Adapting Threat Modeling Methods for the Automotive Industry

Adapting Threat Modeling Methods for the Automotive Industry

- 15th ESCAR Conference, Berlin 2017 -

Adi Karahasanovic[1], Pierre Kleberger[1], and Magnus Almgren[2]

[1] Combitech AB
Lindholmspiren 3A
SE–417 56 Gothenburg, Sweden
adi.karahasanovic@combitech.se, pierre.kleberger@combitech.se
[2] Chalmers University of Technology - Department of Computer Science and Engineering
SE–412 96 Gothenburg, Sweden
magnus.almgren@chalmers.se

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, embedded control units (ECUs), and multiple connection points to the Internet which makes them vulnerable to various on-line threats. Recent attacks on connected vehicles have all been results of security vulnerabilities that could have been avoided if appropriate risk assessment methods were in place during software development. In this paper we demonstrate how the threat modeling process, common for the computer industry, can be adapted and applied in the automotive industry. The overall contribution is achieved by providing two threat modeling methods that are specifically adapted for the concept of the connected car and can further be used by automotive experts. The methods were chosen after an extensive literature survey and with support of domain experts from the vehicle industry. The two methods were then successfully applied to the connected car and the underlying software architecture based on the AUTOSAR standard. We have empirically validated our results with domain experts as well as tested the found vulnerabilities in a simulated vehicle environment.

1 Introduction

The world as we know it is changing and many of the devices we use daily are becoming "smart". This buzzword is appearing in everything from smart grids to smart homes with the smart appliances therein. The main aspect of these devices is their connection to the Internet, and because of it, previously local vulnerabilities are now widely exposed. The same goes for many new vehicles. A high-end car may now have more than 100 million lines of code [1], as well as multiple connections to external networks including the Internet. All this code has to be properly developed and tested in order to ensure the safety and security of the vehicle. This paper refers to these types of cars as *connected cars*.

The connected cars are equipped with a number of new technologies and features that are not possible without an Internet connection. For example, drivers now have the possibility to receive service information and traffic reports through the vehicle's dedicated cellular connection. They also have the possibility to connect their smart-phone to the vehicle (Bluetooth, Wi-Fi) and use its Internet connection to enable some of the new features of the vehicle's entertainment center. Through this center they can browse the web, access social networks, stream on-line content, etc. Many other services exist depending on the vehicle type and manufacturer. According to the Business Insider report, there will be 380 million connected cars on the road by the year 2021 [2].

Even though the connection to the outside world enables many new services, it also exposes the car and its software to a potential remote attack. There has already been a number of successful cyber-attacks on connected vehicles such as the attacks on Jeep Cherokee [3], Tesla S model [4], Nissan electric car [5] and Chevrolet Corvette [6]. As the production of these vehicles increases, so will the importance of securing them. We argue that it is important to address these security concerns as early as possible. Using threat modeling methods already at the design phase assists in early detection of security flaws instead of later detection, which may lead to a recall of many cars already on the road. Another benefit of our study is to provide a common framework that any car manufacturer can use.

In this paper, we investigate two threat modeling methods widely used in the computer industry and evaluate their suitability for the connected car. We also propose adaptations to these threat modeling methods to make them more applicable to the underlying software architecture used in today's vehicles (AUTOSAR). The first method, TARA, represents an attacker-centric approach while the second method, STRIDE, investigates the software architecture of the system and belongs to the software-centric approach. The contributions of this paper are as follows:

- Two diverged threat modeling methods are considered and then adapted to the automotive domain.
- The usability of a Microsoft Threat Modeling Tool with a template for the automotive domain is demonstrated.
- An approach to model threats to software based on the AUTOSAR standard is presented.
- The adaptation and application of the methods was partly based on an online survey that was completed by industry experts from seven different companies including two major car manufacturers.

– A list of the most exposed areas of the connected car was created with rankings: high, medium and low risk exposure.
– An empirical verification of the found threats is performed using dedicated hardware.

The outline of this paper is as follows. In Section 2, we summarize the two main threat methods that are used in this paper, as well as the automotive standard AUTOSAR. The adaptation of the threat methods to the automotive domain is then described in Section 3. The process of applying the adapted version of these two methods is described in Section 4. Even though the modified frameworks have been vetted by security specialists, we add an empirical verification of the results from the threat analysis by testing the found vulnerabilities in a simulated vehicle environment. The results are described in Section 5. We summarize related work in regards to threat modeling in Section 6. Section 7 presents a discussion of our results, followed by our conclusions in Section 8.

2 Background

After completing a larger survey of relevant literature, we chose two particular threat modeling frameworks popular in the computer industry (TARA and STRIDE) that seemed to be most suitable for the automotive industry. In this section, we give a high level overview of these frameworks before we discuss our suggested changes in Section 3. We also describe the AUTOSAR standard, as it is a central concept in the paper.

2.1 TARA

The Threat Agent Risk Assessment (TARA) method was developed by security experts from Intel Security [7] and is based on three groups of collected data, denoted as libraries:

– **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 populated internally inside a company by their security expert 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 this area and the recommended security control for this area. The difference between the current and the recommended security control shows which area 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. To conclude, these libraries provide the relevant information that is required in order to align the security strategy and thus target the most important exposures. Once derived, these libraries can be updated and used in future instances of the TARA method.

2.2 STRIDE

The STRIDE method was originally developed by Microsoft [8]. The 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. In order to apply the method, security experts first need to create Data Flow Diagrams (DFD) of the system that needs to be analyzed. The DFDs present the communication patterns between the components under investigation. Afterwards the method examines these diagrams in order to detect possible threats to the system. The threats are divided 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 using the Microsoft Threat modeling tool which uses the STRIDE per-interaction variant. The method conducted in this paper (further described in Section 3) uses the MS Threat modeling tool (version 2016). As a result the tool generates a complete list of all found threats based on the input DFD diagram.

2.3 AUTOSAR

AUTOSAR (AUTomotive Open System Architecture) was founded in 2003, with the goal to develop an architecture, independent of the underlying ECU hardware, that the automotive industry can use to reduce the increasing complexity of software in modern vehicles [9]. It is the de-facto standard for the automotive software today and 80% of global production is based on this standard.

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. The AUTOSAR standard defines security mechanisms that can be used by the software modules implemented into the vehicle system. It further specifies interfaces and procedures to provide secure on-board communication, and the exact implementation is left for the OEMs to decide on. OEMs choose the cryptographic algorithms and encryption techniques which they want to implement and use in the vehicle system [10]. The three main security mechanisms in the AUTOSAR are: Crypto Service Manager (CSM), Crypto Abstraction Library (CAL) and Secure On-Board Communication (SecOC).

3 Threat Models for the Automotive Domain

In the following, we describe our suggested modifications (based on domain expertise from industry representatives) to make TARA and STRIDE more suitable for automotive threat modeling.

3.1 Adaptation of TARA

In order to adapt and apply the TARA method to the automotive industry in general and the connected car in particular, certain modifications were made to the method. The method 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 paper, our goal was to create a more general framework that can be taken and refined within the car companies as described above. For example, the structure of the TAL and MOL library should be adapted, while the CEL library has no strict structure and as such does not require any adaptations. Three sources of information were used. First, we performed an extensive literature survey related to automotive cyber security and recent cyber attacks on vehicles. In addition to this, an on-line survey was also created and filled in by domain experts (seven different companies, including two major car manufacturers) in order to gather valuable input. The process was then followed by individual meetings with a few experts from the industry. The process is further described in a separate report [11] and only the proposed changes are discussed below due to space limitations.

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 new adapted version of this library is presented in section 4.1. The following changes are made compared to the original TAL library [12] provided by Intel.

- Ten threat agent profiles are removed and eight new profiles are added: *Outward sympathizer, Hacktivist, Cyber vandal, Online social hacker, Script kiddies, Organized crime, Cyber terrorist and Car thief.* The new agent profiles are based on three sources [13–15] along with research and consultation with domain experts.
- The "outcome" attribute is modified and now includes the following parameters: *acquisition/theft, business advantage, material damage to the vehicle, physical harm to the drivers/passengers, reputation damage, technical advantage and "15 minutes of fame".*
- Attributes assigned to one threat agent from the original TAL library were slightly modified. The *skills* and *resources* level for the *Sensationalist* threat agent were raised to a higher level than in the original model. More explanation is given in Section 7.

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 new adapted version of this library is presented in section 4.1. The following changes were made to reflect the automotive domain:

- The sections "Acts" and "Limits" are removed and replaced by the "Method" section with the following values: *theft of PII and business data, denial of service, intentional manipulation, unauthorized physical access* and *"unpredictable"*. The "Limits" section can be found in the TAL library.
- The levels of the "Impact" attribute are replaced with new impact levels: *reputation damage, privacy violation, loss of financial assets/car, traffic accidents* and *injured passengers.* The impact level reveals consequences that an attack would have on the connected car.

3.2 Adaptation of STRIDE

The main part of the adaptation of STRIDE is reflected in the template of the MS Threat modeling tool, since the template provides the different elements to create DFD diagrams. Each element is associated with a specific list of threats, and based on the type of interaction between the elements in the DFD diagram, the tool generates a threat report. We use the template

developed by the NCC Group [16] with some additions due to the higher abstraction level used here; three new elements are added that represent the underlying architecture that is based on the AUTOSAR standard.

The main reason why this method needs to be adapted is because the method itself was created for the computer industry. The MS Threat modeling tool is also intended to model DFD diagrams for environments such as Windows and Linux operating systems or different applications inside these system (i.e. web applications, client-server environments). For these reasons a special template was used, as previously stated, which contains the elements that reflect the vehicle software environment and the associated applications and interfaces. Each of these elements is associated with a group of threats that are specifically related to the automotive industry and the connected car. More information is given in Section 4.2.

4 Applying the Adapted Threat Models to the Automotive Domain

4.1 Applying TARA

The following sections describe the process of threat modeling using the adapted version of the TARA method. The target of this process is the connected car.

Methodology and Tools. The threat modeling was conducted with support of domain experts and a project manager from Intel Security in charge of the TARA method. The method is performed in six steps, the goal of which is to find the critical exposures of the connected car. The following is a short description of how these steps were performed:

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 (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 (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 were 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 attacks on vehicles can be classified into five attack methods and can have five impact levels accordingly.
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, stated in Section 5.1, can be further used by car manufacturer companies to align their security strategy and focus their resources to the areas of greatest concern.

Threat Agent Library (TAL). The adapted version of the TAL library specifies 19 different threat agents that are relevant for the automotive industry. Each threat agent is described by nine different attributes. The TAL library provides all the information that is needed in order to determine which threat agents present the greatest risk to the connected car. Thus, the TAL library is used by security experts while conducting the first two steps of the TARA method. The results of these steps are given in Section 5.1. The following is a list of attributes with a short explanation.

- **Intent** describes whether the agent's intent is to cause harm or not.
- **Access** describes what type of access the agent has to the target: internal (insider) or external (no access to internal data or resources).
- **Outcome** is an attribute that describes the final results of the agent's actions, e.g. actions taken by a threat agent could have business or technical advantage for another competing company by stealing some confidential information.
- **Resource** attribute represents the type of resources the agent has access to, e.g. does the threat agent work alone or in a team with several other threat agents, or it may even have the support of a government implying almost unlimited resources.
- **Skills** attribute describes the level of skill that the agent has.
- **Motivations** is a newly introduced attribute that explains the motivation behind an action conducted by each of the threat agents. Whether it is for personal satisfaction or financial gain it is important to know because it reveals the reason and the intensity behind the attack.
- **Visibility** describes the extent to which the agent wants to hide or reveal their identity. Some attacks are known to the victim immediately (overt/covert) while other attacks are hidden (clandestine) and the victim does not know that an attack even took place.
- **Limits** attribute describes the extent to which the agent would go in order to accomplish their goals. Whether the agent would break the law or not is described by this attribute.
- **Objective** describes the primary action the agent will take in order to achieve their goal.

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																			

Fig. 1. TAL Library showing 19 threat agent profiles and their attributes

Methods and Objectives Library (MOL). The methods and objectives library (Figure 2) shows the defining motivations (primary cause of their actions) of threat agents, their main goals and the most likely methods they would employ in order to successfully accomplish their goals. In comparison to the TAL library, where each threat agent has one or more possible motivations, 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 on-line survey. Note that the goal attribute of the MOL library is very similar to the outcome attribute of the TAL library. The difference is, in the MOL library it represents the desired result one wishes to achieve while in the TAL library, it represents consequences of threat agent actions.

Based on the research and consultation with the experts, most of the cyber attacks on vehicles today can be summarized with five attack methods. It is difficult to state which specific method 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 (Personally Identifiable Information) 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. The attacker would infect the vehicle with ransomware by exploiting one of the attack surfaces. This would prevent the driver from using the car until the ransom is paid.
- **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.
- **Unauthorized physical access.** Different methods for car-jacking are the main ones that are covered by this category, but there can also be other reasons for unauthorized access to the vehicle. Attacker could inject malware over the USB interface or the OBD port for later remote access.
- **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, which can refer to the car manufacturer company, the vehicle, or the PII information stored in the vehicle memory.

Common Exposure Library (CEL). The CEL library does not have a standardized format because it contains confidential information and is derived by each organization. The library maps existing security controls to each of the identified exposures

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					✓		✓	✓			

Fig. 2. MOL Library showing preferred attack methods of different threat agents

and then compares those security controls with the list of recommended security controls. By doing so, the library provides insight into the residual risk with respect to the existing security control compared to the ones recommended by security standards. This information is very sensitive, confidential and specific to each car manufacturer which is why it was not included in our Common Exposure Library. Therefore, the CEL library presented here is not complete, but still gives important information about the greatest exposures in the automotive industry. The list of exposures and the rankings are based on an extensive literature survey and consultation with security experts from seven different companies, including two major car manufacturers. Figure 3 shows the CEL library with rankings from the highest exposure (OBD II port) to the lowest exposure (CD/DVD player). The library has three attributes that describe each of the listed exposures:

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	✓		✓		

Fig. 3. CEL Library showing the OBD port as the most exposed interface

- **Level.** Describes the level of vulnerability. It has three levels: high, medium and low.
- **Type of Access.** Describes the most likely type of access needed in order to successfully perform an attack, either *physical access* or *wireless access* is considered the most likely.
- **Impact Potential.** The impact describes the potential impact if the attack surface is successfully exploited. It has the following three parameters: (1) *Safety* is the highest impact level which means if the attack surface is exploited the possibility of affecting the safety of the passengers is high, (2) *Data privacy* level refers to attack surfaces which if exploited could lead to privacy violations, and (3) *Car-jacking* describes an attack surface that directly relates to unauthorized physical access to the vehicle (car theft).

4.2 Applying STRIDE

To demonstrate the STRIDE analysis, we choose a specific software application: *the interior lights* of the car. The main reason for choosing this application is that the *Interior lights application* is available as an AUTOSAR application, both for simulation and as a runnable on real hardware. Furthermore, the *Interior lights application* implements information flow from the ECU level up to the application level, which is of interest for STRIDE analysis. We can then demonstrate the modeling (this section) and the results (with hardware validation, discussed in Section 5.2).

Methodology and tools. The STRIDE analysis is performed on the AUTOSAR platform provided by the company Arccore. First, analysis of the *Interior lights application* was conducted, so that the DFD diagrams could be derived. These were then created by the Microsoft Threat modeling tool using the NCC Group template. These steps were conducted with the support of domain experts from Arccore and the NCC Group. Finally, the threat report was generated and examined in order to exclude false positives. Additional validation was conducted by testing some of the found threats in a simulated vehicle environment, more information on this is given in Section 5.2.

The Interior Light Application. The 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 application 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 analyzing 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 is exchanged using the CAN network.

Data Flow Diagrams. This section introduces the DFD diagram (Figure 4) that represents the *Interior light application*. The DFD diagram is based on two previously created diagrams, one representing *AUTOSAR communication services* and the other representing the *AUTOSAR I/O services*. In Figure 4 these diagrams are summarized in two nodes, "AUTOSAR COM Layer" and "AUTOSAR I/O Layer" respectively. *AUTOSAR communication services* are in charge of transferring messages from other ECUs on the CAN network and messages that could come from external and potentially malicious users. *AUTOSAR I/O services* provide access to sensors and the actuators that the *Interior light application* needs in order to function properly.[3]

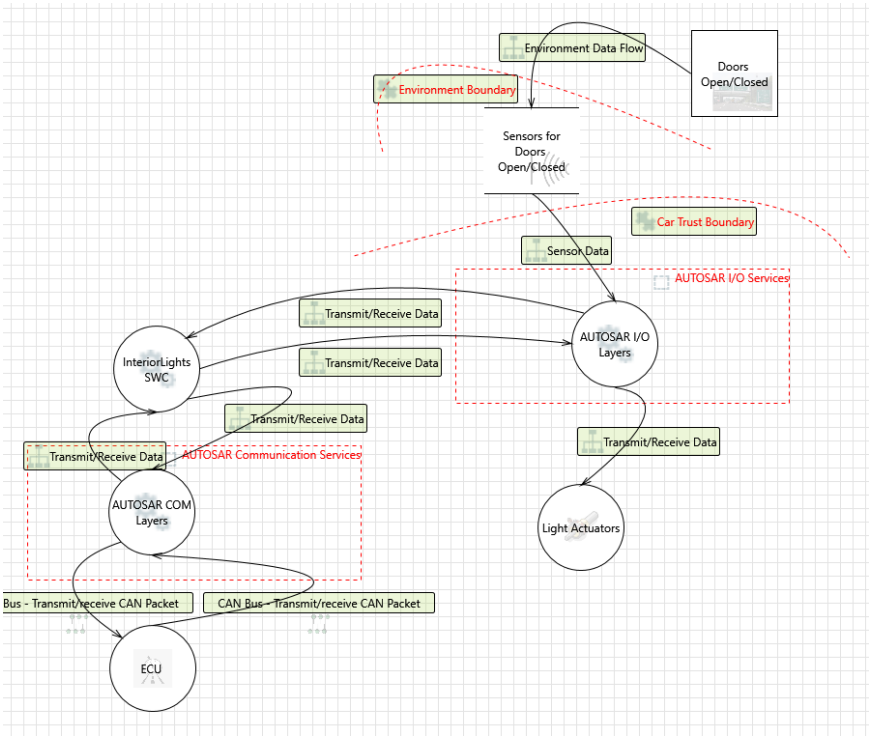

Fig. 4. DFD created with the MS Threat modeling tool and the NCC Group template

[3] The entire DFD diagram is not included as most threats would be found on trust boundaries and interfaces to external actors.

5 Results

5.1 TARA

Results of the TARA method are reflected in the three libraries that were created during the threat modeling process and the risk comparison shown in Figure 5. It is especially important to analyse the CEL library as it contains a list of the most exposed areas and the graph as it identifies the threat agents that pose the greatest risk. The CEL library identified the OBD port as the interface that is exposed the most followed by the Wi-Fi connection on the second place. The rest of the exposed areas are then listed in descending order.

Figure 5 is based on the survey results and the support of domain experts. It shows risk levels for each threat agent when the connected car is taken as the target. The *Default risk*, as stated in the figure, represents the general risk to different IT services while the *Project risk* represents the connected car. The method identified six threat agents that have an elevated risk level, where the *Sensationalist* was identified as the one posing the greatest risk. This threat agent refers to people who wish to attract public attention by employing any method for notoriety just to get their "15 minutes of fame."

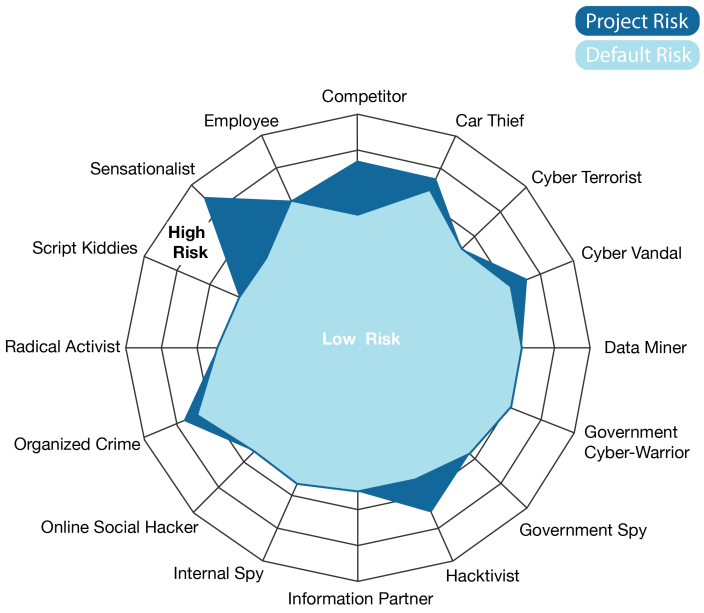

Fig. 5. Risk comparison of different threat agent profiles

5.2 STRIDE

After the MS Threat modeling tool analysed the DFD diagram for the *Interior light application*, it generated a threat report with 74 different potential threats, where at least one threat from each STRIDE category was found. It also found 17 threats that were not applicable to the application.

To ensure that the results of the threat modeling process are credible and should be further analyzed by experts, we verified the found threats with an actual hardware implementation of the application. Testing was performed on an AUTOSAR hardware board (with the *Interior light application*) connected to a small CAN network and a computer to analyze the communication and the exchanged packets (Figure 6). By conducting this validation process we could investigate whether the threats generated by the threat modeling tool are applicable to the actual AUTOSAR software application, and as such, to a real vehicle system.

The validation process was conducted successfully and the threats discovered by the threat modeling process were confirmed. Hence, the adapted STRIDE method can be applied to other systems in the automotive domain and as such become a valuable tool for automotive security experts.

6 Related Work

Very little research has been found regarding threat modeling of the connected car. Two of the first papers that discuss security analysis of modern vehicles were published in 2010 and 2011 by researchers Koscher *et al.* [17] and Checkoway *et al.* [18]. They

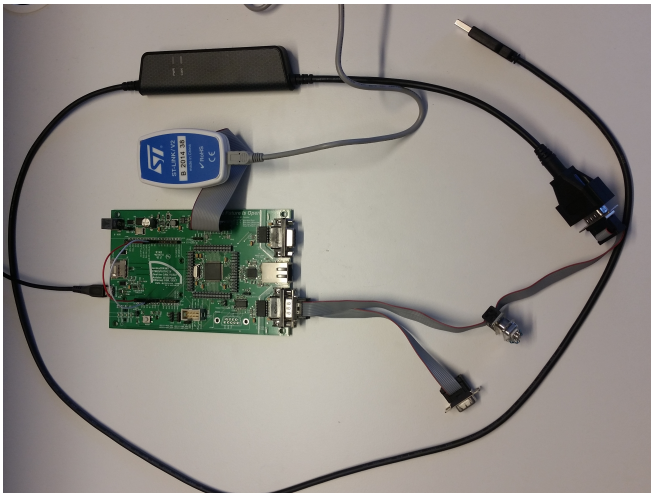

Fig. 6. Equipment used to simulate a vehicle environment running the *Interior light application*

conducted a series of experiments and road tests on a modern vehicle, and among other things found that it was possible to manipulate the vehicle by injecting false messages on the CAN network. They also analysed the external attack surface of the vehicle and managed to exploit some of the connection points i.e. bluetooth function and the vehicle's cellular connection used for the telematics system. However, the team that conducted the research did not use any specific methods for analyzing the vehicle's attack surface.

The work by Wolf and Scheibel [19] from 2012, was one of the first that gave a new risk analysis method tailored to the needs of the automotive industry. Their 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 decreases costs. Furthermore, in 2014 the U.S. National Highway Traffic Safety Administration (NHTSA) [20] presents a composite modeling approach of cyber security threats to the connected vehicles. They created threat models and threat reports of different types of possible threats to vehicles along with a list of potential attacks.

Threat analysis methods have also been presented by the following authors. The first, by Mundhenk *et al.* [21], presents a new method for security analysis. This method uses Continuous-Time Markov Chains (CTMC) to model the architecture at the system level. Afterwords, the model is analyzed for confidentiality, integrity, and availability by using probabilistic model checking. Another approach to combine safety and security risk analysis was proposed by Machera *et al.* [22]. 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 most recent paper, by Islam *et al.* [23], gives some more information about the process of risk assessment for the automotive embedded systems. 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.

The described papers introduced some new threat modeling methods, however the application of the TARA method and the usage of MS Threat modeling tool with the NCC Group template has not been done before. This paper tries to fill this gap and present these methods and tools to the automotive industry.

7 Discussion and Future Work

The TARA method is rather new with little supporting documentation except what is published by Intel Security [7]. For that reason, additional work had to be conducted in order to successfully adapt and apply the method to the automotive industry. The method ranked the *Sensationalist* and the *OBD port* as having the highest risk in their respective category. The former mirrors well the majority of the attacks that have been widely documented and discussed. These were conducted by different researchers and experts that wanted to show how insecure the vehicles really are. The final goal of the researchers was maybe not to get famous and hit the head-lines of all news portals in the world, but it was definitely the outcome of their research and as such has to be taken into 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[6]. It is also the oldest interface in the CEL library and accessing the OBD port gives the attacker almost full access to the CAN network.

Unlike the TARA method, STRIDE has been used before in the automotive industry. However, the method in this paper was conducted by using the MS Threat modeling tool along with the template designed for the automotive industry, and this was not done before to the best of our knowledge. The template used with the MS Threat modeling tool has shown to be very useful and adaptable, where further work may allow this template to be used on even more low-level software applications.

The results generated by the tool in this paper are maybe not completely comprehensive but they clearly show the extent of vulnerabilities of an AUTOSAR based software application. Even though the application in question, the vehicle's interior lights, does not seem like something worth analyzing, one can just imagine driving down the highway in the middle of the night when suddenly the lights in the car start going on/off every second - it could distract the driver or even cause an accident.

8 Conclusion

In this paper, we adapted two threat modeling methods from the computer industry in order to better fit the needs of the automotive industry. The next step was to apply these methods to the connected car and the underlying software architecture, which in turn generated valuable results that were carefully validated. The entire work was done with support of domain experts from different companies that have extensive knowledge in this field. TARA was used to provide a high-level overview of threats in the area of connected vehicles while STRIDE was used to evaluate a specific functionality of the vehicle.

The three libraries created by the TARA method and the template used by the STRIDE method would be a good starting point for any future application. The research described in this paper, including the actual validation of STRIDE results on real hardware, demonstrates the usefulness of these methods and domain experts should be able to include them in their tool set for future analysis.

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 with the introduction of V2X technology and the autonomous driving, 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.

References

[1] Currie R. and Santander M. "Developments in car hacking". In: *SANS Institute InfoSec Reading Room* (2015).

[2] Greenough J. "The Connected-Car Report: The Transformation of the Automobile". In: *Bussines Insider Intelligence* (2016).

[3] Miller C. and Valasek C. "Remote Exploitation of an Unaltered Passenger Vehicle". In: *Black Hat USA* (2015).

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

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

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

[7] 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/. 2009.

[8] OWASP. *Threat Risk Modeling*. https://www.owasp.org/. 2016.

[9] Vector Corp. *http://www.elearning.vector.com*. Accessed 2016-10-03. 2015.

[10] AUTOSAR. *Utilization of Crypto Services - AUTOSAR Release 4.2.2*. Accessed 2016-10-03. http://www.autosar.org/standards/classic-platform/release-42/.

[11] Adi Karahasanovic. *Automotive Cyber Security - Threat modeling of the AUTOSAR standard*. http://studentarbeten.chalmers.se/publication/247979-automotive-cyber-security. 2016.

[12] Casey T. "Threat Agent Library Helps Identify Information Security Risks". In: *White Paper Intel Information Technology* (2007).

[13] Houlding D., Casey T., and Rosenquist M. "Improving Health-care Risk Assessments to Maximize Security Budgets". In: *Intel White paper* (2012).

[14] ENISA. *Threat Landscape 2015*. https://www.enisa.europa.eu/publications/etl2015. 2015.

[15] Casey T. "A field guide to insider threat". In: *Intel White paper* (2015).

[16] NCC Group. *The Automotive Threat Modeling Template*. Accessed 2016-11-04. https://www.nccgroup.trust/uk/about-us/newsroom-and-events/blogs/2016 july/the-automotive-threat-modeling-template/.

[17] Koscher K., Czeskis A., Roesner F., Patel S., Kohno T., Checkoway S., et al. "Experimental Security Analysis of a Modern Automobile". In: *2010 IEEE Symposium on Security and Privacy* (2010).

[18] Checkoway S., McCoy D., Kantor B., Anderson D., Shacham H., and Savage S. "Comprehensive Experimental Analyses of Automotive Attack Surfaces". In: *SEC'11 Proceedings of the 20th USENIX conference on Security Pages 6-6* (2011).

[19] Wolf M. and Scheibel M. "A Systematic Approach to a Quantified Security Risk Analysis for Vehicular IT Systems". In: *Automotive – Safety and Security 2012 Conference, Karlsruhe* (2012).

[20] McCarthy C., Harnett K., and Carter A. *NHTSA - Characterization of Potential Security Threats in Modern Automobiles A Composite Modeling Approach*. https://trid.trb.org/view.aspx?id=1329315. 2014.

[21] Mundhenk P., Steinhorst S., Lukasiewycz M., Fahmy S.A., and Chakraborty S. "Security Analysis of Automotive Architectures using Probabilistic Model Checking". In: *DAC '15 Proceedings of the 52nd Annual Design Automation Conference* (2015).

[22] Machera G., Armengauda E., Brennerb E., and Kreinerb C. "Threat and Risk Assessment Methodologies in the Automotive Domain". In: *The 1st Workshop on Safety and Security Assurance for Critical Infrastructures Protection (S4CIP)* (2016).

[23] Islam M.M., Lautenbach A., Sandberg C, and Olovsson T. "A Risk Assessment Framework for Automotive Embedded Systems". In: *Proceedings of the 2nd ACM International Workshop on Cyber-Physical System Security* (2016).