓ Personal Satisfaction
	Internal Spy	✓ Personal Financial Gain	✓ Ideology ✓ Personal Financial Gain ✓ Coercion
	Disgruntled Employee	✓ Disgruntlement	✓ Disgruntlement
	Reckless Employee	✓ Accidental	✓ Accidental
	Untrained Employee	✓ Accidental	✓ Accidental
	Outward Sympathizer	✓ Personal Satisfaction	✓ Personal Satisfaction

The TARA threat modeling method defines the following 10 types of motivation:

Accidental - Type of motivation that is usually connected to a threat agent with harmless intent that through distraction or poor training causes unintentional harm to the company.

Coercion - When someone is forced into doing something against their will on

behalf of another is the core of this motivation type. An employee from a car manufacturer e.g. could be forced by intimidation or blackmail to give out confidential information or perform some other action that is harmful to his company.

Disgruntlement - Motivation type that is closely tied to employees or former employees that want to do harm to their company. The reason for this is mostly revenge or retaliation because of some wrong-doing by that company. This motivation type implies that there was some sort of prior interaction between the threat agent and the target company.

Dominance - An attempt to establish superiority over another individual, company, organization or even another country. It can take many forms such as intimidation, threatening to expose sensitive data or stealing information assets in order to become more powerful toward a goal of dominance. Access to this information allows the attacker to leverage them or exploit their vulnerabilities when they decide to attack.

Ideology - The agent motivated by ideology primarily relies on some personal belief, political loyalty, sense of morality or justice.

Notoriety - This motivation type describes someone that is trying to become famous for his harmful actions in the cyber world. A threat agent with this type of motivation usually looks for confirmation and respect from the community in which they act.

Organizational gain - An unlawful action by a threat agent that would increase an organization's profit or obtain some other advantage over a competing organization or company. This can be information theft, misuse of information, inappropriate acquisition, sabotage etc.

Personal financial gain - Probably one of the most common motivations where an individual or a group of individuals performs cyber attacks with only one goal - improving their financial status.

Personal satisfaction - Another very common type of motivation where a threat agent acts in order to accomplish some personal wish or a desire in order to satisfy their emotional self-interest.

Unpredictable - An action conducted by a threat agent that is totally random, strange and has no logical explanation. It creates unpredictable events.

6.5.2 Outcome

The outcome attribute of threat agents gives information about the final goal of their actions. By determining the goal of their actions companies can focus on developing security mechanisms that would prevent the threat agents from achieving their

goal or at least make it more difficult for them to achieve that goal. The objectives descriptions stated in the TARA method were modified for this thesis in order to relate more to the automotive industry and some additional objectives were added (new objectives are marked).

Acquisition/theft - When the final goal of the threat agent is to steal or gain access to a certain asset of the connected car. This can be theft of PII, different parts of the vehicle or even the entire vehicle. Agents could also acquire RFID immobilizer signals, key codes and frequencies in order to unlock the car afterwards.

Business advantage - This is closely related to a competitive advantage over another company or organization. One car manufacturer might want to gain insight into other companies and copy their business processes or assets, so they can become more competitive on the market.

Material damage* - Material damage to the car itself could be a possible goal of some threat agents depending on their specific motivation. It could be for revenge or personal financial gain.

Physical harm to the passengers* - A very dangerous objective that could increase in the near future as autonomous driving cars go on the road. Organized crime, cyber terrorists or government spies could use the underlying technology of connected cars in order to perform targeted attacks on specific people and their vehicles.

Embarrassment/Reputation damage - Any successful cyber attack on the connected car that is published, can affect the reputation of that car manufacturer. Last year when Miller and Valasek [20] published their findings that concerned the Jeep Cherokee car, the stock value of Fiat Chrysler went down and they had to recall 1.4 million vehicles in order to perform a software update.

Technical advantage - The primary focus here is to acquire production processes instead of business processes in order to improve a specific product or production ability. Some specific technology could be replicated and even improved in order to gain technical advantage.

“15 minutes of fame”* - This is the main goal of the Sensationalist threat agent who would do anything just to get a moment in the spot-light. This means performing any type of attack on the connected car and publishing the results on-line in order to attract public interest and attention.

6.5.3 Skills

To be able to perform a successful cyber attack on the connected car, a threat agent needs to have a certain skill level and knowledge. Depending on their final goal the skill level can vary, but in order to gain any kind of unauthorized access to the car

itself, the attacker has to have at least some knowledge of the underlying technology. The TARA methodology defines the following skill levels:

None - Average intelligence and ability that allows them to carry out some random acts of disruption or damage, but has no expertise, knowledge or training that would allow them to perform a targeted attack.

Minimal - This skill level concerns agents that can copy and use existing attack methods that they find on-line or someone instructs them on how to perform the attack. Script kiddies is one example of a threat agent with this skill level.

Operational - A higher skill level where the threat agent understands the technology and the methods that allows them to create new attacks in a limited domain.

Adept - These are experts in connected car technology and can use existing or create new methods for any type of attack.

6.5.4 Resources

The amount of resources that are available to a threat agent is very important because it defines the organizational level on which the threat agent is working along with the skill level they have access to. The TARA methodology defines the following resource levels:

Individual - These are the resources limited to an average individual acting alone. This was one of the limiting factors in security research of connected vehicles, because buying a vehicle just so you can do security testing on it requires a large amount of money and was one of the discouraging factors. *Minimum skill level: None.*

Club - An example of this could be a blog or a forum on which members share their experience and tips on some security issues related to the connected car, on a purely volontary basis and with very little personal interest in the target. *Minimum skill level: Minimal.*

Contest - A competition organised by some specific threat agents whose goal could be, for example, to get unauthorized access to the connected car and control the brakes or the steering wheel. This could be done just for thrills and to see who is the most skilled attacker. Cyber-vandals are the potential threat agents that could organise such an event. *Minimum skill level: Operational.*

Team - An organised group of individuals with a specific skill set that is motivated by a common goal. What defines a team is that it exists for a longer period of time and usually within one geographic area. The now famous security researchers Miller and Valasek teamed up and performed security research on vehicles for a few years and at the end they published their work. Even though these were people with

harmless intent, we could expect people with harmful intent to do similar things if they are motivated enough.*Minimum skill level: Operational.*

Organization - The organization is usually larger and better resourced than a team, typically a company. We have recently seen in the news when a small Chinese company [79] managed to exploit a vulnerability in the Tesla S model. Again, as for Miller and Valasek, their intent was harmless and they notified Tesla about this before they published the details of their research. *Minimum skill level: Adept.*

Government - Implies almost unlimited resources with extensive access to public assets and functions within the government jurisdiction. Government spies or cyber-warriors are one examples of threat agents that have this type of resources. *Minimum skill level: Adept*

6.5.5 Limits

The attribute describes the extent to which the threat agent is ready to go in order to achieve their goal. It represents the legal and ethical limits that the agent is willing to break. It is defined by four parameters:

Code of conduct - Refers to agents that follow the law and also additional ethical boundaries tied to a specific professional occupation.

Legal - The agents conduct their actions within the limits of applicable law. These actions might not be ethical in themselves, but they follow the limits of the law.

Extra-legal(minor) - Describes agents that de-facto break the law, but in a minor way such as unauthorized access to confidential information or minor vandalism. The Hacktivist is a typical example of this parameter.

Extra-legal(major) - Refers to agents that would take any action necessary just to accomplish their goal. This could involve major material damage, physical harm to people, violence and major financial impact.

6.5.6 Objective

The objective attribute describes the general action in which the threat agent's method of attack usually corresponds as means of achieving their final goal.

- **Copy** - Make a copy of an asset so the agent can have access to it as well.
- **Deny** - An action that would deny access to the victim of the attack (e.g. Denial of Service).
- **Damage** - Damaging an asset or a vehicle which has limited use for the owner afterwords.

- **Destroy** - The asset or the vehicle is destroyed and no one has access to it, including the attacker.
- **Injure** - Physically injuring the passengers of the vehicle.
- **Take** - Gain full access to a certain asset that prevents the victim from accessing it.
- **"Don't care"** - The agent does not have a specific plan on which action to take in order to get to their goal. The decision of an attack could be randomly taken at the time of the attack.

6.5.7 Visibility

The visibility attribute determines the extent to which the attacker wants to hide or reveal their identity. TARA defines four parameters for this attribute.

Overt - The agent intentionally makes the attack and their identity is known before or during the attack.

Covert - The agent performs the attack but intends to keep their identity secret. The victim knows that an attack took place.

Clandestine - The attacker intends to hide their identity and to hide the fact that an attack took place.

"Don't Care" - The agent makes a decision randomly just before the attack or they do not even care about hiding their identity or the attack.

6.6 Results

This section gives the final results of the Threat Agent Risk Assessment (TARA) method that was applied in the automotive industry to the concept of the connected car. The results are summarized into three libraries that are the final product of this method and are presented as specifically structured tables for the use in the automotive industry. Additionally, a graph is designed that shows the threat levels of different threat agents along with the elevated risk for six of the agents that were identified as being especially dangerous for the connected car.

6.6.1 Threat Agent Library (TAL)

Based on the list and descriptions of threat agents and their attributes stated in the previous sections, a customized TAL library was created (Figure 6.3) just for the use in the automotive industry. All the relevant threat agents are listed in this library along with their most important attributes. Different car manufacturer companies can use this list to determine which threat agents are most likely to pose a risk to their vehicles and the company itself.

THREAT AGENT ATTRIBUTES		NON-HOSTILE INTENT				HOSTILE INTENT													
		Reckless Employee	Untrained Employee	Outward Sympathizer	Information Partner	Hacktivist	Competitor	Cyber Vandal	Data Miner	Online Social Hacker	Script Kiddies	Government CyberWarrior	Organized Crime	Radical Activist	Sensationalist	Cyber Terrorist	Cyber Criminal	Government Spy	Internal Spy	Disgruntled Employee
Access	Internal	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■	■
	External																			
Outcome	Acquisition/theft							■		■	■		■				■		■	
	Business advantage						■		■									■		
	Material damage*	■	■					■				■	■	■		■	■			■
	Harm to the passengers*											■	■			■		■		
	Reputation damage	■	■	■	■	■		■			■	■		■	■					■
	Technical advantage						■		■									■	■	
	15 minutes of fame*										■				■					
Resources	Individual	■	■	■													■			■
	Club										■				■					
	Contest							■												
	Team								■	■										
	Organization				■	■	■						■	■		■			■	
	Government											■						■		
Skills	None																			
	Minimal		■								■				■		■			
	Operational				■			■		■										■
	Adept	■		■		■	■		■			■	■	■		■		■	■	
Visibility	Overt		■											■	■					
	Covert	■		■		■		■					■			■	■			
	Clandestine				■		■		■	■								■	■	
	"Don't care"										■	■								■
Limits	Code of Conduct		■		■															
	Legal	■																		
	Extra-legal - Minor			■		■	■	■	■	■	■			■	■		■		■	
	Extra-legal - Major											■	■			■		■		■
Objective	Copy					■	■		■	■								■	■	
	Deny											■								
	Injure												■	■		■		■		
	Destroy											■				■				■
	Damage			■								■				■				■
	Take												■			■				
	All above / Don't care	■	■		■			■			■			■	■		■			
Motivation	Accidental	■	■		■															
	Coercion																			
	Disgruntlement																			■
	Dominance							■				■								
	Ideology					■								■		■		■		
	Notoriety														■					
	Organizational gain						■		■				■							
	Personal financial gain									■							■		■	
	Personal satisfaction			■							■									
	Unpredictable																			

Figure 6.3: Threat Agent Library (TAL) for the Automotive industry

6.6.2 Methods and Objectives Library (MOL)

The methods and objectives library shows the defining motivations of threat agents, their main goals and the most likely methods they would employ in order to successfully accomplish their goals. In the TAL library each threat agent has one or more different possible motivations, but the MOL library just states one main and most likely motivation when it comes to the automotive industry. The decision on which motivation to include in the MOL was based on consultation with domain experts and the online survey. The goal attribute of the MOL library is very similar to the outcome attribute of the TAL library, the difference is that in the MOL library it represents the goal which the threat agent wishes to achieve and in the TAL library it represent the outcome of threat agent actions.

For example, in the case of Outward Sympathizer, the outcome of their actions will most likely be reputation damage to the company they work for, while the goal they want to achieve could possibly be to prevent some outside target from accessing their vehicle. They are able to perform this attack because they have internal access to the vehicle company, but their intention is to cause harm to their personal target and not the company they work for. So the reputation damage was a type of collateral damage in this specific case.

Table 6.2: Methods and Objectives Library (MOL)

AGENT NAME	ATTACKER					OBJECTIVE		METHOD					IMPACT				
	Access	Trust				Motivation	Goal										
		None	Partial Trust	Employee	Administrator			Theft of PII and Business Data	Denial of Service	Intentional Manipulation	Unauthorized Physical Access	Unpredictable Action	Reputation Damage	Privacy Violated	Loss of Financial Assets / Car	Traffic Accidents	Injured Passengers
Competitor	External	✓				Organizational Gain	Technical advantage	✓					✓				
Car Thief	External	✓				Personal Financial Gain	Acquisition / Theft				✓		✓		✓		
Cyber Terrorist	External	✓				Ideology	Physical harm; Damage			✓						✓	✓
Cyber Vandal	External	✓				Dominance	Personal Satisfaction	✓	✓	✓			✓	✓	✓	✓	
Data Miner	External	✓				Organizational Gain	Technical advantage	✓					✓	✓			
Disgruntled Employee	Internal		✓	✓	✓	Disgruntlement	Reputation Damage	✓		✓			✓		✓		
Government Cyber-warrior	External	✓				Dominance	Physical harm; Damage	✓	✓	✓						✓	✓
Government Spy	Internal		✓	✓	✓	Ideology	Technical advantage	✓	✓	✓	✓			✓		✓	✓
Hacktivist	External	✓				Ideology	Reputation Damage	✓					✓	✓			
Information Partner	Internal		✓			Organizational Gain	Business advantage					✓	✓	✓			
Internal Spy	Internal		✓	✓	✓	Personal Financial Gain	Acquisition / Theft	✓					✓	✓	✓		
Online Social Hacker	External	✓				Personal Financial Gain	Acquisition / Theft	✓							✓		
Organized Crime	External	✓				Organizational Gain	Acquisition / Theft	✓	✓	✓	✓			✓	✓	✓	✓
Outward Sympathizer	Internal		✓	✓	✓	Personal Satisfaction	No Malicious Intent		✓	✓			✓	✓		✓	
Radical Activist	External	✓				Ideology	Material Damage	✓	✓	✓			✓	✓		✓	
Reckless Employee	Internal		✓	✓	✓	Accidental / Mistake	No Malicious Intent					✓	✓	✓			
Script Kiddies	External	✓				Personal Satisfaction	"15 Minutes of Fame"	✓	✓	✓			✓	✓	✓		
Sensationalist	External	✓				Notoriety	"15 Minutes of Fame"	✓					✓	✓			
Untrained Employee	Internal		✓	✓	✓	Accidental / Mistake	No Malicious Intent					✓	✓	✓			

Based on the research and consultation with the experts, all the cyber attacks on vehicles today can be summarized in five attack methods. The specific details of methods that are covered by these five method categories are dependent on the skill level of the threat agent, vehicle make and model and the final goal. It is difficult to state which specific method that each of the threat agents might conduct and without insight into real incident/breach reports the decision was made to categorize the methods on a higher level.

Theft of PII and business data - The threat agent can employ a variety of methods for stealing PII data from the vehicle or from the car manufacturer company. Business data can also include technical data about the company's products, production processes and technologies they are developing.

Denial of Service - The method that has the biggest potential to be used in the automotive industry is ransomware. This means the attacker would infect the vehicle with ransomware by exploiting one of the attack surfaces. Ransomware would prevent the vehicle from starting or from performing some other action that is critical for the vehicle to function properly. Afterwords the attacker would seek ransom money from the victim, their car would be unusable until the ransom is payed, after which the attacker would provide them with a key-code to unlock and allow access to their vehicle.

Intentional manipulation - This method refers to any type of attack that gives the attacker access to the control functions of the vehicle such as the steering wheel, brakes, engine etc. Having access to these functions can allow the attacker to cause

traffic accidents, traffic jams or even to cause serious or deadly injuries to the driver/-passengers.

Unauthorized physical access - Different methods for car-jacking are the main ones that are covered by this method category, but there can also be other reasons for unauthorized access to the vehicle. The "Evil maid" attack could be one example that does not lead to car-jacking, but rather to some other objectives. The attack refers to getting physical access to the vehicle, infecting the vehicle with some type of malware through an USB port or any other connection point in the vehicle and later on the attacker can access the car remotely and perform different malicious actions.

Unpredictable - The main purpose of this method type is to reflect the methods of the employees (threat agents) and the information partner. These threat agents do not have a malicious intent but rather through mistakes and accidental actions create a harmful situation for the company.

The final attribute of the MOL library is the impact of the actions taken by threat agents, this can refer to the car manufacturer company, the vehicle or the PII information stored in the vehicle memory.

6.6.3 Common Exposure Library (CEL)

The third library that the TARA methodology relies on is the Common Exposure Library (CEL) where it lists all known exposures and vulnerabilities at the company. In our case the exposures and vulnerabilities are related to the connected car and the automotive industry.

Figure 6.4: 18 most common attack surfaces of the connected car

The library should also map existing security controls to each of the identified exposures and then compare those security controls with the list of recommended

security controls. By doing this the library provides insight into the residual risk that is present because the existing security control is not the one recommended by security standards. This information is very sensitive, confidential and specific to each car manufacturer which is why we were not in the position to include it in the Common Exposure Library in this thesis. Because of this the CEL library in this section is not complete and should be perceived as a list of the most common vulnerabilities in the automotive industry. Figure 6.4 shows 18 of the most common attack surfaces or exposures of the connected car.

The list of common exposures was based on extensive literature survey and consultation with security experts from one major car manufacturer. Security experts with experience in the automotive industry have evaluated the list and rated each exposure according to the level of likelihood of being exposed. The security experts work across seven different companies, including two major car manufacturers. The CEL library created for the purpose of this thesis has three attributes that describe each of the exposures listed in the library.

Level - Describes the likelihood of being attacked and exploited for their vulnerabilities. It has three levels: high, medium and low.

Type of Access - Describes the most likely access to the attack surface in order to exploit their vulnerability and perform a successful attack. Two parameters define this attribute:

Physical access means that the attacker would need to physically access the vehicle or a device that will be connected to the vehicle at some point, in order to perform an attack. This does not imply that there is no wireless means of exploiting this surface, but rather that the most likely scenario would include prior physical access.

Wireless access means that the most likely scenario in order to exploit the vulnerability of this attack surface would include wireless access and attack.

Impact Potential - The impact attribute describes the potential impact if the attack surface is exploited and a successful attack is performed. It has the following three parameters:

Safety - This is the highest impact level which means if the attack surface is attacked the possibility of affecting the safety of the passengers is high. This means that the attacker could get access to some of the critical functions of the vehicle if that is the goal of the attack. This level also includes the next “data privacy” level meaning that if the attacker can get access to the critical vehicle functions, then it would not be a problem to access private user information stored in the vehicle. This attribute shows clearly how the segregation between different in-vehicle systems is almost non-existent because if the attacker penetrates any of these attack surfaces, they could also access some of the critical vehicle functions. The attacker’s goal and persistency determines the length of the attack and the safety functions thus affected.

Data privacy - This level refers to attack surfaces which if exploited could, most likely, lead to privacy violations.

Car-jacking - This attack surface directly relates to unauthorized physical access to the vehicle - car theft.

Table 6.3: Common Exposure Library (CEL)

Level	Exposures	TYPE OF ACCESS		IMPACT POTENTIAL		
		Physical access	Wireless access	Safety	Data Privacy	Car-jacking
HIGH	OBD II port	✓		✓		
	Wi-Fi		✓	✓		
	Cellular connection (3G/4G)		✓	✓		
	Over-the-air update		✓	✓		
	Infotainment System		✓	✓		
	Smart-phone	✓		✓		
MEDIUM	Bluetooth		✓	✓		
	Remote Link Type App		✓	✓		
	KeyFobs and Immobilizers		✓			✓
	USB	✓		✓		
	ADAS System		✓	✓		
	DSRC-based receiver (V2X)		✓	✓		
LOW	DAB Radio		✓	✓		
	TPMS		✓		✓	
	GPS		✓		✓	
	eCall		✓	✓		
	EV Charging port	✓		✓		
	CD/DVD player	✓		✓		

The exposures in table 6.3 are sorted from the highest exposure (OBD II port) to the exposure that has the minimum likelihood of attack (CD/DVD player). The next sections will give brief information about each of these attack surfaces starting from the highest ranked exposure.

OBD II Port

The **OBD II port** (On-Board Diagnostics) is the oldest interface in the CEL library. The interface is typically located under the steering wheel. It is mainly used by service shops to run diagnostic checks and to read status information about different vehicle subsystems.

It was firstly used to make modifications related to tweaking the engine or the vehicle mileage, while today this port can be used for orchestrating a wireless attack or violating the privacy of the driver. The attacker would need prior physical access to the OBD port in order to pull off any type of attack. The security mechanism of this interface is so low that it would give almost full access to the entire vehicle system. Some of the possible wireless attacks could be conducted in case an aftermarket telematics unit is connected to this port [47], or if a wireless insurance/rent-a-car dongle (Figure 6.5) [68, 120] is plugged into it. The attack could affect the safety features of the vehicle as well as violate the privacy of the driver [102, 59, 30, 101, 5].

Figure 6.5: Connecting an OBD dongle to the OBD II port [91]

Wi-Fi

The Wi-Fi connection is a new feature of vehicles today. The vehicle can offer this in a form of a hot-spot over a dedicated 3G/4G connection, and in this case the vehicle owner would have to pay additional fees to use the feature. The other form of this function is to use the Internet connection of the driver's smart-phone in which case no additional charges would be made. In both cases the Wi-Fi connection is broadcasted through the in-vehicle system.

This interface gives direct wireless access to the vehicle, although the range is limited it can still be used to perform an attack. The initial attack can be used to infect the vehicle with malware which would enable the attacker to access the car later on, possibly from a greater distance using the vehicle's cellular connection. Recent attacks have shown that this interface can be used to perform attacks allowing the attackers to disable the alarm system, control the vehicle lights, drain the battery or even control the brakes of the vehicle [79, 44, 20].

Cellular connection (3G/4G)

Vehicles can have a dedicated cellular connection using a SIM-card that is implemented by the OEM and can not be replaced by the driver. This connection is used for exchanging information with the car manufacturer such as delivering software updates or providing Internet access for applications in the Infotainment center.

This was the entry point for the famous Jeep Cherokee attack performed in 2015 [20]. The attackers exploited a vulnerability that allowed them access to the critical vehicle functions such as the steering wheel, brakes, infotainment system etc. A constant connection over a cellular network is certainly a tempting attack surface and the research shows it as a very likely target [102].

Over-The-Air (OTA) updates

This feature refers to software and firmware updates delivered to the vehicle over an Internet connection without visiting the service shop. A very small number of vehicles has this feature today but it is estimated that by 2022 over 200 million connected cars will have OTA updates enabled [40]. The main reason for the OTA updates becoming a standard is because they provide a cheaper and more effective way of delivering updates for software bugs and vulnerabilities.

It is very important for this feature to have a strong security mechanism that would ensure a secure connection with the service provider and the integrity of the software package. If this feature gets compromised by an attacker it could lead to major safety issues endangering the driver and the passengers. Research has shown that OTA updates are a major security concern and need to be addressed very carefully [59, 12, 45, 42, 32].

Infotainment system

The infotainment system is gradually becoming a standard in the automotive industry and is turning the car into an entertainment center with various features and Internet access. This system offers access to web browsers, social media applications, games and other applications (Figure 6.6) that the user can download from the Internet.

The famous Jeep Cherokee attack from 2015 used a flaw in the Uconnect [20] entertainment system in order to get remote access to the vehicle. The Infotainment system is connected directly to the Controller Area Network (CAN) bus. As previously mentioned the in-vehicle network segmentation is very low which is why the attacker can access critical systems just by compromising the entertainment center [102, 59]. A recent paper [106] demonstrated another flaw in the infotainment system that exploits the MirrorLink Protocol in order to get remote access to the vehicle's controls.

Figure 6.6: Common example of applications in the Infotainment system [95]

Smart-phone

Almost every new car today has an option to pair with your smartphone and make it easier to make phone calls, access the phone book, play music from the phone on to the car's speaker system or even share the smartphone's Internet connection with the vehicle.

If the smartphone gets infected by malware it could easily spread to the vehicle and allow the attacker to further extend the length and scope of the attack and compromise the vehicle system. The smartphone could be used to send malicious messages to the CAN network if the attacker gains access to it and, prior to the attack, enables a certain communication protocol in the infotainment system [106]. Applications in the smartphone could also be exploited and this has already happened a number of times, but more details will be given in the "Remote link Type App" section.

Bluetooth

The main usage of the Bluetooth interface in the vehicle is to pair the smartphone with the vehicle system. This enables making phone calls through the in-car system, accessing your phone book and playing music on the car speaker system. The range of Bluetooth is around 10 meters but it can be extended through amplifiers and directional antennas.

Attacks on the Bluetooth connection can be conducted with an un-paired device and with a device paired with the in-vehicle system. The research shows that a malicious payload can be injected into the vehicle system by exploiting a vulnerability in the Bluetooth interface connected to the vehicle's telematics unit [20, 102, 36].

Remote link Type App

This refers to different applications in the Infotainment system or in the driver's smartphone that provide remote access to the vehicle system. This feature allows drivers to unlock, locate, track, turn on the heating, AC or even start the car's engine and all of this remotely using an application on their smartphone.

Although this feature is very appealing to the driver it has significant security vulnerabilities that could allow the attacker to gain access to the vehicle system and the inside network. Many of the major car manufacturers (GM, BMW, Tesla, Nissan) have had security issues with this feature that was exploited by the attacker [77, 97, 117, 119].

KeyFobs and Immobilizers

The main usage of these two technologies is for unlocking the vehicle and preventing any unauthorized access that would enable the attacker to get inside the car and start the engine. The immobilizer is a small device that prevents the fuel injection to the engine and thus prevents the engine from starting up, unless a correct key is inserted in the vehicle. This mechanism is mandatory in all vehicles. Key Fob is a

remote key that unlocks the vehicle at the push of a button.

Car thieves are the main threat agents that target these attack surfaces. A common attack involves intercepting the frequency and the code that the car owner sends by pressing the button on the car keys, later on the thief tries to replay this code to the car in order to unlock it. In a recent paper by security experts from the University of Birmingham, it was revealed that over 100 million cars sold by Volkswagen since 1995 have a security flaw in the key-less entry systems and are vulnerable to an attack [37]. Various researchers have proven that KeyFobs and Immobilizers are not secure enough and need more improvement in order to protect the vehicle from being stolen [4, 99, 3].

USB

Almost every modern car today has a USB interface for various purposes such as updating the vehicle software or charging the smartphone. USBs are very well known in the computer world as devices that can easily transfer malware from one computer to another even without an Internet connection. The same situation can happen in the automotive industry which is why this interface needs proper security mechanisms. It was also discovered that using a USB dongle can allow an attacker to exploit it and gain access to the vehicle's functions [39].

ADAS System

Figure 6.7 shows different subsystems of the ADAS (Advance Driver Assistance System) used by modern cars today. The main features of this system are the LDW (Lane Departure Warning), ACC (Adaptive Cruise Control) and the Brake Assistance/Collision Avoidance System.

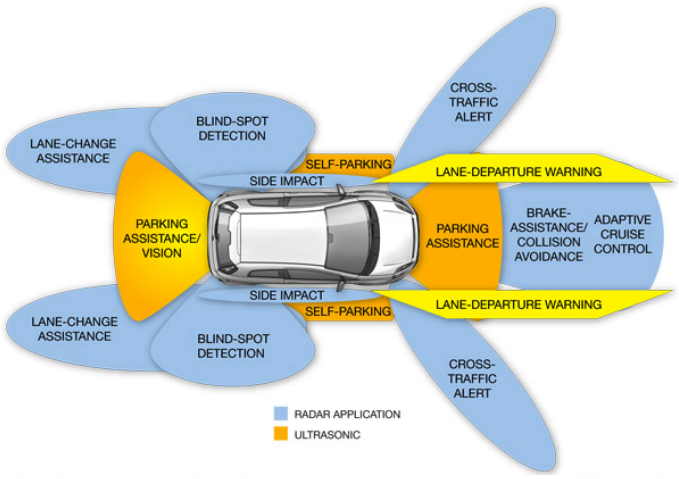

Figure 6.7: Advanced Driver Assistance Systems [85]

If the attacker would be able to inject malicious data into these systems or force the sensors to read false data, it could lead to major safety issues which could as a

consequence cause material damage or injury to the driver and the passengers. A recent paper by Intel Security presented possible threats and vulnerabilities of this system [75].

DSRC-based receiver (V2X)

The DSRC (Dedicated short-range Communications) is a high-speed wireless technology with a medium range (< 1 km) and a very low latency (50ms) that is specifically designed for the use in the automotive industry [9, 128]. This is one of the key wireless protocols to be used with the upcoming V2V and V2I technologies. It is constructed in a similar way as the existing Wi-Fi communication systems (IEEE 802.11p is the standard used in DSRC which is a subset of the IEEE 802.11 standard).

Because it is based on a similar standard as the Wi-Fi, it is vulnerable to similar attacks. These attacks include jamming, spoofing, interference and attacks on user confidentiality [34, 17].

DAB Radio

The DAB (Digital audio broadcasting) radio broadcasts digital audio radio services and it is used in most countries in Europe and Asia. The radio is in most cases integrated into the Infotainment center and as such connected to the internal CAN network.

A security expert from the NCC Group company managed to perform a successful attack on a vehicle through the DAB Radio. Davis created a fake DAB Station which broadcasted malicious data to the targeted car and allowed him to compromise the infotainment center [2]. From this point the attacker could access some of the critical controls such as the steering wheel and the brakes.

TPMS

The TPMS (Tire Pressure Monitoring System) system is used to monitor the air pressure inside the tires and notify the driver if the pressure is too low. The system is suppose to increase the safety of the vehicle by notifying the driver in time about potential problems with the tires.

The main vulnerability of the system is that it broadcasts a specific ID number which can be used to identify the car and as such could be used for tracking specific vehicles. Even though the range of TPMS sensors is around 40 meters it still represents an interesting attack surface that could be exploited by the attackers [48, 102].

GPS

The GPS (Global Positioning System) is a technology that most cars today have that is used to help the drivers find the right path to their destination. The reason it is vulnerable is that an attacker can use this system to locate and track specific

vehicles as well as extract GPS history and get information about driver's recent routes and home address. The attack surface is mainly seen as a threat to privacy.

eCall

The eCall is a new initiative of the European Union that would allow the car system to call the emergency services and send location data in case of a serious traffic accident. According to the EU this feature would decrease the response time of emergency services by up to 40% in urban areas and by 50% on the country side saving up to 2500 lives every year. The eCall system is not implemented in many cars today but in the future it could potentially be exploited by attackers because of its connection to the mobile network [127].

EV Charging port

The usage of vehicles powered by electricity is becoming more popular by each year, electric car manufacturers such as Tesla have their own charging stations across the world that can be used for free. The main threat to the EV charging port is represented through the use of the charging stations (Figure 6.8). These stations are usually connected to the Internet and have access to PII data of the driver when the car gets connected to the charging station. Various attack scenarios were presented in a recent talk by a security experts working for a company that produces these charging stations [14]. These scenarios included identity theft, financial theft and DoS attacks that could take down the entire smart grid which will in the future be connected to these charging stations.

Figure 6.8: EV charging station [96]

CD/DVD Player

Every vehicle today has a CD/DVD player in their infotainment center and even though it sounds very unlikely that a music CD could be used to attack the vehicle, it is actually possible to do this. Researchers have shown that a specifically designed mp3 file could be used to compromise the CD/DVD player which is already integrated in the infotainment center and as such connected with the internal CAN network [102, 78].

6.6.4 Risk comparison for threat agent profiles

Based on the survey results and with support of the domain experts a graph was created that shows risk levels for each threat agent when the connected car is taken as the target.

Figure 6.9 shows which threat agents are especially important to consider when developing security mechanisms for the connected car. The *default risk* as stated in the figure represents the general risk to different IT services in the IT world while the *project risk* represents the connected car. The method identified six threat agents that have an elevated risk level as can be seen in the figure. The threat agent that was identified as the one posing the greatest risk was the Sensationalist; the other five agents are shown in Figure 6.9. The level of risk that each threat agent represents today will change over time and it will be interesting to see the way it will change when services such as autonomous driving, V2V and V2I become a reality.

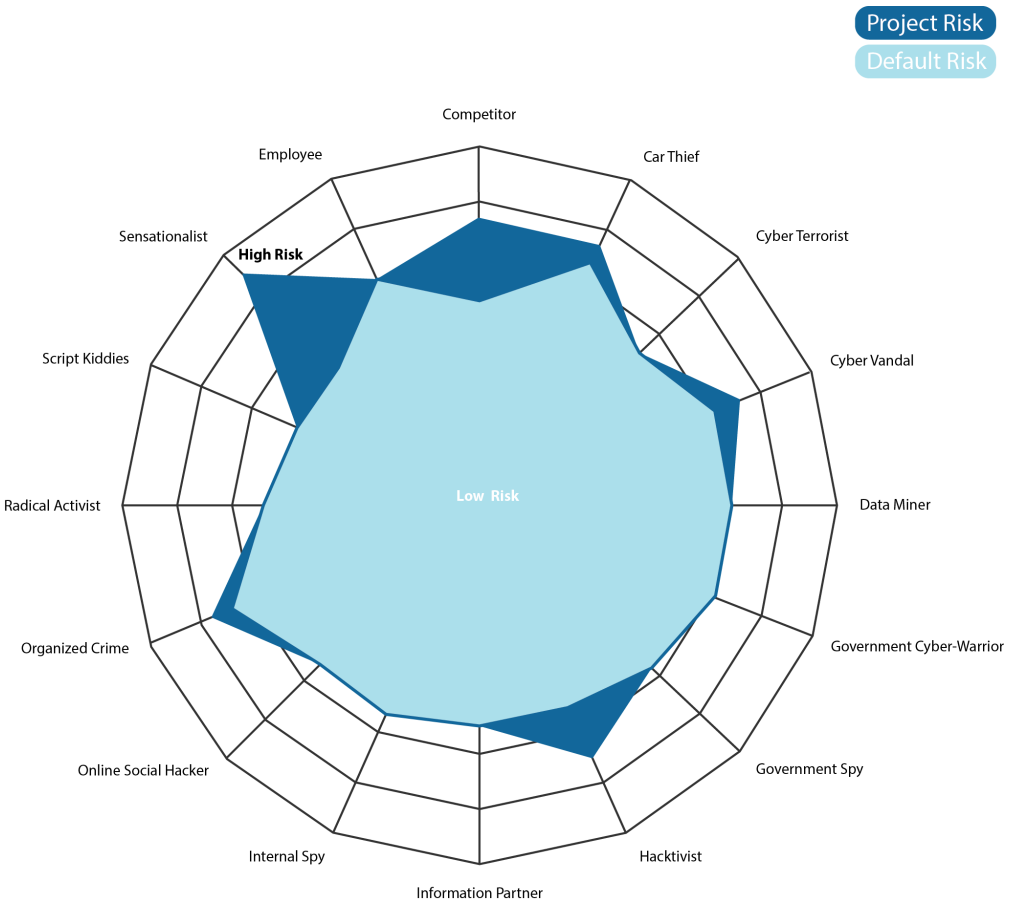

Figure 6.9: Risk comparison for threat agent profiles

6.7 Summary

The TARA method that was adapted and applied to the connected car showed that it can be used in the automotive industry to identify threat agents and their attributes, common exposures and attack methods. By creating all three libraries (TAL, MOL and CEL) the method provided useful information that can later be used by security experts in different car manufacturer companies.

The CEL library that was created is not complete because of its sensitive nature, but when a car manufacturer company creates it internally they will have a more accurate image of which attack surfaces have insufficient protection mechanisms. By focusing their attention on the identified attack surfaces they will use the companies resources in a more efficient way and avoid over-securing any part of the system.

The TARA method showed how adaptable and comprehensive it is and with some minor corrections it can be used in the automotive industry without any constraints. One important value of the TARA method is that the results of it are fairly easy to understand even for people in other departments of the company that have no technical experience.

7

Threat modeling of the AUTOSAR standard

After conducting the TARA method and applying it to the connected car concept, in this chapter the focus will be on the vehicle software architecture that is based on the automotive standard AUTOSAR. The method that is used for the software-centric approach of the threat modeling process is the STRIDE method, invented by Microsoft. This method is probably the best method when applying the software-centric approach and it has a special tool that was designed by Microsoft in order to make the method easier to use even for people with less technical backgrounds.

The method will be applied on a very specific part of the vehicle that controls the interior lights, and this part of software is based on the AUTOSAR standard. The process will show how the STRIDE method can be successfully applied to systems in the automotive industry in order to discover security vulnerabilities and learn which security protocols need to be improved or implemented.

The second part of this methodology includes testing the vulnerabilities found in a real-world system. This system is represented by a hardware board provided by Arccore, that contains an implementation of a software application that controls the interior lights in the vehicle. This process will double-check the existence of threats from each of the STRIDE categories and ensure more reliable results.

7.1 The Interior Light Application

The AUTOSAR architecture is very complex and it takes quite some time until one understands the entire standard with all of its components and services. The time limitation that this thesis has did not permit a more extensive threat modeling of this standard which is why only one smaller part of the vehicle, that is based on this standard, was taken as a target of the threat modeling process.

The software application that controls the interior lights in the car is the target of this threat modeling process. This application is based on the AUTOSAR standard, and the information flow from the ECU level up to the application level is implemented in this example. The main reason for choosing this component is because the Arccore company provided us with a complete hardware and software solution needed to simulate this component as if a real vehicle environment was involved.

The staff from Arccore provided support in understanding this hardware board and the software that the board was running on.

The *Interior light application* consists of seven different software components (SWCs) such as the Light Actuator and the Door Sensor SWC, each providing a specific function for the interior light application. The functionality and the logic of this software application is simple. It receives input data from the sensors (Door Sensor SWC) that notify the application if the vehicle door is open/closed and if the car trunk is open/closed. After analysing the input data from the sensors, the application sends signals to the actuators (Light Actuator SWC) that control the interior light of the vehicle and notifies them if the lights should be turned on/off. The information in this example is sent over the internal vehicle network CAN. More details about the software and the hardware board will be given in section 7.3.

7.2 STRIDE

The STRIDE method allows threat identification in the design phase of any software or hardware and as such gives insight into potential attack scenarios. There are two variants of the STRIDE method, per-interaction and per-element, as mentioned in an earlier chapter. In order to apply the method, security experts first need to create DFD diagrams of the system that needs to be analyzed. Afterwards the method examines these diagrams in order to detect possible threats to the system. The threats are categorized into six different categories:

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privileges

The inspection of DFD diagrams can be done manually (brainstorming sessions) or by the Microsoft Threat modeling tool which uses the STRIDE per-interaction variant. The method conducted in this thesis will use the last version of the Microsoft Threat modeling tool (version 2016). As a result the tool generates a complete list of all found vulnerabilities based on the input DFD diagrams.

7.2.1 Adaptations

The STRIDE method and the Microsoft Threat modeling tool are both intended for the use in the computer industry which is why certain adaptations had to be made to the methodology.

The main part of this adaptation is reflected in the template that is used with the MS Threat modeling tool. This template is the core of this tool because it provides different elements that are used to create a DFD diagram. Each of these elements

is associated with a specific list of threats, and based on the type of interaction between elements in the DFD diagram, the tool generates a threat report. For this reason the original Microsoft template will not be used because the elements and the associated threats are based on the computer industry and do not translate well to the automotive industry.

The template [43] used in this thesis was created by the NCC Group, is specifically designed for the automotive industry, which means that the elements in the template correspond to different vehicle entities, parts and interfaces. The current version of this template consists of elements on a higher abstraction level which is why some additional elements had to be created.

7.2.2 NCC Group template

NCC Group is a company with extensive knowledge and experience in cyber security that has recently started to get more involved in the automotive cyber security area. Earlier in 2016, one of the security experts from this company published research in which he managed to perform a successful attack on a vehicle using a fake DAB Radio station [2].

The template this company created is designed for the automotive industry and some of the main features of this template are [43]:

- Elements that represent processes and data stores are directly related to the connected car
- External Interactors are based on the automotive industry
- Data Flows correspond to the messages that are exchanged on the internal CAN network or externally, over the air.
- Trust boundaries are suitable for the environment, V2V technology and the internal vehicle network.
- Threat types are based on the STRIDE method and customized to the components of the connected car
- Each threat has a Priority level, description of the possible attack method and a mitigation strategy to prevent that attack.

7.2.3 Methodology and tools

The initial step of this method is to do research on the specific, AUTOSAR based, *Interior Light application* that was provided by the Arccore company. The needed documentation was also provided by Arccore along with support in understanding some of the functionality of different SWCs that are used by this application.

After understanding how this application works and the logic behind it, the next step was to create the DFD diagrams that represent the flow of information that

goes through this AUTOSAR application. The DFD diagrams are the main part of this method and they are created using the Microsoft Threat modeling tool and the NCC Group template. This step is conducted with the support of domain experts from Arccore and NCC Group.

The last step is to generate a threat report by using the MS Threat modeling tool and examine the list of threats in order to exclude the false positives. Additional validation was conducted by performing security tests on a real system that was simulated by the hardware and software acquired from the Arccore company. More details on the validation is given in section 7.3.

The next section will explain the process of creating the DFD diagrams and the information flow in the AUTOSAR architecture. Each layer of AUTOSAR that handles the information is explained in detail. The results are given in the last section.

7.2.4 Data Flow Diagrams

This section introduces two DFD diagrams that represent the *Interior light application*. The focus of these diagrams is on the information flow through different layers of the AUTOSAR architecture. Figure 7.1 shows the layered AUTOSAR architecture along with different modules that will be used in the two DFD diagrams created in the next sections. The diagrams will show all the input/output data of the *Interior light application* such as the information that comes from the sensors, actuators or some other ECU on the CAN network.

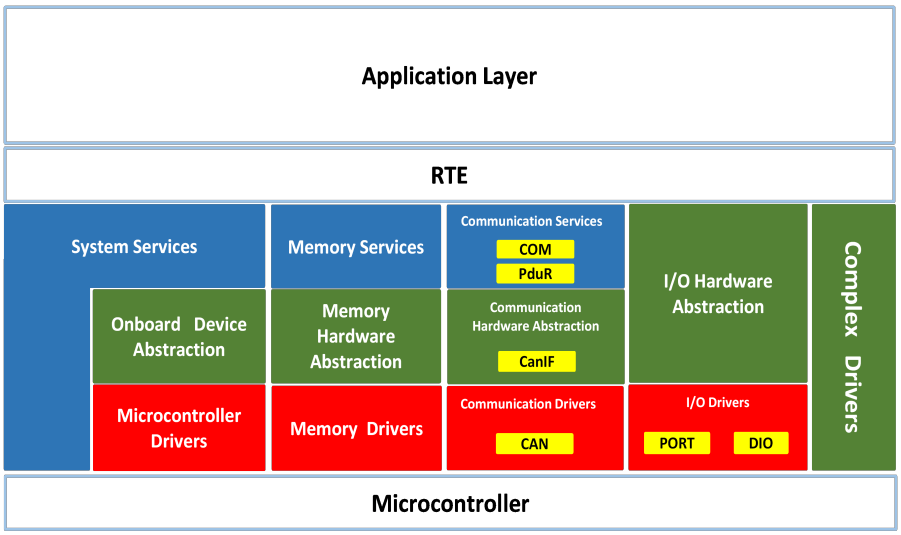

Figure 7.1: The layered AUTOSAR architecture

AUTOSAR Communication Layers

The first diagram that was created (Figure 7.2) shows different modules, from each layer, that are involved in the communication services of the AUTOSAR architecture. Elements are represented with different colors depending on which AUTOSAR layer they belong to. The information flow from the ECU level up to the *Interior lights application* (Application layer) is clearly visible. The main point of input in this DFD diagram is the internal CAN network to which the ECU with the *Interior lights application* is connected.

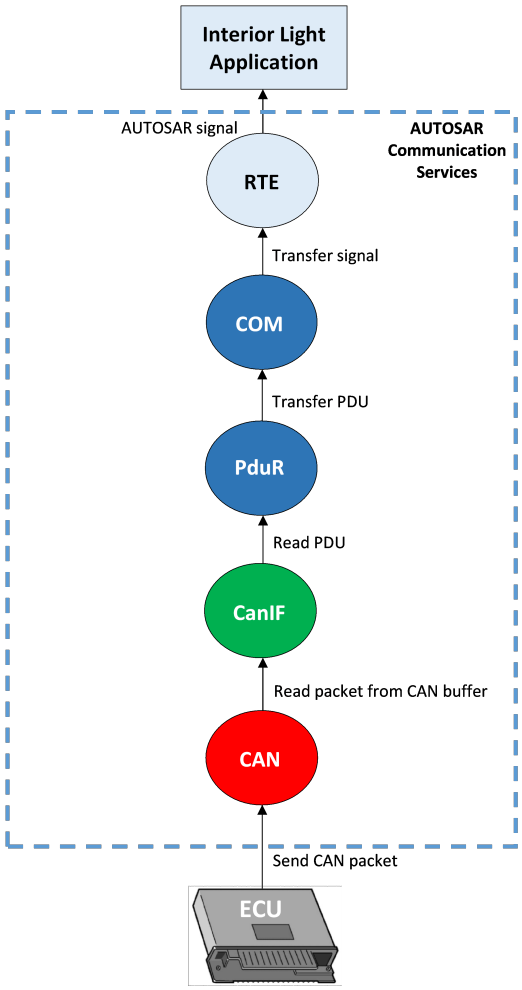

Figure 7.2: DFD diagram of the *Interior light Application* - COM Layers

Most vehicles today use the CAN network and this is why the example in this thesis is also based on this network. The example represents part of one ECU that controls the interior lights of the vehicle. This ECU is connected to other ECUs over the CAN network. When a message comes over the CAN network from another ECU or some other source that has access to the CAN network, it is transferred through the different layers of the AUTOSAR communication stack and finally to the *Interior light application*.

The packet arrives first at the **CAN Driver module** located in the *Communication Drivers* layer. It gets stored in the CAN buffer. This module is located in the lowest layer; it is responsible for hardware access and offers services to the upper layers.

The packet then goes to the next layer called the *Communication Hardware Abstraction* layer. The **CANIF module** (CAN Interface) reads the packet from the CAN buffer and converts it to a PDU (Protocol Data Units) packet. This module provides a unique interface that can manage different types of CAN hardware. These can be CAN controllers or CAN transceivers used by the specific ECU.

The following layer that handles the packet is the *Communication services* layer which has two different modules. The **PduR module** (Protocol Data Unit Router) receives the packet from the CANIF module and then routes the packet onwards to the COM module. This module is also responsible for routing of the packages that come from the COM module.

The **COM module** converts the PDU packets into signals and sends it to the *Interior Light Application* through the **RTE (Run-time Environment)**. This module also converts AUTOSAR signals from the RTE into PDU packets for transmission to the lower layers. Some AUTOSAR software components are protected by the AUTOSAR End-to-End protection library, but that was not the case with the Interior Light Example.

The DFD diagram created shows two external entities. One entity is another ECU that is connected over the CAN network while the second external entity is the *Interior Lights Application*. The DFD could have one more external user such as an External user that connects to the system and the in-vehicle network and performs some changes (Malicious/non-malicious) but these actions will be visible from the threats that the MS Threat modeling tool finds after it analyzes the DFD.

AUTOSAR I/O Layers

The second DFD diagram that was created (Figure 7.3) shows different modules, from each layer, that are involved in the I/O services of the AUTOSAR architecture. These services provide the application layer with the access to different input/output information coming from the lowest layer of the AUTOSAR architecture (Microcontroller layer). In our case the modules in this DFD diagram provide access to sensors and the actuators that are required for the *Interior Light application* to function properly. The sensors provide information about whether the car doors are open/closed while the actuators are used to turn the interior lights on/off. In the DFD diagram the sensors and the actuators are represented by the "Hardware" node, because the example used from Arccore can be implemented on multiple hardware boards. More details on the hardware board will be given in section 7.3.

The DFD diagram in Figure 7.3 shows three new modules that were not part of the first DFD diagram. Each of them has a specific function to provide the application layer access to the lowest layer that communicates with the underlying hardware.

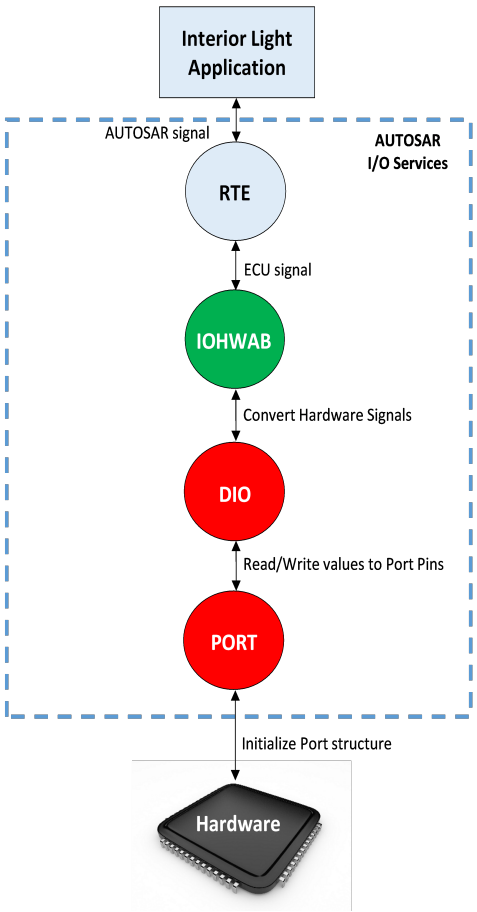

Figure 7.3: DFD diagram of the *Interior light Application* - I/O Layers

The lowest AUTOSAR layer, *I/O Drivers*, in this diagram has two modules that together provide access to the hardware. The **PORT module** is used to initialize the entire port structure of the microcontroller which includes Ports and Port Pins. In our case the microcontroller structure is represented by the Arccore hardware board, which has specific pins that simulate the door sensors and also four LED lights that simulate the actuators and the interior lights of the vehicle. This module allows the configuration of different functionality for each of these Ports and Port pins.

The next module in the lowest layer is the **DIO module**. The module works on the Ports and the Port pins configured by the PORT module. This module is responsible for controlling the digital input/output of the microcontroller as well as providing a mechanism for transferring data to/from the microcontroller's hardware pins. The module consists of DIO channels, DIO ports and DIO channel groups. A DIO channel is represented by a single hardware pin on the microcontroller.

The following upper layer called the *I/O Hardware Abstraction* (IOHWAB) is responsible for abstracting the signal path coming from the underlying hardware and providing a signal based interface for the upper software layer. It provides the SWCs with access to modules in the I/O Drivers layer.

7.2.5 Microsoft Threat modeling tool

The DFD diagram created in the MS Threat modeling tool (Figure 7.4) represents a summary of both of the previously created DFD diagrams. The modules from the "AUTOSAR communication services" are represented with a node called the "AUTOSAR COM Layer", while the modules from the "AUTOSAR I/O Services" are represented by an additional node called the "AUTOSAR I/O Layer". The other nodes in Figure 7.4 are self-explanatory and do not need any further explanation.

After consulting with the experts in the field and after performing some tests with different DFD diagrams, it was concluded that most of the threats are found on the trust boundaries and interfaces to External actors outside these boundaries. For this reason, the diagram in Figure 7.4 does not contain all the modules that were included in the DFD diagrams from the previous section. Nevertheless, the focus of this threat modeling process is to determine how to apply the STRIDE method to the AUTOSAR and to see which types of threats exist. The details of each threat that the MS Threat modeling tool generates are less important.

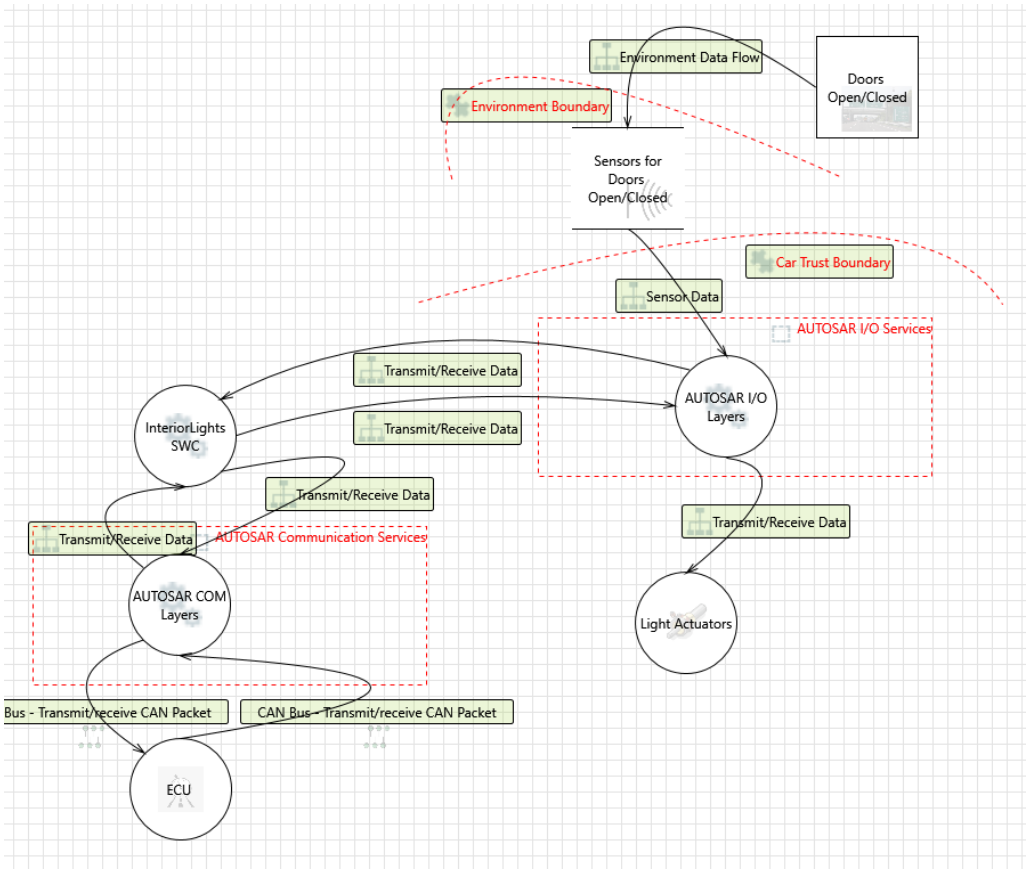

Figure 7.4: Data flow diagram created with the MS Threat modeling tool

7.2.6 Results

After the MS Threat modeling tool analysed the DFD diagram it generated a threat report with 74 different potential threats. The details of this report were not disclosed in this thesis in accordance with the Non-Disclosure Agreement (section 1.5). It is important to say that a threat from each STRIDE category was found, but it also found 17 threats that were not applicable to the *Interior Light Application* example. In order to verify the threats found, further testing described in section 7.3 was performed on the AUTOSAR hardware board which had the Interior Light example mounted on it. This ensured that the threats generated by the threat modeling tool are applicable to the actual AUTOSAR software application.

7.3 Validation

After conducting the threat modeling process it was important to test if the found vulnerabilities are applicable to a real-world vehicle system. This ensured that the results of the threat modeling process are credible and can be further analyzed by experts in order to improve the security of the system at hand. This section will give details on the testing environment as well as information about the hardware and the software equipment that was used in order to create a simulation of the vehicle system including the application that controls the interior lights.

7.3.1 Hardware equipment

In order to create a simulation of a real-world vehicle system it was required to set up a small CAN network that was attached to a computer in order to analyze the communication and the different packets that were exchanged over this network. This simulation enabled the implementation of the *Interior Light application* that was the target of the threat modeling process. The test environment that was created in order to perform security testing of the AUTOSAR hardware board consists of the following parts and can be seen in Figure 7.5.

1. **STM32 Arctic hardware board** - The main part of the equipment that simulated an ECU and contained the implementation of the *Interior Light application*.
2. **ST-Link v2 Debugger** - A standard JTAG/serial wire debugging interface that was used to flash the *Interior Light application* on to the board.
3. **Kvaser Leaf Light v2** - A CAN analyzer device that is used for analyzing the traffic on the CAN network.
4. **Capacitors** - Enabled the creation of the CAN network by acting as the network termination points.
5. **CAN-port** - This port was used to connect the CAN analyzer device to the computer.
6. **Mini USB power supply**

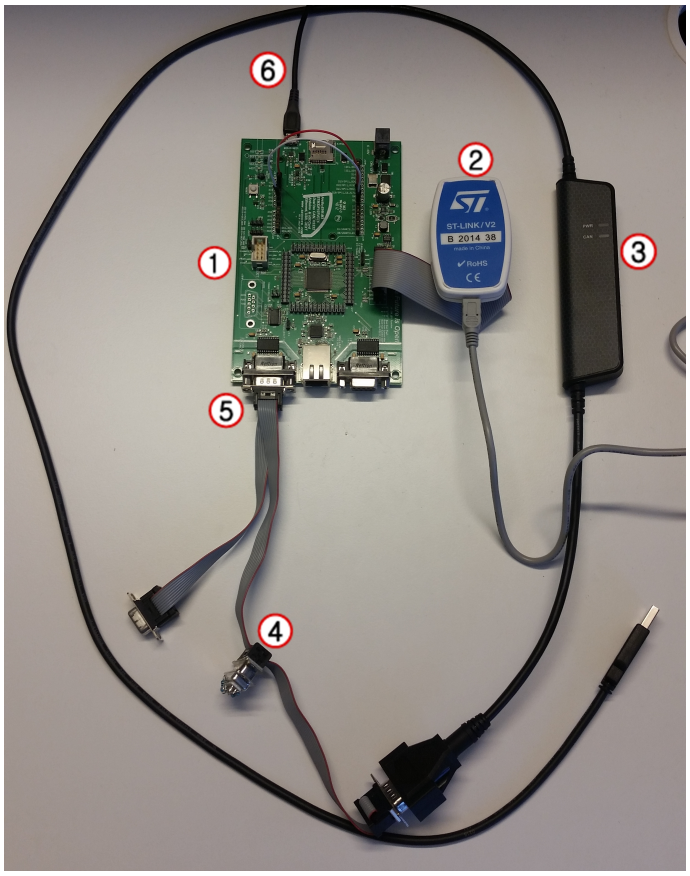

Figure 7.5: STM32 Hardware board provided by Arccore company

7.3.2 Software equipment

Besides the hardware equipment presented in the previous section, the testing required the use of the following three software applications:

1. **Arctic Studio** - used to compile the *Interior Light application*.
2. **WinIDEA** - used to flash the hardware board with a file generated by the Arctic Studio. This software was used to initialize the Arccore hardware board that was running the *Interior Light application*.
3. **BusMaster** - used to capture and send packets on the CAN network. This software is used for most of the security tests that were performed.

7.3.3 Simulation environment

The hardware equipment described in section 7.3.1 was connected to a standard Toshiba laptop running the Windows 10 operating system along with the required software that was also installed on this machine. The first step in creating the simulation of the vehicle system is to compile the *Interior Light application* using the Arctic Studio; subsequently a file that was compiled was flashed to the hardware board using the WinIDEA program. This program is also used to initialize the hardware board and enable the simulation environment for testing.

It is important to emphasize two parts of this board that were used for monitoring and the security testing. The first part is the four LED lights that indicate whether the interior lights in the vehicle are turned on/off as can be seen in Figure 7.6.

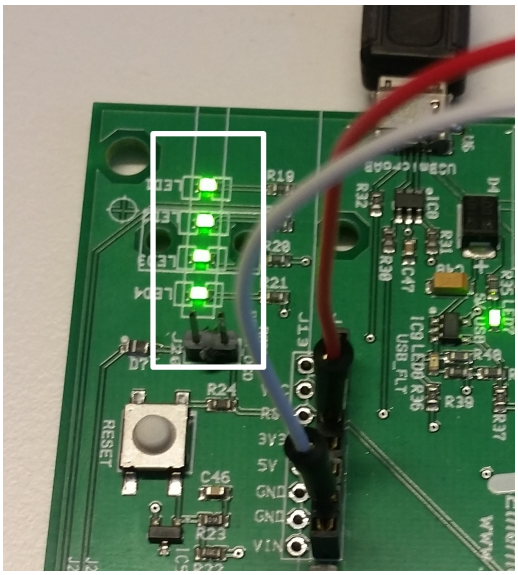

Figure 7.6: LED lights indicating if the interior light is on/off

The second part is the two wires shown in Figure 7.7, red and white, which are used to simulate the front/back door of the vehicle opening/closing. By physically changing the pin in which the wire is placed, it simulates the doors opening/closing along with the LED lights turning on/off accordingly. This is directly related to the actual car doors opening or closing.

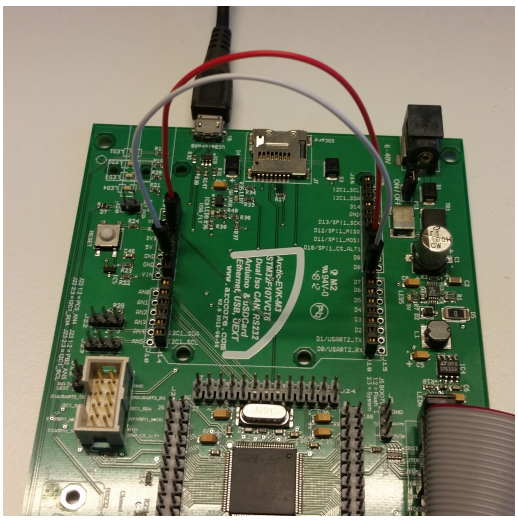

Figure 7.7: Two wires used to simulate car doors opening/closing

7.3.4 Security test cases

The goal of this testing is to demonstrate that the *Interior Light Application* implemented on the board is vulnerable to threats from each of the STRIDE categories. This would corroborate the results of the threat modeling process applied in the previous section.

The testing was performed using the BusMaster program and the CAN analyzer device. This program can capture packets on the CAN network and it also has the option to forward packets to the CAN network. By categorizing the attacks with STRIDE, the following attacks were performed.

Spoofing

It was possible to send messages to the CAN network and make the hardware board to turn the interior lights on/off even though the doors were closed/opened. This directly showed that sending a spoofed message was successful because it tricked the application into thinking that it was a valid message.

Tampering

The BusMaster program allowed us to capture packets, modify the packets and send them back on to the CAN network. This action did not cause any error messages being transmitted back, but instead the packets were accepted by the CAN network as if they were genuine ones. By capturing a message that indicated the door opening/closing, we were able to replay that message on the CAN network and cause the lights to turn on/off.

Repudiation

This type of attack refers to denying responsibility for an attack that was carried out. It is somewhat difficult to establish if this attack was successful as we do not have access to the actual vehicle and therefore we can not say which attack surface we would use to get access to the CAN network. It also depends on the logging system of the vehicle and the AUTOSAR architecture. Nevertheless, the author of this thesis is confident that such an attack would be possible to accomplish successfully but with a more complex attack vector which would make sure no traces of an attack were left in the system.

Information Disclosure

By gaining access to the CAN network, the attacker has insight into all the packets transferred between different ECUs. The example in this thesis is just a small part of the CAN network on which the *Interior Light application* sends and receives messages. It was possible to capture the messages and determine their purpose; which one is used to turn the lights on/off. Of course, in case of an actual vehicle, the number of messages would be significantly larger and it would take much more time to identify the packets, their origin and purpose - but not impossible.

Denial of Service

By sending a large amount of messages to the CAN network and the *Interior Light Application*, it is possible to jam the interior lights. This means that after a successful DoS attack the light stayed ON even when the doors were physically closed (switched the placement of the wires).

Elevation of privileges

After examining all the threats from previous sections, it is more than obvious that the elevation of privilege is also a possible attack. All the actions in the previous sections were performed acting as an External user without any authorization.

7.3.5 Results

The validation process was conducted successfully and the threats discovered by the threat modeling process were confirmed. This means that the STRIDE method described in this thesis can also be applied to other systems in the automotive industry and as such become a valuable tool for automotive security experts.

One possible attack scenario that could cause distraction to the driver and cause an accident would be if someone would suddenly perform an attack causing the interior lights to turn ON and OFF every second. This could impact the driver's concentration and subsequent ability to safely operate the vehicle.

7.4 Summary

The threat modeling process and the security testing performed in this chapter, on a small part of the AUTOSAR architecture, showed that the Interior Light application was vulnerable to attacks from each STRIDE category. The method was proven to be useful in the automotive industry and the usage of the NCC Group template contributed to this success.

Even though the latest release of the AUTOSAR standard specifies a new security module (SecOC) which is supposed to prevent most of the attacks performed in this chapter, this still means that all the cars on the road today are vulnerable. The car manufacturers that implement the new SecOC module will reduce the vulnerability of their cars, but it is still undetermined if they will implement this module on every ECU or on just the critical ones. The example here certainly would not qualify for the critical list of ECUs.

8

Discussion

8.1 TARA

Threat modeling that relates to the actual attackers is not a very common approach to threat modeling, mainly because it is hard to understand the attackers and their motivations. In order to fill this gap, Intel Security experts created a threat modeling method called TARA, described in chapter 5.1, and this method was adapted and applied to the connected car (chapter 6). The method is rather new and no research has been done outside the one published by Intel Security which is why additional work had to be conducted in order to successfully adapt and apply the method to the automotive industry. The entire work of adapting and applying the method to the connected car was done by the author of this thesis with the support of domain experts.

The method evaluates the level of threat that each of the identified threat agents poses to the matter at hand, in our example, the connected car. In order to determine this, the method combines motivation, skills, resources, vulnerable attack surfaces along with the most frequently used attack vectors. By cross-referencing these values the method determines which threat agent, attack surface and attack method would most likely be of danger to the connected car. This informs the security experts about which parts of the vehicle they need to put their focus on, in order to prevent these attacks and to make sufficient use of the company's resources.

In performing the TARA method in this thesis, we used a combination of an extensive literature survey, consultation with domain experts and an on-line survey distributed to different companies that have the experience required in this field. The information and feedback received were analysed and the TARA method was conducted. The threat agent that came out highest on the risk scale was the Sensationalist while the attack surface that is most exposed is shown to be the OBD port. These results are not far from the truth as all the attacks that we have seen up until the present day were conducted by different researchers and experts that wanted to show how insecure the vehicles really are. Even though the TARA method in its original form gives the sensationalist a minimal skill level it is obvious that when it comes to the automotive industry that this attribute has to change. The final goal of the researchers was not maybe to get famous and hit the head-lines of all news portals in the world, but it is definitely the outcome of their research and as such has to be taken in consideration.

The OBD port is shown to have the highest risk potential, and even though it requires physical access there are some cases where it can be exploited remotely which would require an insurance-dongle or a rent-a-car dongle connected to it. These devices are used by insurance companies and rent-a-car companies to track drivers and their driving behavior. The device has a cellular connection that sends information back to the owner company. Accessing the OBD port gives the attacker almost complete access to the in-vehicle CAN network.

One of the possibilities to perform this method in a better way and to get more concrete results would be to conduct it internally inside one of the vehicle manufacturer companies. This way we would have access to all the breach and incident reports that are otherwise confidential, and we would include experts that have access and real insight into the vulnerabilities and attack surfaces of that particular car manufacturer.

8.2 STRIDE

The STRIDE threat modeling method is probably one of the most comprehensive methods that exists and gives very useful results on the threats and the security mechanisms violated by these threats. Unlike the TARA method, STRIDE was used before in the automotive industry and some research has already been done concerning this specific method. This resulted in less amount of work on adapting the STRIDE method compared to the TARA method where all the adaptations had to be done from scratch. The template used with the STRIDE method already existed and just minor changes had to be made.

The STRIDE method can be performed by using the MS Threat modeling tool to generate threats based on a DFD diagram or it can be a process of multiple brainstorming sessions with experts in the field that through discussions and workshops can determine which threats exist and which security mechanisms are violated.

Because of the lack of security experts that have experience in the automotive industry, we chose the approach using the MS Threat modeling tool. The DFD diagram modeled in this tool consists of different entities that are interconnected in order to represent a model of the system. The characteristics and configuration of each entity is important because it determines the amount of potential false positive threats to be generated. Because of this reason the template used with the MS threat modeling tool was not the original template from Microsoft, but another template created by the security experts from the NCC Group. The template was tailored to be of use in the security analysis in the automotive industry. This is one step toward a mutual solution that many other companies can use in their own security analysis when it comes to vehicle security.

The results generated by the MS threat modeling tool in this thesis are maybe not completely comprehensive but they clearly show the extent of vulnerabilities of the connected car. Especially because one threat from each STRIDE category was successfully performed on the AUTOSAR hardware board which represents a real-world example. The only difficulty would be to find an appropriate attack surface to exploit in order to get this access. If the attacker gets access to the inside CAN network, the extent of damage that can be caused is potentially enormous.

8.3 Ethical and sustainable problems in relation to the thesis work

As this thesis deals with security of connected cars it is understandable that certain ethical issues had to be addressed. The thesis is publicly available for everyone which is why it is important to make sure no sensitive information is disclosed in the thesis report. Malicious attackers could otherwise use the thesis in order to get a better understanding on how to exploit certain vulnerabilities and gain access to the targeted connected car. This was an ethical dilemma, because in order to describe the methodology and show the results of the two methods, the author had to give as much information as possible. While on the other hand, the information had to be carefully selected and filtered so that it can not be misused in any way. This was accomplished successfully and the methods are explained in detail without exposing any sensitive information.

By providing two threat modeling methods specifically adapted to the automotive industry the thesis contributes to the process of sustainable development in the car industry. This will in the future ensure that vehicles have sufficient security mechanisms that will prevent attackers from gaining unauthorized access to the vehicle system and thus enable a longer life-cycle of these vehicles as they will be self-preservative. The automotive industry will need more of these methods in the future because vehicles will interact much more with other vehicles (V2V) and the environment around them (V2I).

9
Conclusion

The security of vehicles today is far from being on a level that it should be. Even though we as yet have not had any attack that caused harm to someone or to a specific company, it does not mean that this will not happen in the coming years. The automotive industry needs to implement appropriate security mechanisms on time. One way to improve the security of vehicles is to form a threat modeling method specifically designed for the automotive industry. In this thesis we adapted two threat modeling methods from the computer industry to be applicable to the automotive industry as well.

The TARA method, if performed internally inside one of the vehicle OEMs, can provide very useful results that the security experts of that company can use to further improve vehicle security. The method ensures that the company focuses on the right areas and does not over-protect or under-protect different parts of vehicle systems. The three libraries created in the thesis can be further developed and adjusted by each car OEM and used internally for improving the security of their vehicles.

The STRIDE method also has major potential to be the first method that the automotive industry experts can use to obtain reliable results. A mutual collaboration on the template used from the NCC Group is one step towards that goal. The method is intended to be applied in the design phase of the system allowing for early detection of vulnerabilities and building of a more secure software.

Finally, it is important to learn from the mistakes made by the computer industry, but it is also vital to recognise which threat modeling methods and which security mechanisms from the computer industry can be applied to the automotive industry. We need to use the existing technology and experience, adapt it to fit the automotive industry, and apply it to secure the vehicles on our roads. As the vehicles get more connected and the autonomous driving becomes a reality more threat modeling methods will be needed. The only way to build a secure connected car is to incorporate security from the start and not as an afterthought.

Bibliography

[1] Bretting A. and Ha M. Vehicle control unit security using open source AUTOSAR. *Chalmers University of Technology - Master Thesis*, 2015. http://publications.lib.chalmers.se/records/fulltext/219822/219822.pdf.

[2] Davis A. Broadcasting your attack: Security testing DAB radio in cars. *Black Hat USA 2015*, 2016.

[3] Francillon A., Danev B., and Capkun S. Relay attacks on passive key-less entry and start systems in modern cars, 2010. https://eprint.iacr.org/2010/332.pdf.

[4] Richardson A. Security of vehicle key fobs and immobilizers, 2015. www.cs.tufts.edu/comp/116/archive/fall2015/arichardson.pdf.

[5] Yadav A., Bose G., Bhange R., Kapoor K., Iyengar N.Ch.S.N, and Caytiles R.D. Security, vulnerability and protection of vehicular On-board Diagnostics. *International Journal of Security and Its Applications Vol. 10, No. 4*, 2015.

[6] AUTOSAR. www.autosar.org. Last Accessed on 2016-10-03.

[7] AUTOSAR. Specification of Module Secure Onboard Communication AUTOSAR Release 4.2.2, http://www.autosar.org/standards/classic-platform/release-42/. Last Accessed on 2016-10-03.

[8] AUTOSAR. Utilization of crypto services - AUTOSAR release 4.2.2, http://www.autosar.org/standards/classic-platform/release-42/. Last Accessed on 2016-10-03.

[9] Maitipe B. and Hayee M.I. Development and field demonstration of DSRC-Based V2I traffic information system for the work zone. *ITS Institute - Intelligent Transportation System*, 2010. http://www.its.umn.edu/Publications/ResearchReports/reportdetail.html?id=2148.

[10] Potter B. Microsoft SDL threat modelling tool, 2009. Network Security archive Volume 2009 Issue 1.

[11] Schneier B. Attack trees - modeling security threats, https://www.schneier.com/academic/archives/1999/12/attacktrees.html. Last Accessed on 2016-10-28.

[12] Link Motion Blog. Why are OTA updates so important for connected vehicles?, http://link-motion.com/blog/why-ota-updates-are-so-important-for-connected-vehicles/. Last Accessed on 2016-11-30.

[13] Steven F. Burns. Threat modeling: A process to ensure application security. *SANS Institute InfoSec Reading Room*, 2005. https://www.sans.org/reading-room/whitepapers/securecode/threat-modeling-process-ensure-application-security-1646.

[14] Naked Security by Sophos. How to hack an electric car-charging station, https://nakedsecurity.sophos.com/2013/05/17/how-to-hack-an-electric-car-charging-station/. Last Accessed on 2016-12-02.

[15] Bernardeschi C. and Din G. Security modeling and automatic code generation in AUTOSAR. *Università di Pisa Dipartimento di Ingegneria dell'Informazione Corso di Laurea Magistrale in Computer Engineering*, 2016. https://etd.adm.unipi.it/theses/available/etd-04042016-183740/unrestricted/TesiAUTOSAR.pdf.

[16] Czosseck C., Ottis R., and Ziolkowski K. Paradigm change of vehicle cyber security. *2012 4th International Conference on Cyber-Conflict*, 2012.

[17] Laurendeau C. and Barbeau M. Threats to security in DSRC/WAVE, 2006. http://people.scs.carleton.ca/ claurend/Pubs/adhocnow2006.pdf.

[18] McCarthy C., Harnett K., and Carter A. Characterization of potential security threats in modern automobiles: A composite modelling approach. *Report No. DOT HS 812 074*, 2014. https://www.nhtsa.gov/document/812074characterization potentialthreatsautos1pdf.

[19] McCarthy C., Harnett K., and Carter A. NHTSA - characterization of potential security threats in modern automobiles a composite modeling approach, 2014. https://trid.trb.org/view.aspx?id=1329315.

[20] Miller C. and Valasek C. Remote exploitation of an unaltered passenger vehicle. *Black Hat USA*, 2015. Las Vegas.

[21] Richards C. and Addams J. Boyd's OODA Loop, 2012. https://fasttransients.files.wordpress.com/2010/03/boydsrealoodaloopvii.pdf.

[22] Smith C. *The Car Hacker's Handbook : A Guide for the Penetration Tester*. William Pollock, 2016.

[23] Valasek C. and Miller C. Adventures in automotive networks and control units. *DefCon 21 Hacking Conference*, 2013. Las Vegas, USA.

[24] Valasek C. and Miller C. Car hacking: For poories. *SYSCAN'14 Conference*, 2014. Singapore.

[25] Valasek C. and Miller C. A survey of remote automotive attack surfaces. *DefCon 22 Hacking Conference*, 2014. Las Vegas, USA.

[26] Combitech. http://www.combitech.com/about-combitech/. Last Accessed on 2016-10-03.

[27] CAR2CAR Communication Consortium. https://www.car-2-car.org. Last Accessed on 2016-10-03.

[28] Vector Corp. http://www.elearning.vector.com. Last Accessed on 2016-10-03.

[29] Houlding D., Casey T., and Rosenquist M. Improving health-care risk assessments to maximize security budgets. *Intel White paper*, 2012. http://www.intel.com/content/dam/www/public/us/en/documents/solution-briefs/risk-assessments-maximize-security-budgets-brief.pdf.

[30] Klinedinst D. and King C. On board diagnostics: Risks and vulnerabilities of the connected vehicle, 2016. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=453871.

[31] Ward D., Ibarra I., and Ruddle A. Threat analysis and risk assessment in automotive cyber security. *SAE 2013 world congress and exhibition, Detroit, MI*, 2013.

[32] Nilsson D.K. and Larson U.E. Secure firmware updates Over-the-Air in intelligent vehicles. *ICC 2008 workshop proceedings*, 2008. Chalmers University of Technology.

[33] Software engineering institute CERT Program. Introducing OCTAVE allegro: Improving the information security risk assessment process, 2007. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=8419.

[34] Yeh E.R., Choi J., Prelcic N.G., Bhat C.R., and Heath R.W. Security in automotive radar and vehicular networks. *Microwave Journal*, 2016.

[35] EVITA. Security of automotive on-board networks, http://www.evita-project.org/index.html. Last Accessed on 2016-11-02.

[36] Jakob F., Kremer W., Schulze A., Großmann J., Menz N., and Schneider M. Risk-based testing of bluetooth functionality in an automotive environment, 2012. http://subs.emis.de/LNI/Proceedings/Proceedings210/211.pdf.

[37] Garcia F.D., Oswald D., Kasper T., and Pavlides P. Lock it and still lose it—on the (in)security of automotive remote key-less entry systems. *Proceedings of the 25th USENIX Security Symposium*, 2016.

[38] C'T Magazine for Computer Technique. Beemer, open thyself! – security vulnerabilities in BMW's ConnectedDrive, http://www.heise.de/ct/artikel/Beemer-Open-Thyself-Security-vulnerabilities-in-BMW-s-ConnectedDrive-2540957.html. Last Accessed on 2016-10-03.

[39] SC Magazine for IT Security Professionals. 2 million cars vulnerable to USB dongle attack, http://www.scmagazineuk.com/2-million-cars-vulnerable-to-usb-dongle-attack/article/393269/. Last Accessed on 2016-12-01.

[40] Computer World from IDG. Cybersecurity and recalls will mean OTA updates for 203m cars by 2022, http://www.computerworld.com/article/3044499/emerging-technology/cybersecurity-and-recalls-will-mean-over-the-air-updates-for-203m-cars-by-2022.html. Last Accessed on 2016-11-30.

[41] Machera G., Armengauda E., Brennerb E., and Kreinerb C. Threat and risk assessment methodologies in the automotive domain. *The 1st Workshop on Safety and Security Assurance for Critical Infrastructures Protection (S4CIP)*, 2016. Madrid, Spain.

[42] Pedroza G., Sabir M., Apvrille L., and Roudier Y. A formal methodology applied to secure Over-the-Air automotive applications. *74th IEEE Vehicular Technology Conference*, 2014. San Francisco, CA, USA.

[43] NCC Group. The automotive threat modeling template, https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2016/july/the-automotive-threat-modeling-template/. Last Accessed on 2016-11-04.

[44] The Guardian. Yet another car can be hacked – this time it's the mitsubishi outlander hybrid,

https://www.theguardian.com/technology/2016/jun/06/mitsubishi-outlander-car-hacked-security. Last Accessed on 2016-11-30.

[45] Dakroub H. and Cadena R. Analysis of software update in connected vehicles. *SAE International*, 2014. http://euro.ecom.cmu.edu/resources/elibrary/auto/2014-01-0256.pdf.

[46] Schweppe H. Security and privacy in automotive on-board networks. *Télécom ParisTech*, 2015. https://tel.archives-ouvertes.fr/tel-01157229/document.

[47] Foster I., Prudhomme A., Koscher K., and Savage S. Fast and vulnerable: A story of telematic failures. *9th USENIX Workshop on Offensive Technologies*, 2015. Washington, D.C., USA.

[48] Roufa I., Millerb R., Mustafaa H., and Taylora T. Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study. *19th Usenix Security Symposium*, 2011.

[49] The European Telecommunications Standards Institute. Intelligent transport systems (ITS). security, threat, vulnerability and risk analysis (TVRA), 2010. www.etsi.org.

[50] The European Telecommunications Standards Institute. Telecommunications and internet converged services and protocols for advanced networking (TISPAN). methods and protocols. part 1: Method and proforma for threat,risk, vulnerability analysis, 2011. www.etsi.org.

[51] The institution of engineering and technology(UK). Automotive cyber security:an IET/KTN thought leadership review of risk perspectives for connected vehicles. *The Knowledge Transfer Network*, 2015. www.theiet.org/sectors/transport/documents/automotive-cs.cfm.

[52] DeMeer J. and Rennoch A. The ETSI TVRA security-measurement methodology by means of TTCN-3 notation. *A Contribution to the 10th TTCN-3 User Conference*, 2011. SmartSpaceLab and GmbH Fraunhofer FOKUS Institute.

[53] Greenough J. The connected-car report: The transformation of the automobile. *Bussines Insider Intelligence*, 2016. https://www.businessinsider.com/intelligence/research-store?IR=T!/THE-CONNECTED-CAR-REPORT/p/47113866/category=11987294.

[54] Svensson J. AUTOSAR at Volvo AB. *Volvo 3P*, 2010. http://docplayer.net/17244597-Presented-by-jens-svensson-volvo-3p-volvo-group.html.

[55] Weschke J. and Hesslund F. Testing and evaluation to improve data security of automotive embedded systems. *Chalmers University of Technology - Master Thesis*, 2015. publications.lib.chalmers.se/records/fulltext/219731/219731.pdf.

[56] Ingalsbe J.A., Kunimatsu L., Baeten T., and Mead N.R. Threat modeling: Diving into the deep end. *Ford Motor Company, Software Engineering Institute Vol.25, No.1*, 2008.

[57] IPA Agency Japan. Approaches for vehicle information security - information security for networked vehicles, 2013. https://www.ipa.go.jp/files/000033402.pdf.

[58] Amirtahmasebi K. and Jalalinia S.R. Vehicular networks – security, vulnerabilities and countermeasures. *Chalmers University of Technology - Master Thesis*, 2010. http://publications.lib.chalmers.se/records/fulltext/123778.pdf.

[59] Koscher K., Czeskis A., Roesner F., Patel S., Kohno T., Checkoway S., McCoy D., Kantor B., Anderson D., Shacham H., and Savage S. Experimental security analysis of a modern automobile. *2010 IEEE Symposium on Security and Privacy*, 2010. University of Washington and University of California San Diego.

[60] Lemke K., Paar C., and Wolf M. *Embedded Security in Cars - Securing Current and Future Automotive IT Applications.* Springer-Verlag Berlin Heidelberg, 2006.

[61] Strandberg K. Avoiding vulnerabilities in connected cars, a methodology for finding vulnerabilities. *Chalmers University of Technology - Master Thesis*, 2016. http://publications.lib.chalmers.se/records/fulltext/238172/238172.pdf.

[62] Sung K. and Han T. Development process for AUTOSAR-based embedded system. *International Journal of Control and Automation Vol.6 No.4*, 2013.

[63] Mikulka L. Low-level software for automotive electronic control units. *Bachelor Thesis - Czech Technical University in Prague, Department of Cybernetics*, 2013. https://cyber.felk.cvut.cz/theses/papers/380.pdf.

[64] Othmane L., Weers H., Mohamad M.M., and Wolf M. A survey of security and privacy in connected vehicles. *Wireless Sensor and Mobile Ad-Hoc Networks*, 2012. Springer New York.

[65] McAfee Labs. Mcafee labs report 2016 threats predictions. *Intel Security*, 2016. www.mcafee.com/mx/resources/reports/rp-threats-predictions-2016.pdf.

[66] Lucidchart. All about data flow diagrams (dfds), https://www.lucidchart.com/pages/data-flow-diagram. Last Accessed on 2016-10-03.

[67] Böhner M., Mattausch A., and Much A. Extending software architectures from safety to security. *CIS-Technology Elektrobit Automotive GmbH*, 2015. Erlangen. Germany.

[68] Enev M., Takakuwa A., Koscher K., and Kohno T. Automobile driver fingerprinting. *Proceedings on Privacy Enhancing Technologies*, 2015.

[69] Muckin M. and Fitch S.C. A threat-driven approach to cyber security. *Lockheed Martin Corporation*, 2015. https://cyber.leidos.com/a-threat-driven-approach-to-cyber-security.

[70] Rosenquist M. Prioritizing information security risks with threat agent risk assessment, 2009. https://itpeernetwork.intel.com/whitepaper-prioritizing-information-security-risks-with-threat-agent-risk-assessment/.

[71] Schmid M. Automotive bus systems. *Atmel Applications Journal: Issue 6*, 2006. http://www.efo.ru/doc/Atmel/pdf/Atmel-Apps-Journal-6.pdf.

[72] Wille M. Automotive security - an overview of standardization in AUTOSAR. *31. VDI/VW-Gemeinschaftstagung Automotive Security*, 2015. Wolfsburg.

[73] Wolf M. *Security Engineering for Vehicular IT Systems.* Vieweg and Teubner; GWV Fachverlage GmbH, Wiesbaden, 2009.

[74] Wolf M. and Scheibel M. A systematic approach to a quantified security risk analysis for vehicular IT Systems. *Automotive – Safety and Security 2012 Conference, Karlsruhe*, 2012.

[75] Zhao M. Advanced driver assistant system - threats, requirements, security solutions. *Intel Security - Technical White paper*, 2015. http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/advanced-driver-assistant-system-paper.pdf.

[76] Machine2Machine Magazine. Global connected car M2M connections 2020, http://www.machinetomachinemagazine.com/connected-car-m2m/. Last Accessed on 2016-10-01.

[77] Wired Magazine. This gadget hacks GM cars to locate, unlock, and start them, https://www.wired.com/2015/07/gadget-hacks-gm-cars-locate-unlock-start/. Last Accessed on 2016-12-01.

[78] WIRED Magazine. GM took 5 years to fix a full-takeover hack in millions of onstar cars, https://www.wired.com/2015/09/gm-took-5-years-fix-full-takeover-hack-millions-onstar-cars/. Last Accessed on 2016-10-03.

[79] Wired Magazine. Tesla responds to chinese hack with a major security upgrade, https://www.wired.com/2016/09/tesla-responds-chinese-hack-major-security-upgrade/. Last Accessed on 2016-10-05.

[80] Metering and Smart energy International Image credit: Continental Corporation. http://www.metering.com/news/silicon-valley-startup-raises-us22m-investment-in-internet-of-moving-things/. Last Accessed on 2016-10-03.

[81] Islam M.M., Lautenbach A., Sandberg C, and Olovsson T. A risk assessment framework for automotive embedded systems. *Chalmers Security Forum*, 2016. Advanced Technology and Research, Volvo AB. Chalmers University of Technology.

[82] Morana M.M. and Velez T.U. *Risk centric threat modeling.* John Wiley and Sons, Incorporated Hoboken, New Jersey, 2015.

[83] Johnstone M.N. Threat modelling with stride and uml. *Proceedings of the 8th Australian Information Security Management Conference*, 2015. School of Computer and Security Science, Edith Cowan University, Perth, Western Australia.

[84] MyAppSecurity. Myappsecurity threat modeler, http://threatmodeler.com/. Last Accessed on 2016-10-03.

[85] EDN Network. Automobile sensors may usher in self-driving cars, http://www.edn.com/design/automotive/4368069/Automobile-sensors-may-usher-in-self-driving-cars. Last Accessed on 2016-12-01.

[86] European Union Agency For Network and Information Security (ENISA). Threat landscape 2015, 2015. https://www.enisa.europa.eu/publications/etl2015.

[87] Society of American Engineers (SAE). Cyber-security guidebook for cyber-physical vehicle systems, 2016. http://standards.sae.org/wip/j3061/.

[88] University of California at Berkeley. Cybersecurity for the automobile, is the car of the future still a car? *I and C Research Days*, 2012. Lausanne.

[89] Chalmers University of Technology. Chalmers publishing rules, http://www.lib.chalmers.se/en/publishing/to-publish/student-theses/. Last Accessed on 2016-10-03.

[90] U.S. Department of Transportation National Highway Traffic Safety Administration (NHTSA). Cybersecurity best practices for modern vehicles, 2016. https://www.huntonprivacyblog.com/2016/10/28/nhtsa-releases-new-automobile-cybersecurity-best-practices/.

[91] One2More. OBD II car diagnostic reader - bluetooth to android, pc, http://www.one2more.com/en/274-obdii-car-diagnostic-reader-bluetooth-to-android-pc.html. Last Accessed on 2016-11-30.

[92] OWASP. Threat risk modeling, https://www.owasp.org/. Last Accessed on 2016-10-03.

[93] Mundhenk P., Steinhorst S., Lukasiewycz M., Fahmy S.A., and Chakraborty S. Security analysis of automotive architectures using probabilistic model checking. *DAC '15 Proceedings of the 52nd Annual Design Automation Conference*, 2015. San Francisco, California.

[94] Lockheed Martin White paper. Gaining the advantage - applying cyber kill chain methodology to network defense, 2015. https://cdn2.hubspot.net/hubfs/91979/gaining-the-advantage-cyber-kill-chain.pdf.

[95] CarAdvice Portal. Apple carplay by pioneer, http://www.caradvice.com.au/314065. Last Accessed on 2016-11-30.

[96] The Inhabitat Portal. Japan has more electric vehicle chargers than gas stations, http://inhabitat.com/japan-has-more-ev-chargers-than-gas-stations-diffusing-range-anxiety-for-good/. Last Accessed on 2016-12-02.

[97] The Register Portal. Grand app auto: Tesla smartphone hack can track, locate, unlock, and start cars, http://www.theregister.co.uk/2016/11/25/tesla-car-app-hack-enables-car-theft. Last Accessed on 2016-12-01.

[98] Currie R. and Santander M. Developments in car hacking. *SANS Institute InfoSec Reading Room*, 2015. https://www.sans.org/reading-room/whitepapers/ICS/developments-car-hacking-36607.

[99] Verdult R. and Garcia F.D. Dismantling megamos crypto: Wirelessly lockpicking a vehicle immobilizer. *Proceedings of the 22nd USENIX Security Symposium*, 2013.

[100] Dutta R.K. A framework for software security testing and evaluation. *Lindköping University - Master Thesis*, 2015. http://www.uppsatser.se/uppsats/e148e75999/.

[101] Bayer S., Jung R., and Wolf M. OBD=open barn door? Security vulnerabilities and protections for vehicular on-board diagnosis (obd), 2015. https://www.escrypt.com/security-lab/publications/papers/.

[102] Checkoway S., McCoy D., Kantor B., Anderson D., Shacham H., and Savage S. Comprehensive experimental analyses of automotive attack surfaces. *SEC'11 Proceedings of the 20th USENIX conference on Security Pages 6-6*, 2011. University of California and University of Washington.

[103] Dhaneshwar S. Information security of a connected vehicle, https://www.linkedin.com/pulse/information-security-connected-vehicle-shashank-dhaneshwar. Last Accessed on 2016-10-03.

[104] Fürst S. AUTOSAR adaptive platform for connected and autonomous vehicles. *Euroforum Elektronik-Systeme im Automobil 11th and 12th*, 2016. Munich, Germany.

[105] Jasek S. Connected car security threat analysis and recommendations, 2015. https://www.securing.pl/wp-content/uploads/2015/10/SecuRing-Connected-Car-Security-Threat-Analysis-and-Recommendations.pdf.

[106] Mazloomy S., Rezaeirady M., Hunter A., and McCoy D. A security analysis of an in-vehicle infotainment and app platform. *10th USENIX Workshop on Offensive Technologies*, 2016.

[107] Myagmar S., Lee A.J., and Yurcik W. Threat modeling as a basis for security requirements. *Symposium on Requirements Engineering for Information Security (SREIS)*, 2005. National Center for Supercomputing Applications (NCSA) and University of Illinois at Urbana-Champaign.

[108] Infineon Car Security. Trusted driving - data security from infotainment to airbags, http://www.infineon.com/cms/en/about-infineon/company/our-contribution/car-security-infographic/. Last Accessed on 2016-10-03.

[109] Adam Shostack. *Threat Modeling – designing for security.* John Wiley and Sons, Inc., 2014.

[110] Kadhirvelan S.P. and Söderberg-Rivkin A. Threat modelling and risk assessment within vehicular systems. *Chalmers University of Technology - Master Thesis*, 2014. http://publications.lib.chalmers.se/records/fulltext/202917/202917.pdf.

[111] Casey T. A field guide to insider threat. *Intel White paper*, 2015. http://www.intel.com/content/dam/www/public/us/en/documents/best-practices/a-field-guide-to-insider-threat-paper.pdf.

[112] Casey T. Understanding cyberthreat motivations to improve defense. *Intel White paper*, 2015. http://www.mcafee.com/us/resources/deflect-targeted-attacks/wp-understanding-cyberthreat-motivations-to-improve-defense.pdf.

[113] Hoppe T., Kiltz S., and Dittmann J. Automotive IT-Security as a challenge: Basic attacks from the black box perspective on the example of privacy threats. *Computer Safety, Reliability, and Security*, 2015. Springer Berlin Heidelberg.

[114] Martin-Vegue T. How to improve your risk assessments with attacker-centric threat modeling. *Think Big*, 2014. http://www.slideshare.net/tonymartinvegue/how-to-improve-your-risk-assessments-with-attackercentric-threat-modeling.

[115] Samad T. and Annaswamy A.M. The impact of control technology - Vehicle-to-Vehicle/Vehicle-to-Infrastructure Control. *IEEE Control Systems Society*, 2011. http://ieeecss.org/general/impact-control-technology.

[116] Tesla Team. The week that electric vehicles went mainstream, https://www.teslamotors.com/blog/the-week-electric-vehicles-went-mainstream. Last Accessed on 2016-10-03.

[117] International Business Times. BMW connecteddrive hack sees 2.2 million cars exposed to remote unlocking, http://www.ibtimes.co.uk/bmw-

connecteddrive-hack-sees-2-2-million-cars-exposed-remote-unlocking-1486215. Last Accessed on 2016-12-01.

[118] International Business Times. Connected cars at widespread risk from hackers as manufacturers admit cyber security failings, http://www.ibtimes.co.uk/connected-cars-widespread-risk-hackers-manufacturers-admit-cybersecurity-failings-1547153. Last Accessed on 2016-10-03.

[119] International Business Times. Hacker takes control of nissan electric vehicle from other side of the world through leaf app, http://www.ibtimes.co.uk/hacker-takes-control-nissan-electric-vehicle-other-side-world-through-leaf-app-1545808. Last Accessed on 2016-10-03.

[120] International Business Times. Hackers disable Corvette brakes by texting dongle meant to lower insurance risk, http://www.ibtimes.co.uk/hackers-disable-corvette-brakes-by-texting-dongle-meant-lower-insurance-risk-1515125. Last Accessed on 2016-10-03.

[121] International Business Times. Tesla Model S hacked: Researchers discover six security flaws in popular electric car, http://www.ibtimes.co.uk/tesla-model-s-hacked-researchers-discover-six-security-flaws-popular-electric-car-1514352. Last Accessed on 2016-10-03.

[122] VICTA. Vehicle ICT Arena, http://vehicle.lindholmen.se/en. Last Accessed on 2016-10-03.

[123] Trumler W., Helbig M., Pietzowski A., and Satzger B. Self-configuration and self-healing in AUTOSAR. *Asia Pacific Automotive Engineering Conference*, 2007.

[124] Intel Security McAfee Whitepaper. Automotive security best practices. *Recommendations for security and privacy in the era of the next-generation car*, 2015. http://www.intel.com/content/www/us/en/automotive/automotive-security-best-practices-white-paper.html.

[125] WikiPedia. Data flow diagram, https://en.wikipedia.org/wiki/Data FlowDiagram. Last Accessed on 2016-10-03.

[126] WikiPedia. Threat model - visual representations based on process flow diagrams, https://en.wikipedia.org/wiki/ThreatModel. Last Accessed on 2016-10-03.

[127] The Computer World. New european law mandates ecall in all new cars, http://www.computerworld.com/article/2497747/vertical-it/new-eu-law-mandates-ecall-in-all-new-cars.html. Last Accessed on 2016-12-02.

[128] Li Y.J. An overview of the dsrc/wave technology, 2010. http://www.techrepublic.com/resource-library/whitepapers/an-overview-of-the-dsrc-wave-technology/.

A

Appendix 1

Survey questions

1. State the name of your company and your job description.

3. Rate each threat agent according to the level of risk which that specific threat agent represents today in the IT world. (Names of threat agents along with short descriptions were listed. Each agent had a scale of 1-4 (None-Low-Medium-High) from which the respondents could choose the appropriate level)

4. Rate each threat agent according to the level of risk which that specific threat agent represents to the connected car. (Same answer-choices were given as in the previous question)

5. What skill level is needed in order to perform a cyber attack on the connected car ? (Respondents were offered choices that corresponded to the parameters of the TARA skill attribute)

6. What are the main motivations in performing a cyber attack on the connected car ? (Respondents were offered choices that corresponded to the parameters of the TARA motivation attribute)

7. What are the main goals of the threat agents targeting the connected car ? (Respondents were offered choices that corresponded to the parameters of the TARA objective attribute)

8. What kind of resources would one need, at least, in order to perform a cyber-attack on the connected car ? (Respondents were offered choices that corresponded to the parameters of the TARA resources attribute)

9. Which of the attack surfaces below are most likely to be exploited ? (Respondents were offered with 18 different attack surfaces that are now part of the CEL library)

10. What type of method is most likely to be used when attacking the connected car? (Different type of methods were offered which were then sorted in four categories a can be seen in the MOL library)