CHALMERS
UNIVERSITY OF TECHNOLOGY

UNIVERSITY OF GOTHENBURG

Investigating the Use of Honeypots in Vehicles

Master's thesis in Computer Science and Engineering

Elin Eriksson & Lisa Fahlbeck

Department of Computer Science and Engineering
Chalmers University of Technology
University of Gothenburg
Gothenburg, Sweden 2022

Master's thesis 2022

Investigating the Use of Honeypots in Vehicles

Elin Eriksson
Lisa Fahlbeck

UNIVERSITY OF GOTHENBURG

CHALMERS
UNIVERSITY OF TECHNOLOGY

Department of Computer Science and Engineering
Chalmers University of Technology
University of Gothenburg
Gothenburg, Sweden 2022

Investigating the Use of Honeypots in Vehicles
Elin Eriksson & Lisa Fahlbeck

Supervisor: Tomas Olovsson, Department of Computer Science and Engineering
Advisors: Christian Sandberg and Afshin Soltani Esterabadi, Volvo Group Trucks Technology
Examiner: Magnus Almgren, Department of Computer Science and Engineering

Master's Thesis 2022
Department of Computer Science and Engineering
Chalmers University of Technology and University of Gothenburg
SE-412 96 Gothenburg
Telephone +46 31 772 1000

Gothenburg, Sweden 2022

Abstract

Vehicles today are increasingly connected through services such as 4G/5G, Bluetooth, and smartphone tethering. These external interfaces can become attack surfaces and can be used as entry points into the central vehicle architecture to gain unauthorized access to safety-critical features. This increase in connectivity correlates to an increase in cybersecurity threat levels and corresponding cybersecurity protection measures need to be taken. One possible protection mechanism is the use of a honeypot placed in the vehicle architecture. A honeypot is a tool used in cybersecurity that can be used to gain information about potential adversaries and attacks, similar to intrusion detection systems.

To date and to the best of our knowledge, there has been no published research about honeypots placed within the vehicle architecture. Therefore, this study was performed to try and fill that gap and potentially inspire further research. This study has aimed to conduct a thorough theoretical investigation into vehicle honeypots and present recommendations about how they best can be implemented in a connected vehicle architecture. This has been done through a combination of literature studies and interviews with candidates from the automotive industry. The interviews played an integral part in connecting research about honeypots in other domains to the automotive industry. They were used to gain information about the current cybersecurity threat landscape towards vehicles, approaches towards cybersecurity protection measures in the industry, and a wide range of ideas and opinions about using specifically honeypots in vehicles. On some questions the answers were unanimous, but on other questions a wide range of answers was given, indicating that there is no consensus yet within the industry on the best way to implement honeypots in vehicles.

The results of this study are a proposed set of requirements for a functional vehicle honeypot, a series of aspects to consider before implementing a vehicle honeypot, and a series of aspects to consider in the design of a vehicle honeypot. The results cover, among other topics, the risks and challenges vehicle honeypots can potentially pose, and possible implementation details like placement in vehicle architecture. Lastly, we make detailed recommendations on what we think are the most suitable honeypot implementations to begin with in the current vehicle cybersecurity landscape, specifically tailored towards commercial vehicles.

Keywords: Honeypot, Vehicle, Cybersecurity, Connectivity, Automotive, Truck, UNECE R155, ISO/SAE 21434

Acknowledgements

First and foremost we would like to thank our supervisors Christian Sandberg and Afshin Soltani Esterabadi for all their help, guidance, and feedback during this thesis. Thank you for always being receptive to our questions, for entertaining and engaging discussions, and for providing us with key contacts, documents, and papers. We would also like to thank the entire department of Cybersecurity at Volvo Trucks and especially Sofia Skoglund for welcoming us warmly.

We would also like to thank everyone who participated in our interviews and gave us their time and expertise. A grateful thank you to Johannes Weschke, Nasser Nowdehi, Thomas Rosenstatter, Christian Sandberg, Niklas Wiberg, Lourie Fouche, Mathias Widman, Urban Thorsson, Andreas Bokesand, Afshin Soltani Esterabadi, Arefeh Golshan and Jean-Baptiste Serrou Soares.

Finally, we would like to thank Tomas Olovsson for being our academic supervisor and Magnus Almgren for being our examiner, and for the feedback we have received throughout this thesis project.

Elin Eriksson, Gothenburg, August 2022
Lisa Fahlbeck, Gothenburg, August 2022

Contents

List of Acronyms

APN	Access Point Name 30
ASAM	Association for Standardisation of Automatic and Measuring Systems 22
CAN	Controller Area Network 11, 12, 21, 31
CPS	Cyber-Physical Systems 4
CSMS	Cybersecurity Management System 2, 12, 13
CyReV	Cyber Resilience in Vehicles 7, 11, 24, 29, 34
ECU	Electronic Control Unit 11, 12, 22, 31
IDS	Intrusion Detection System 2, 3, 9, 11, 19, 23, 25, 28, 29, 34, 38
IIoT	Industrial Internet of Things 4, 6
IoT	Internet of Things 4, 6
IP	Internet Protocol 1, 21, 30
IPS	Intrusion Prevention System 9, 29, 38
ISO	International Organization for Standardization 12
ISO 14229	International standard for diagnostic services in road vehicles 22
ISO/SAE 21434	International standard for cybersecurity risk management in road vehicles 2, 12, 37
LIN	Local Interconnect Network 11
OBD	Onboard Diagnostics 1, 14
OEM	Original Equipment Manufacturer 2, 14, 15, 23, 28, 30, 39
OS	Operating System 21, 25
SIEM	Security Information and Event Management 21

SOA	Service Oriented Architecture 21
SOC	Security Operations Center 24, 30
SSH	Secure Shell 21
SSID	Service Set Identifier 21
TA	Threat Agent 15, 16
TARA	Threat Analysis and Risk Assessment 12, 13, 27
TCP	Transmission Control Protocol 21, 24
TGU	Telematic Gateway Unit 1, 21, 29
UDS	Unified Diagnostics Service 21, 22
UNECE R155	United Nations Regulation No. 155 for cybersecurity and cybersecurity management systems of wheeled vehicles 2, 12, 33, 37
V2X	Vehicle-to-Everything 1
VANET	Vehicular Ad-Hoc Network 3
VSOC	Vehicle Security Operations Center 24, 30
XCP	Universal Measurement and Calibration Protocol 21, 22

1 Introduction

In the current digitized world, the likelihood of cyber attacks on vehicles is ever-increasing due to the implementation of various connected services [1]. Examples of these are long-range services such as 4G/5G for V2X (Vehicle-to-Everything) communication and short-range services such as Bluetooth and smartphone tethering for the use of third-party services like playing music. In the connected vehicle ecosystem, most things are interconnected. This means that these external interfaces can become attack surfaces that can be used as entry points into the central vehicle architecture to reach safety critical features and/or gain unauthorized control of the vehicle [2]. This increase in attack surfaces correlates to an escalation of threats and risks of cybersecurity breaches if secure solutions are not actively designed and implemented.

A security breach in a vehicle can have severe consequences. It can potentially impact an entire organization and result in unauthorized access to customer data, loss of reputation, theft of intellectual property, and downtime [3]. However, it can potentially also lead to even more serious consequences such as vehicle failure and bodily harm to drivers, passengers, and other road users. Due to this, the stakes are high when it comes to automotive cybersecurity.

There have been several notable and widely publicized automotive hacks that have illustrated the potential consequences that could follow from similar attacks. Over time, the attackers have needed less and less physical access to the vehicles, but the severity of the breaches has stayed critical. One of the first published hacks of a car was carried out in 2009 [4]. In this hack, a group of scientists connected a laptop to the car's OBD (Onboard Diagnostics) port and gained access to the internal network to the extent that they could manipulate safety-critical systems in the car. A year later a former employee of a car rental company managed to gain unauthorized access to the company's systems even after being fired and managed to remotely disable more than 100 cars at once [5]. However, the most famous and still relevant hack happened in 2015, when two individuals managed to take control of a Jeep completely remotely through the car's cellular network connection [6]. All they needed was the car's IP-address to gain unauthorized access to the car's transmission, brakes, and steering wheel. Just one year after that, it was discovered that some TGUs (Telematic Gateway Units), often present in commercial vehicles like trucks, buses, and ambulances, were also shown to be vulnerable to fully remote exploits [7].

All the examples of hacks above were carried out by researchers or white-hat/ethical hackers with the intent of highlighting vulnerabilities in order to strengthen the cybersecurity protection measures within the industry. The danger, however, lies in not knowing what adversaries with malicious intent and black-hat actors are capable of. In 2021, black-hat actors were reported to have outnumbered white-hat actors, representing almost 57% of all reported incidents of vehicle attacks [3].

Despite the increasing number of connected services in vehicles bringing an increase in potential entry points and possible cyberattacks, most OEMs (Original Equipment Manufacturers) and companies have managed to counterbalance these threats with sufficient cybersecurity measures. We have not yet seen any catastrophic examples of vehicle cyber attacks. However, up until now the cybersecurity measures of vehicles have been up to each OEM themselves and not centrally regulated or required. Each OEM has had its own responsibility and likely managed it differently. Now, however, the United Nations have introduced the first regulation, UNECE R155 [8], UN regulation No. 155 to standardize automotive cybersecurity and cybersecurity management systems [3]. In addition to this regulation, a new standard for cybersecurity risk management of road vehicles, the ISO/SAE 21434 [9] has also recently been introduced. As the first phase of the UN regulation No. 155 comes into effect in 2022, the type approval of future vehicles will only be granted once a certified CSMS (Cybersecurity Management System) has been put in place. This represents a paradigm shift in the industry and has put cybersecurity front and center.

As previously mentioned, it is however not clear what black-hat actors and other attackers are currently capable of, or how often vehicles are indeed being exposed to remote cyber attacks. In addition to developing a CSMS and looking at increased implementations of IDSs (Intrusion Detection Systems), there is interest in potentially using honeypots in vehicles to gain additional intelligence about the current cyber threat landscape and existing threat agents. Honeypots in the next-generation intelligent vehicle architecture could act as supplementary decoy systems collecting information about the way attackers operate and approach the vehicle networks. This could help in gathering information about intruders and their actions, which in turn can help in identifying network vulnerabilities and action can be taken to fill these gaps.

A honeypot is a tool used in cybersecurity to gain information about potential adversaries and attacks. The honeypot as a component does not add any actual functionality to the system and it does not generate much traffic on its own [10]. This makes it a useful tool as almost all traffic on the honeypot is data obtained clear of any legitimate traffic on the network. The data analysis is therefore much simpler as there is a very low possibility of false positives and essentially all data obtained will be from malicious parties. The collected information can then be studied to gain information about new attacks or approaches by attackers. Honeypots do not prevent attacks, instead, they provide data and information about potential attacks and can help highlight possible vulnerabilities in the network [11]. However, more

interactive honeypots can become a vulnerability in themselves, as attackers can possibly discover how to use the honeypot to launch other attacks in the network or test the system in other ways, without the owner's knowledge. Additionally, if attackers identify the honeypot they can avoid it, leaving its potential advantages inconsequential. Adversaries could also possibly manipulate and tamper with the honeypot to mislead the owners with the information gathered by it. These negative effects however can be eliminated to a large extent by careful implementation and design.

To identify secure and efficient implementations and designs for honeypots in vehicles this master thesis presents a comprehensive investigation into this subject. As far as we know, this is an area of research that has not been studied before. One focus of this study has therefore been to lay the groundwork for future research into this area by surveying all information and opinions available to date that we could identify. This means the scope of this study has been rather broad. We have therefore also presented specific recommendations for honeypot designs created from a subset of the results that we believe are most favorable for the industry at this point in time.

1.1 Related Work

Honeypots in connection to vehicles is a rather uncharted research area. To our knowledge, there is no previous research into honeypots placed in the actual vehicle architecture, as is the focus of this study. Much of the literature reviewed for this project has therefore either been about honeypots used in other domains or about other aspects of vehicle cybersecurity.

The earliest paper found about honeypots in relation to vehicles was published by Verendel et al. in 2008 [12]. They propose a honeypot simulating an in-vehicle network on a computer that in turn is driven around by a real vehicle. Another paper written in 2021 by Panda et al. presents an approach to making decisions when implementing honeypots in vehicle networks [13]. The authors deemed their solution HoneyCar a successful tool to determine optimal configurations for honeypots. However, neither of these papers cover honeypots placed in vehicles, as is the focus of our study.

A neighboring area of research where there have been a few more papers published is the use of honeypots in VANETs (Vehicular Ad-Hoc Networks). In [14] Sharma et al. present an overview of IDSs for VANETs as well as a proposed solution for a honeypot based IDS. Honeypot solutions in VANETs are also explored by Patel et al. in [15] and in the book Future Information Technology from 2014 [16]. However, similarly to the earlier mentioned papers, these papers only discuss honeypots in the context of the VANET and have therefore only been moderately relevant to this study.

A number of sources about honeypots in other domains proved useful for this thesis. One example is [17], the book Honeypots: A New Paradigm to Information

Security by Joshi and Sardana, which gives a comprehensive overview of the history of honeypots and honeynets, their range of applications, and examples of different classifications. In [18], Franco et al. present a survey of honeypots for Internet of Things, Industrial Internet of Things and Cyber-Physical Systems, which we identified shared similarities to honeypots in automotive applications. Another paper that was very useful was [11] by Zobal et al., which presents a comprehensive taxonomy of honeypots and examples of previously developed and/or deployed honeypots, as well as an overview of advantages and challenges in using honeypots.

1.2 Aim

This thesis aims to present well-substantiated conclusions and recommendations about possible ways to implement honeypots in vehicles. The main task is to investigate how one can integrate different honeypot designs to secure in-vehicle networks securely and efficiently. This was done by investigating aspects like the advantages and challenges of using honeypots as a security mechanism in vehicles. The findings include an overview of aspects to consider such as placement in the vehicle architecture, level of interaction, and possible contents of a vehicle honeypot. Recommendations about the specific implementations that we have identified as the most beneficial in the current vehicle cybersecurity landscape will also be presented.

1.3 Thesis Outline

This thesis is structured as follows. In Chapter 1 we introduce the problem and put in it a context. We also present related literature as well as the aim of the thesis. In Chapter 2 we explain the methodology and approach used. In Chapter 3 we present a theoretical background to honeypots and vehicle cybersecurity relevant for this study. In Chapter 4 we present our results which is followed by Chapter 5 containing our recommendations for future implementations of honeypots. In Chapter 6 we follow that up with a discussion, and in Chapter 7 we conclude the paper and suggest future work within the subject area.

2 Method

Our approach was a thorough literature study in combination with the conducting of interviews with people from the industry, described in more detail below. Initially, the scope of the project was very broad, but after beginning our research with an initial literature overview and having held the first few interviews, we managed to narrow the scope of the project slightly to a more focused and manageable size. We chose to mainly focus on remote attacks as opposed to attacks needing physical access to the vehicle as that seemed to be the area that has been least studied and was of most interest to the automotive industry. We also chose to mainly focus on software solutions as opposed to solutions requiring separate hardware, as the process of introducing additional hardware components is longer and more complicated when aspects like cost and inventory are taken into consideration. We did not however completely disregard hardware and we came to discuss it in some of the interviews.

As our research area contains very limited previous research, we chose to conduct our project as a combination of an explorative and normative study. An explorative study is most suitable when there is as of yet limited knowledge within a research area and the aim is to gain a fundamental understanding of it. A normative study is most suitable when there is some knowledge within the research area and the goal is to provide recommendations and suggest measures [19]. The existing research within specifically vehicle honeypots is, as previously mentioned, very limited. But the adjacent, more general research areas of honeypots and vehicle cybersecurity respectively have larger bodies of research behind them. As we aimed to present an overview of the existing research as well as conclusions and recommendations on ways to implement honeypots in vehicles, we concluded that this combination approach was most suitable. Additionally, we have taken an analytical approach in this study in that we have aimed to be as objective as possible in our research by for example interviewing candidates from several different companies within the automotive industry.

2.1 Literature Review

To define the problem in more detail, we started by doing a broad literature overview. This initial literature overview study was done to explain the current state of knowledge within our wider research area, as is the norm at the beginning of a research process [20]. In the initial literature overview, we attempted to gain a foundational

understanding of the research area. We read up on the existing research within vehicle honeypots as well as honeypots in other domains and other aspects of vehicle cybersecurity. We rather quickly realized the amount of research within vehicle honeypots was very limited but built a foundation of knowledge within the other areas.

We attempted to follow our initial overview with a systematic literature review with instructions that could be repeated further on to see the evolution of research within this area. However, the research was so limited that this approach was not useful or practical. We instead conducted a broader literature review by for example looking into the sources and the citations of the papers we had already collected. We also looked into papers about honeypots used outside the automotive domain that used specific services or vulnerabilities that we had identified as interesting, for example, Bluetooth. Some papers about honeypots developed for IoT (Internet of Things) or IIoT (Industrial Internet of Things) were also found to contain relevant information.

2.2 Interviews

To understand the current level of knowledge within the research area we held interviews with several people within the automotive industry. We conducted the interviews to gain further insight into the range of opinions and ideas regarding honeypots in vehicles that different people have depending on their background and current work. The information and questions we sent in our interview requests is available in Appendix A. We chose to conduct these as informal semi-structured interviews as we had a set of questions we wanted input on, but we also did not want to be too rigid in our questioning and miss the opportunity to ask follow-up questions or discuss specific points [21]. This gave us the freedom to be able to follow up on interesting points, tailor the wording of some questions according to the interviewees' experience and knowledge, and not have to necessarily read questions that the interviewee had already included the answer to in a previous question. Additionally, we chose to take written notes instead of recording the interviews, as this let interviewees answer and discuss more freely and openly.

The interview candidates were chosen to try and get a broad picture of opinions from people with a connection to cybersecurity within the automotive industry. We attempted to get as broad a selection of candidates as possible but were naturally hindered by the connections we could make during the period of this study, as well as some non-replies and people who simply did not have the time. All candidates we contacted had some knowledge of or connection to cybersecurity but differed in years of experience, and previous and current roles. In the end, we interviewed 12 candidates, and an overview is given in Table 2.1 below.

A number of the interview candidates were from the department of cybersecurity at Volvo Group Trucks Technology, as that is where this thesis was carried out. The department has several candidates with very different backgrounds and areas of expertise, all with a great insight into cybersecurity in vehicles. To broaden our

selection, we then contacted people from several other departments at the Volvo Group that work closely with the services and systems we were most interested in. This included the departments for Pentesting, Vehicle Connectivity, and Connected Solutions, where the last two both have insight into the communication between vehicles and the back office in different ways. We then expanded our selection of candidates outside of the Volvo Group. Some of these candidates were identified and chosen through their connection to the CyReV project (Cyber Resilience in Vehicles) as this thesis idea was born out of a proposed idea within CyReV. CyReV is an ongoing research project conducted by the Volvo Group, Volvo Cars, Combitech, Assured, RISE (Research Institutes of Sweden), and Chalmers University of Technology [22]. Out of these, we secured interviews with candidates from Volvo Cars and RISE. We also found a candidate from Scania through the larger research project of AutoSec [23].

Number of Candidates	**Department and/or Company**
6	Cybersecurity, Volvo Group Trucks Technology
1	Pentesting, Volvo Group Trucks Technology
1	Vehicle Connectivity, Volvo Group
1	Connected Solutions, Volvo Group
1	Volvo Cars
1	RISE
1	Scania

Table 2.1: Interview candidates

3 Literature Overview

This chapter presents some fundamental background knowledge within the research area. It covers intrusion detection and prevention systems and how they compare to honeypots, as well as gives a deeper explanation and classification of different honeypots. It also covers some basic vehicle architecture and an overview of the current cybersecurity threat landscape.

3.1 Intrusion Detection Systems

An Intrusion Detection System, shortened IDS, is a mechanism designed to detect malicious traffic on a network, either by looking for anomalies or by looking at predefined patterns in the payload or the traffic flow [24]. IDSs are a useful tool to increase cybersecurity in many networks, including vehicle networks. They can be placed in many different parts of the system and can be implemented in a variety of ways. Intrusion Prevention Systems, shortened IPS, are similar to IDS, but usually have additional functionality to not only detect anomalies or malicious activity but also to take action to prevent it. In the rest of this paper, we will primarily use the term IDS. It may sometimes be used as an umbrella term referring to both IDS and IPS.

Honeypots are sometimes categorized as a kind of IDS as it is also a tool to increase the security of a system or network by monitoring unwanted traffic. Compared to honeypots, IDSs are to date to a higher degree being both researched and implemented in vehicle networks, even if it also is a rather new field [25].

Honeypots however have some distinct features in comparison to other IDSs, the main one being the low or nonexistent rate of false positives. This is because honeypots are uniquely designed as an independent part of the system, and do not have much regular traffic to and from it. This means that most traffic logged on a honeypot can be assumed to be malicious (or an indication of a poorly designed honeypot). This differs from most other IDSs, as they are most often integrated into existing software with the task of analyzing or blocking parts of the existing traffic on the network [24]. This difference in types of interaction and the kind of information that can be collected by a honeypot makes them an interesting research subject in itself, but especially as a complement to other IDSs.

3.2 Honeypots

Honeypots are used to strengthen the cybersecurity of a system by providing a way to study and analyze the attacks they are exposed to. Honeypots were introduced in the 1990s and one of the first definitions of a honeypot in literature was written by Lance Spitzner in the early 2000s. That definition defines honeypots as a *security resource whose value lies in being probed, attacked, or compromised* [26]. This definition is still used today but is nevertheless quite vague in its categorization of what a honeypot is and can look like.

3.2.1 Taxonomy

Honeypots can be categorized into different types depending on their design and usage. A number of papers, such as [27], [18] and [17] have aimed to present a common taxonomy or categorization of honeypots. Some of the more universal and relevant classifications and types will be discussed in this section.

One of the most widely used categorizations for honeypots is the distinction between low interaction and high interaction honeypots [11] [18] [27] [17]. A low interaction honeypot, like the name implies, provides the hacker with little to no possibility to interact with it. It is beneficial in that it is easy to set up, easy to maintain, and has a lower risk of adding additional vulnerabilities to the system. It does however provide less information or data about the attacks it is exposed to. The main information gained from a low interaction honeypot is the existence and quantity of attempted attacks. A high interaction honeypot is more complex and more demanding to maintain and can become a vulnerability in itself as it often provides the attacker with an operating system and can expose parts of the network. However, compared to a low interaction honeypot it provides more useful data and information about the attempted attacks and possibly the attackers themselves. A honeypot can also have a medium level of interaction, or be a hybrid of low and high interaction [18] [27]. This is a way of trying to obtain the benefits from both the low and the high interaction honeypots. The choice between a high-interaction and a low-interaction honeypot is a trade-off between the complexity of implementation and management, and thereby also cost, risk of adding vulnerability, and the benefits of more useful information obtained by the honeypot.

Honeypots can also be categorized either as research or production honeypots, based on their usage or main purpose [11] [17] [18]. A research honeypot is used to gather information and data about new threats and attacks so these can be studied and researched and new prevention methods can be added to the system. Therefore, they are usually implemented in a way to gain as much information as possible from the attacker by being more interactive. The main purpose of production honeypots is instead to prevent attacks on an organization, either by misleading the attacker or by alerting the system or the organization when an attack occurs. This usually implies that a production honeypot is less interactive than a research honeypot, however, their distinction is more based on usage than on design.

3.2.2 Honeynets

Honeynets can be seen as an extension of honeypots and were introduced some years after the idea of honeypots. A honeynet is more complex than a single honeypot usually is. Even if honeynets have gained popularity and usage over the last years their definition is still somewhat unclear [27]. They can be defined as either a high interaction honeypot [17], or as two or more honeypots on a network [18]. Their purpose is the same as for a honeypot and the added complexity allows it to capture data to a greater extent. A honeynet can contain a combination of high and low-interaction honeypots. In general, however, it is the higher interactivity that provides an opportunity for more information collection.

A well-implemented and well-managed honeynet can provide a considerable amount of security to a system, mainly in terms of threat intelligence. A honeynet can also be used as a way to mislead attackers and keep them away from the real network. As for a single honeypot, the potential benefit of increased security comes at the cost of added system complexity, financial cost, and increased vulnerability.

3.3 Vehicle Cybersecurity

The other theme of this study is vehicle cybersecurity. In this section, a brief introduction to the unique challenges and aspects of working in a vehicle architecture is given, as well as an explanation of the regulations about to be introduced regarding automotive cybersecurity.

3.3.1 Basic Vehicle Architecture

The vehicle architecture considered in this study is the public reference architecture published by the CyReV project (Cyber Resilience in Vehicles), illustrated in Figures 3.1 and 3.2 [28]. The aim of the CyReV project is as the name suggests for vehicles to be resilient to cyber attacks and adaptable in terms of what kind of protection measures need to be included. The architecture proposed by CyReV is segmented into four different security zones divided by security borders, as illustrated in Figure 3.2. Different components in the system are placed in the zones *untrusted zone*, *exposed zone*, *protected zone*, and *critical zone* depending on their need for protection. For example, the infotainment system is placed in the exposed zone and the ECU (Electronic Control Unit) controlling the breaks is placed in the critical zone [28]. All off-board communication is done through the untrusted zone and the safety-critical components are placed in the critical zone. This is visualized further in the context of the vehicle architecture in Figure 3.1.

The security of ECUs, both hardware and software modules, and bus systems like CAN (Controller Area Network), LIN (Local Interconnect Network), Ethernet, etc. are the most significant branches of in-vehicle security. These systems pose different challenges compared to more traditional software or web systems where honeypots and IDSs are already common. CAN is a protocol widely used for in-vehicle networks

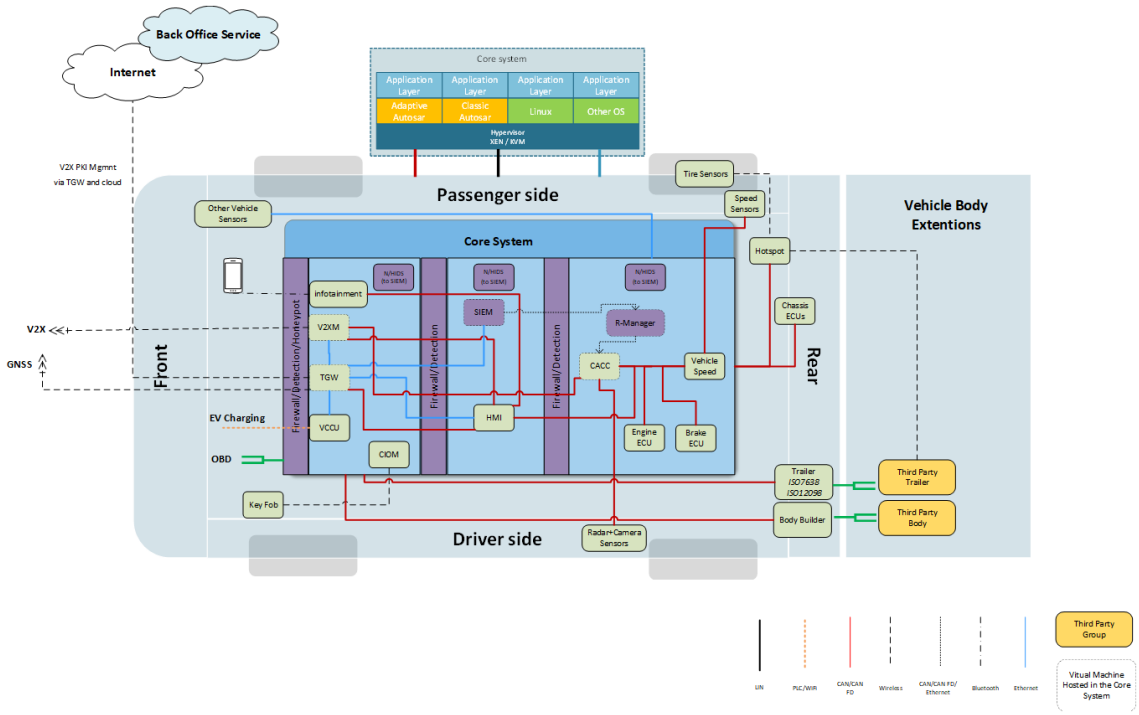

Figure 3.1: CyReV reference architecture overview [28], page 9.

due to its efficiency and reliability in transmitting messages between many different parts of the system. It does however have limitations, including the fact that the packets sent do not have space for any kind of authentication or integrity [29]. This becomes a vulnerability because by gaining access to a single ECU connected to the CAN bus, the whole network could be compromised through the sending of spoofed messages without any other nodes noticing.

3.3.2 Laws and Regulations

Cybersecurity is slowly becoming something that is not just good to have internally or to please customers, but something that is required. This is due to a wider understanding of cyber threats bringing more laws and regulations into play. The UNECE R155 [8] makes requirements of cybersecurity management systems for vehicles mandatory in phases starting in the summer of 2022 in the EU. UNECE R155 states that two core requirements need to be fulfilled for the type approval of a vehicle to be granted. The first is the operation of a certified CSMS (Cybersecurity Management System) and the second is the application of the CSMS to the specific vehicle in question [1] [8]. In addition to the UNECE R155, the International Organization for Standardization has introduced the standard ISO/SAE 21434 [9]. This is an international standard for cybersecurity risk management in road vehicles, which similarly puts the focus on having processes throughout the vehicle lifecycle to protect them from cyber attacks [1] [9].

A CSMS is supposed to provide comprehensive and holistic cybersecurity solutions [8]. That includes among others the use of TARA (Threat Analysis and Risk

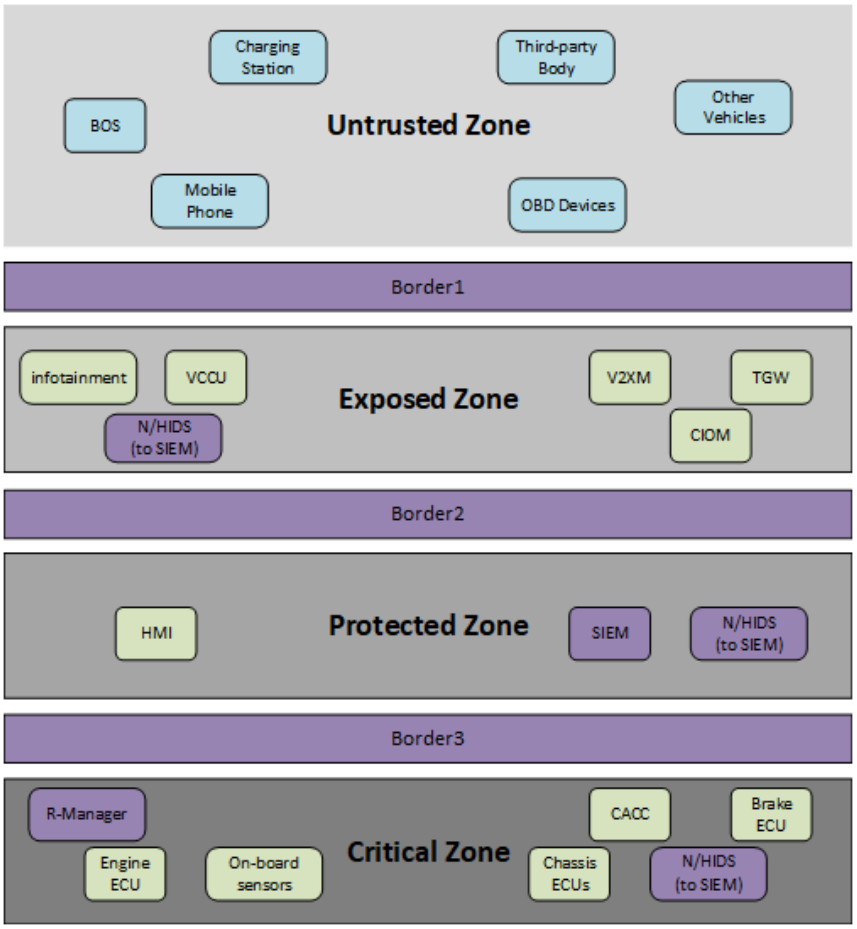

Figure 3.2: CyReV reference architecture showing the proposed security zones [28], page 14.

Assessment), which is a method to identify and assess vulnerabilities and risks to a system. It is a way to consider the plausibility and severity of different security risks and scenarios. TARAs are applicable to all parts of a vehicle and have to be performed on all changes and new implementations.

The demands for the CSMS apply to the whole life cycle of the vehicle, which means that the vehicle must be resilient to cyber threats as long as it is in use. This implies that the cybersecurity of the vehicle must be updated to follow the changes in the threat landscape, which can be aided by the use of a honeypot providing information about new attack patterns and approaches by attackers [8] [1].

3.4 Current Threat Landscape

A comment we have come across several times throughout this study is that within some areas, the industry feels relatively blind to the level of threats to connected vehicles that are out there [2]. The fundamental security and protection mechanisms present in vehicles at this point are not enough to gather information about the comprehensive threat landscape. This is the main motivation for looking at

components like honeypots for additional intelligence gathering.

To be able to make valid decisions about the implementation and placement of a honeypot it is important to know about the current threats facing commercial and connected vehicles. While studies about cyber threats facing vehicles have been conducted, it is still rather unclear who the main threat agents against vehicles in general, and commercial vehicles in particular, are [3] [2]. This is partly due to a lack of research, both from academia and the automotive industry [30]. It can also be due to the lack of detection mechanisms in vehicle networks which further emphasizes the use of honeypots in vehicles. Additionally, the range of threat agents against vehicles is rather broad. They range from the owner and/or driver wanting to slightly tweak or improve functionality of a particular vehicle, all the way to terrorist organizations with the intent of immobilize as many vehicles as possible at once.

3.4.1 Consequences

The consequences of cybersecurity breaches naturally vary in severity [3]. They can be anything from slight damage to a company's reputation to bodily harm or even the death of drivers, passengers, or other road users. This means that protection measures have to be prioritized accordingly.

The most severe consequences are related to safety. The most important priority in protection against cyberattacks is to make sure the systems stay safe and nobody gets hurt [3]. Safety refers to consequences such as bodily harm to either the driver of the vehicle or other road users surrounding the vehicle. These are naturally the most severe and the ones to avoid at any cost. These protection measures entail making sure that the hardest parts of the system to gain unauthorized access to are safety-critical features.

At the next level, there are operational consequences. These are disruptions to the function of the vehicle, affecting a company's ability to use the vehicle for its intended purpose. These can be a vehicle having downtime, standing still and not being in use, harm to or theft of the vehicle [3]. This primarily affects the productivity and uptime that a vehicle, company, or driver is capable of. These primarily lead to financial and possibly legal consequences. If they are widespread within the vehicles from a specific OEM they can also lead to reputational consequences and brand damage.

At the third level, less severe consequences can be found. These are things such as data leakage and other consequences that can lead to reputational or financial consequences [3]. This can be data obtained through unauthorized or incorrect use of the OBD port, third-party services in the infotainment unit, smartphone tethering, or the external communication channels on the vehicles. This data can be the intellectual property of many different types and the unauthorized leak of it could also be a compliance violation that could incur legal consequences. Examples

of data that can be leaked are GPS information, private driver information such as how she drives, or company-specific information such as routes and fleet handling.

3.4.2 Threat Agents

There are several threat agents, shortened TAs, that can reasonably pose a risk towards vehicles or OEMs [3]. There is however an important distinction to be made between white hat TAs and black hat TAs. White hat actors have no or limited malicious intent, whereas black hat actors do. In Table 3.1 several potential threat agents against vehicles are presented, separated into these two categorizations.

Potential Threat Agents	**Motivation**
Researchers Hobbyists Exploratory hackers Script kiddies	White hats or agents with no or limited malicious intent
Organized crime The owner/driver of the vehicle Thieves Political activists National agencies Terrorists	Black hats or agents with malicious intent

Table 3.1: Potential threat agents acting against vehicles

Researchers are considered TAs, and examples of these are the researchers behind the well-known automotive hacks presented in the introduction. They are however considered white hats and are valuable to the industry in that they can help identify vulnerabilities before black hats find them [2]. Other white hat actors are less experienced hackers that can sometimes be considered more curious than focused in their efforts but can still stumble upon vulnerabilities and cause issues, even if their intentions are not necessarily to cause harm.

Among black hat actors, there is also a wide selection. For someone not within the automotive industry, the owner and/or driver of the vehicle could be a surprising one. However, it is not uncommon for the owner of a fleet of vehicles to try and disguise certain information from competitors, or the driver of a particular vehicle to tamper with certain components in order to avoid having to take breaks, fill up with AdBlue for environmental purposes, and other cost-saving measures [3].

The black hat actors with the most malicious intent are terrorists, thieves, organized

crime, and potentially national agencies. These are the TAs that the industry knows the least about regarding their capabilities and what they potentially could carry out at any time. In 2021 it was reported that black hat actors now outnumber white hat actors, representing 57% of all reported incidents [3]. However, worth noting is that this is only in the reported incidents. Since cybersecurity is a sensitive subject it is possible that a portion of attacks is never reported, and that some are never even noticed. For this reason, among others, the industry needs to continue working towards being able to gain increasing threat intelligence and in turn be able to implement increased protection and prevention measures.

4 Results

This chapter presents the overall results of how to implement honeypots in vehicles, both from the existing literature and from the conducted interviews. In the following chapter, more detailed recommendations of our suggested implementations at this point are presented. As previously mentioned, very little research has been done within the area of vehicle honeypots, but it is nevertheless an area of interest within the industry moving forward. For this reason, a goal for this thesis was to hopefully lay the groundwork for future systematic implementations of honeypots in vehicle architecture.

This chapter begins with general requirements for designing vehicle honeypots, presented in section 4.1. In section 4.2 we propose aspects to consider before implementing a vehicle honeypot, for example, challenges that need to be taken into account before deciding to design and implement it. Following this, section 4.3 proposes aspects to consider in the designing of a vehicle honeypot. This section covers for example potential content/assets to include in the honeypot and how to handle data collection and logging of the registered traffic.

The results presented in this chapter are based on both literature and the conducted interviews. Detailed results from the interviews are presented in places where they bring up interesting points, for example, to show how there were some questions where the opinions of interviewees varied greatly and some where there was full consensus. The diverging answers and opinions to some of the questions can reasonably be traced back to the interviewees' different backgrounds. In other cases, opposing opinions and ideas are an indication of the fact that there is no consensus yet on the best way to implement honeypots in vehicles. This was very interesting to see and was what we hoped for when conducting the interviews. It is also worth mentioning that the interviews were relatively informal as the aim was more to gain insight, collect opinions and start discussions rather than to get final, definite answers.

4.1 Requirements for a Functional Honeypot

As the concept of a honeypot is still not clearly and consistently defined we have concluded some key requirements that we think should define a functional vehicle honeypot. The following four requirements are an attempt to facilitate the future development of honeypots by laying a foundation for how they can be designed and implemented. They have been formulated specifically for the case of placement in

vehicle architecture, but are also relatively general and could apply to honeypot implementations in several contexts.

4.1.1 Isolation

A honeypot must be isolated from critical parts of the system. For a honeypot to be functional and useful it must be secure enough to not become a risk for the system. It must be implemented in a way that an attacker can not use it to gain further access to the system or to launch attacks from it. If not, the risks of using a honeypot will exceed the advantages.

4.1.2 Allure

A honeypot must look interesting enough to be attacked. The point of a honeypot is for it to be probed or attacked, and if not it does not provide any value. It is therefore crucial that a honeypot attracts hackers in order to collect data that can be used for threat intelligence to further secure the system.

4.1.3 Logging

A honeypot must be able to log data from attacks effectively. As the collected data is analyzed and studied to further increase the security of the system, the data must be made accessible efficiently. This requires a plan for how and when data is logged.

4.1.4 Adaptation

A honeypot must be usable even after discovery. If a honeypot is discovered it can be bypassed and thereby lose its value or be exploited for malicious purposes. Therefore it is important that a honeypot can be disguised again in some way after discovery. This can also be done preemptively to try and avoid discovery. This can be done in numerous ways by changing some aspects of the honeypot.

4.2 Aspects to Consider Before Implementation

There are currently no known active vehicle honeypots that can be studied, and there is some hesitation within the automotive industry on whether they are too much of a risk to be useful. A goal of this study has therefore been to study whether or not honeypots are an appropriate security measure to implement in vehicles. This has been done by looking at the advantages, challenges, and risks of using honeypots in vehicles both from literature and interviews. Through this, we have concluded that honeypots in vehicles can be motivated as a valuable asset, as the advantages outweigh the challenges and the risks can be eliminated to a large extent by careful design and implementation.

4.2.1 Advantages

The main advantage of a honeypot in a vehicle is the ability to obtain threat intelligence. Threat intelligence consists of information about potential risks, attacks, vulnerabilities, and attack surfaces in the system. A honeypot can be useful in collecting information about whether an attacker has attempted or succeeded in accessing the system. It can also log things like how often attacks occur, at what parts of the system they are aimed, and how an attacker can enter.

Another advantage of using honeypots is the low rate of false positives compared to most other IDSs. This implies that the honeypot provides cleaner data that is easier to analyze.

Depending on the design of the honeypot it can also be used to mislead an attacker and in that way protect a system from actually being attacked. A honeypot that can trick the attacker to think she is accessing the real system can potentially keep her from doing so long enough for the attempted attack to be discovered. In this way, a honeypot can potentially also be a protection mechanism.

4.2.2 Challenges

There are a number of reasons that can make it challenging to implement honeypots for vehicle security. All new components to a system add complexity and take up resources, which can be a vulnerability in itself, especially in systems with real-time constraints such as vehicle networks.

Maintaining and handling the data from a honeypot can also pose a challenge. A honeypot can be discovered and rendered useless or can be exploited. It is therefore important that the honeypot is maintainable in such a way that it can be disguised again, or if necessary, decommissioned. Furthermore, the collected data needs to be analyzed and actions must be taken accordingly. Even if the collection of data is the reason for using a honeypot, handling it efficiently requires time and resources.

Another challenge is the fact that a honeypot can provide a false sense of security. A honeypot only provides data and information if it is being attacked or exploited. However, no recorded data on a honeypot does not mean the system is not being exploited, attackers could simply have bypassed the honeypot. A quiet honeypot is therefore no guarantee for a secure system, which is important to keep in mind.

4.2.3 Risks

Like several other questions, the answers on this topic differed significantly, from one interviewee thinking the biggest risk would be a waste of resources and another thinking it is too risky to ever put a honeypot in the in-vehicle network. A suggested alternative was instead a honeypot placed in a fully separate, external

hardware component such as a Raspberry Pi not connected to the in-vehicle network.

Most interviewees however talked about the risk of a poorly implemented honeypot becoming a vulnerability to the system, which is also what is mainly discussed in the literature. A commonly highlighted risk of an inadequate implementation is the honeypot being used as a gateway further into the network, particularly if the honeypot deliberately includes known vulnerabilities to attract attackers. Also mentioned was the risk of a faulty honeypot being used to launch attacks on the system. Both these risks are mostly the case in poorly implemented high-interactive honeypots that contain operating systems or other interactive components that a skilled attacker could find unintended vulnerabilities in.

Another risk with a poor honeypot design is that it could give away information about how the system looks or what parts of the system are particularly vulnerable. If the honeypot emulates the real system too well, adversaries could be able to gain too much information about how to approach the real system if/when they realize they are currently interacting with a honeypot. Honeypots emulating only parts of the system such as specific services could also inadvertently give an adversary information about what parts of the system the owner finds most worth protecting or most vulnerable.

A honeypot can also become a risk if it is not possible to update it. Another risk regarding this is if the honeypot can not be shut down. If the honeypot is exposed or discovered it is crucial that it is possible to update it or shut it down to avoid further damage.

Lastly, the risk of the honeypot collecting data that it should not also needs to be considered. This can include for example personal or identifying data. While not a safety risk, this can lead to reputational or financial consequences.

4.3 Aspects to Consider in the Design Stage

As there is no common practice for how to implement honeypots in vehicles, we have studied different aspects of how this can be done most advantageously. This chapter is predominantly based on interview data, with support found in the literature. These aspects to consider are investigated on a broad level and no design decisions are looked at in much detail. Instead, this section presents important factors that should be evaluated on a higher level when designing a honeypot.

4.3.1 Content of Honeypot

In Table 4.1 we present all assets/services identified by interviewees. This question regarded the content of the potential honeypot, either in the form of assets to include as bait or interesting services that could be emulated to tempt potential adversaries. The answers are presented in order of the number of mentions, that is, how many of the interviewees mentioned that answer, to illustrate how some answers were much

more common than others.

Identified Assets/Services	**Number of Mentions**
Port 80/web-server	5
Dummy SSH-server offering fake root access TCP-port Telnet UNIX, Linux or other interesting OS TGU (Telematic Gateway Unit)	3
Dummy infotainment system Fake vehicle on the network using a SSID or IP-address	2
Local NoSQL database containing mock data UDS server (Unified Diagnostics Service) Information containing fake symmetric or private keys Unused ID on the CAN, ex HEX25 Something related to the battery in electric vehicles Simply something with a known recent vulnerability XCP (Universal Measurement and Calibration Protocol) SOA-service (Service Oriented Architecture) Services that sound safety-critical (e.g. engage breaks) SIEM (Security Information and Event Management)	1

Table 4.1: Assets identified by interviewees as possible bait for honeypots

As can be seen in Table 4.1, some of the most common answers are related to TCP (Transmission Control Protocol) ports, which would place the honeypot quite close to the external interfaces. Many of these are well-known services or servers most attackers would reasonably check and try to exploit if they came across them. A web-server/port 80 was the most common suggestion, as this was seen as something most hackers would check for vulnerabilities or try to exploit. In a similar way, an exposed Telnet service was a popular suggestion, as was an emulated SSH-server. Telnet has known vulnerabilities that would most likely attract an attacker, and the possibility to exploit an SSH-server to gain root access was also seen as something very few attackers would ignore.

Some of the answers mentioned by only one person are however very interesting too. As not everyone interviewed had the same background this is where specific candidates' expertise was shown.

UDS (Unified Diagnostics Service) is a diagnostic communication protocol specified in the ISO 14229 standard that is used in ECUs within the automotive industry for diagnostic purposes [31]. When diagnostic tools are connected to the vehicle, UDS requests can be sent to all ECUs to read error codes, update firmware, or test specific outputs or services through low-level interaction. As ECUs are used to control almost all functions in modern vehicles, from cab lights to fuel injection and engine control, gaining access to them is a very appealing prospect. For this reason, diagnostic services are often among the first things automotive hackers try to scan, and then possibly try and exploit. Especially the ability to perform low-level interaction on ECUs, including for example brake systems, is a very attractive possibility.

XCP (Universal Measurement and Calibration Protocol) is a network protocol used for connecting calibration systems to ECUs. It is a standard defined by ASAM (Association for Standardisation of Automatic and Measuring Systems) to be a universal and bus-independent protocol [32]. What makes XCP interesting to a potential adversary is that it enables read and write access to memory content and variables of microcontroller systems at runtime. The protocol should generally be disabled after the production of a vehicle is concluded, but an attacker could be expected to check if that is the case or if the disabling step has been forgotten, as the profit of gaining access to it would be great.

An advantage of emulating a vehicle-specific service such as an UDS server or XCP in a honeypot, is that this can give an additional indication that the attackers are specifically knowledgeable of vehicle architecture, and not only common vulnerabilities such as Telnet.

4.3.2 Interaction Level

This question in the interviews asked if the interviewees thought the main purpose of a honeypot should be detection or research. A honeypot focused on detecting an attack and alerting once this occurs is often called a production honeypot, and a research honeypot aims to collect information about attempted attacks that can be studied further. The majority of the interviewees started by asking if they had to choose, emphasizing that both detecting and researching attacks are important. The follow-up to this question included a discussion on whether the honeypot should be low or high interaction as the distinction between these is similar to the distinction between research and production honeypots.

Most interviewees however also said that even though both are important, the best way to start would be to implement a low interaction honeypot focused on detecting if an attack occurs and not as much on collecting information about the attack or attacker. This can also be motivated by the fact that as of now, a lot is unknown

about remote attacks against vehicles and the most interesting information that can be gained is the frequency and the kind of remote attacks attempted. This information could then be used as motivation to deploy a more advanced honeypot further on, or additional IDSs.

4.3.3 Data Collection

In many of the interviews, the collection and handling of data were also discussed even though it was not one of the initial questions indicated in Appendix A. We wanted to find out how candidates envisioned the logging of the data collected by the honeypot should be handled. This included how often data should be transmitted, who should be responsible for it, and what happens to the data when it reaches the back office. Some of the candidates' expertise was within the communication between the vehicle (on-board) and back office (off-board). In those cases, the questions aimed to find out what was possible in terms of logging and sending data between the vehicle and the back office, and if there are any major challenges or restrictions regarding this.

It is possible to send data over the mobile network, even if all data communication comes with a cost. The cost was however not regarded as much of an issue, as the data volumes are expected to be rather small and security, in general, is prioritized and allowed to cost. Another option would be to gather the data when a vehicle is in for service and can be connected via cable. This would however imply that the data cannot be obtained based on when an attack occurs, and instead at rather unpredictable intervals. If a honeypot is used to also detect attacks, ideally an alert should be sent as soon as possible whenever an attack occurs. However, there is also value in only providing data for analysis, and in that case, it might not be necessary for data to be received immediately in the form of an alert. This means that some time delay can be acceptable, and that implies that collecting data when a vehicle is in for service is an option. It is however not the best solution and data should ideally be transferred as soon as possible after an attack has occurred to be of most use, which makes sending data over cellular connections the more attractive alternative if possible.

The action of collecting data from a honeypot in a vehicle is made more complicated by the fact that the vehicle is owned by a customer, and not the OEM acquiring the data from the honeypot. It is however still possible to retrieve data from a vehicle that has left the OEM. It requires administrative work and the owner must be informed in some way that data is being collected, but express consent from the owner is not necessarily required.

As IDSs are being used in vehicles to a greater extent and can effectively be used in combination with honeypots, the data collection from IDSs and honeypots needs to be handled collectively and in a well-thought-out manner. For efficiency and a less complex system, vehicle honeypots and IDSs can favorably send data off-board using the same software solutions. When the data is received at the back office it

must be properly handled for analysis or required action. This is best done by a SOC (Security Operations Center) or ideally a VSOC (Vehicle Security Operations Center) with the express responsibility of handling this data.

One critical aspect of logging data is the importance of keeping the connection between on-board and off-board secure. If the implementation for sending data to the back-office is done poorly that could become a vulnerability or an attack vector in itself. An attacker could gain access to this connection and send unauthorized messages to the back office.

4.3.4 Placement in the Vehicle Architecture

There is nothing in the existing research that discusses best practices when it comes to the placement of a honeypot in in-vehicle systems. This is a rather complex question as it depends a lot on the architecture of the in-vehicle system. As previously mentioned, the reference architecture presented by the CyReV project was used for this thesis.

The question of where to place a potential honeypot was brought up in all conducted interviews and was discussed from several different viewpoints. Some claim that a honeypot should be developed as a separate hardware component that is completely isolated from the rest of the software. The advantage of this is that it significantly reduces the risk of the honeypot becoming a way to gain access further into the system. A hardware component however is much more costly in terms of both money and resources compared to software. For the number of vehicles that could potentially carry a honeypot, it would be much simpler to implement a software solution.

As mentioned in the theory chapter the in-vehicle architecture referenced in this study, illustrated in Figure 3.2, is partitioned into four zones with protective borders in between. The outermost zone is the untrusted zone followed by the exposed zone which contains components that communicate off-board. The most suitable placement for a honeypot would be either the exposed zone or the border between the untrusted and the exposed zone. Firstly because it is the location of the external interfaces which is likely the place where an attack would start. Most attackers will try to enter from some kind of external interface, therefore placing a honeypot there will likely generate the most data at this point. As it is uncertain how often and in what way commercial vehicles are or could be attacked it is interesting to first look at the outermost parts of the system to see if anyone is trying to enter. Secondly, these potential placements are suitable as they do not contain any safety-critical parts of the system and this will therefore minimize the risk of the honeypot becoming a vulnerability in itself.

Another reason to place a honeypot in the exposed zone is that it contains a number of the services we have identified as interesting to emulate or use as bait in a honeypot, such as TCP ports or Bluetooth services. The infotainment system is another example of a component that communicates a lot with external parties and

that is complex enough to have its own OS (Operating System) which could make it a favorable location to place a honeypot.

There is a point in placing a honeypot further into the system as well, as this will tell if a hacker has been able to gain access to other zones, bypassing protective borders and potential IDSs. However, as there is much unknown about the potential attacks on commercial vehicles it is difficult to motivate a honeypot placed somewhere in the system where it could add vulnerability. The fact that it is still unknown what kind of attacks or attackers a honeypot should be designed to capture must also be considered. Combined, these aspects motivate that it is currently not something that can be recommended.

5 Recommendations

Part of the aim of this thesis was to present recommendations for the automotive industry on how best to implement vehicle honeypots at this point in the current cybersecurity landscape. This chapter presents recommendations for the initial steps of designing and implementing a honeypot specifically tailored toward commercial trucks. We have taken into consideration aspects like the current level of knowledge of cyber threats against vehicles and the existing security measures in trucks.

We start by presenting the prerequisites we recommend be taken into account before the designing of a honeypot is begun. We then motivate our recommendations by explaining the intended results and the desired threat intelligence that we conclude needs to be obtained at this point in time. We then present two different potential implementations of honeypots that we conclude are most relevant at this stage, as well as more general recommendations of implementations that could be relevant in future iterations.

5.1 Prerequisites

This section covers the measures we recommend be taken before a vehicle honeypot is designed to ensure the honeypot is valuable as a security measure and does not instead become a vulnerability to the system.

5.1.1 Establish Level of Risk

The implementation of the honeypot must be thoroughly evaluated from a security standpoint as it will become a new component in the system. This is preferably done by performing a TARA on the honeypot to make sure it does not add any unexpected vulnerabilities or risks to the system.

5.1.2 Establish an Owner

The honeypot must have an owner so that it is clear who shall handle it in case of error or failure. As mentioned in previous chapters the honeypot can be compromised in a way that it must be shut down or reconfigured. In that case, it must be clear who has this responsibility so it can be done efficiently. The owner must be clear over time to not allow the honeypot to be forgotten or abandoned and thereby become a vulnerability. It is the owner's responsibility to decide when and how the

honeypot should be decommissioned. If the responsibility for the honeypot is shared by too many parties it can quickly become no one's responsibility.

5.1.3 Establish How Data is Collected

For the honeypot to be useful the data it collects must be properly handled and analyzed. For this to be done efficiently it must be clear how this is to be done, both regarding the analysis of the data and how it is stored. This includes decisions about how often data will be sent off-board, how and when it will be analyzed, and who is supposed to handle this.

5.1.4 Establish How Threat Intelligence is Acted On

The analysis of the data collected from the honeypots could and should provide information about ongoing or attempted attacks. For the honeypot to be useful it is important to consider how this information is acted on once it has been collected. This could include a way to handle ongoing attacks on the system or a clear plan for who is responsible for updates to prevent similar future attacks.

5.2 Intended Results

At this stage in the cybersecurity protection of vehicles, we conclude that the desired threat intelligence obtained by a honeypot is a more direct indication of the threat level. Statistics on the number of attacks against a certain OEMs own vehicles could greatly help motivate the development and/or purchase of more sophisticated IDS. As the cybersecurity of vehicles is still a growing field, simple but broad statistics could help motivate higher budgets and increased interest in further investing in cybersecurity.

This sentiment was shared by several of the interviewees who stated that the best way to start would be to focus on detecting if, and how frequently, an attack occurs, and not as much on collecting detailed information about the attack or attacker.

For this reason, we conclude that the desired data from a honeypot at this stage is rather simple. The number of times a certain vehicle is exposed to probes, passive scans, and direct attacks, even at a rather simple level, is the aim. A lot is still unknown about remote attacks against vehicles, so the frequency and kind of attacks attempted is of great interest. Even rather uncomplicated port scans of different types are therefore of interest.

Further down the line, the honeypot could be reconfigured to obtain more detailed information. One step could be to emulate more vehicle-specific protocols and services, to gauge the level of specific knowledge of the attacker. Similarly, the honeypot could eventually be moved behind the first level of defense, to see if and how many attackers make it through.

5.3 In-Vehicle Implementation

At this point, information about the frequency of attacks and the knowledge and ability of attackers against vehicles is still limited. Therefore, the priority should be to collect information that can help inform decisions on how to move forward with overall security measures. If the frequency of attacks is found to be very high, this will give motivation and indication that it is essential to focus on implementing additional IDS or IPS.

Our recommendation is therefore a low-interaction honeypot placed close to or in the external cellular interfaces of the vehicle to collect information such as the frequency of attacks being carried out. Below we motivate and explain this decision.

5.3.1 Placement

Where to place the honeypot in the vehicle architecture is one of the most crucial decisions to make when implementing a honeypot. We recommend placing it in the exposed zone, in connection to the external interfaces in the vehicle. An example of this can be seen in the CyReV architecture in Figure 3.2 where a proposed honeypot is placed in the border between the untrusted and the exposed zone. That way it is relatively simple to make sure the honeypot is secure by ensuring it is isolated from crucial parts of the in-vehicle network such as safety-critical functions. It is also where it is most likely to get attacked as it is most likely that an attacker would approach the network through the remote interfaces placed in the exposed zone. Additionally, this is where many of the assets we identified as interesting are placed, such as TCP ports and the TGU.

5.3.2 Interaction Level

For the first implementation of a honeypot, we recommend a low interaction honeypot. A low interaction honeypot can be more easily set up as the software solution is less complex than a high interaction honeypot. This is motivated by the fact that the risk of adding vulnerability to the system when introducing a honeypot is lower with a more simple, less interactive solution. Also, even if a high interaction honeypot could provide more data from attacks, as a first step a low interaction will suffice. The data collected from a low interaction honeypot can give a lot of information about the threat landscape toward commercial vehicles, compared to what is currently known. Additionally, as a low interaction honeypot can be a rather simple solution it could be both resource-efficient and relatively quickly launched.

5.3.3 Logging Data

As the purpose of the honeypot is to collect data for analysis, how this data is handled is both interesting and important. Therefore we recommend that the data from an attack be sent from the honeypot to the back office as soon as possible after an attack has occurred. We recommend the data be stored in the vehicle until

transmission to the back office has been confirmed. The data should then reach some kind of SOC or VSOC that has efficient ways to analyze the data and act accordingly if needed.

5.4 Implementation on APN Network

Something we found interesting and looked into briefly was to implement honeypots representing whole fake vehicles on the APN (Access Point Name) network. This could be done in many different ways but the idea is that a hacker attempting to gain access to vehicles through the cellular networks might attack the honeypots instead of the real vehicles. There are several ways a honeypot could be made to emulate a vehicle on the network. This can range from something simple and low-interactive like an IP-address, to something much more intricate and high-interaction such as a whole simulated vehicle network.

One challenge to this alternative is how to tempt an attacker into targeting the honeypot instead of actual vehicles on the network. This requires a balance between designing the honeypot to resemble a real vehicle as precisely as possible or intentionally making it an attractive target by exposing some vulnerability. A possible suggestion to this is to use large enough numbers of honeypots emulating vehicles to make an attack on the honeypots statistically plausible without distinguishing them much from the real vehicles. This decision however has to be made with regard to the kind of information that is desired to be collected.

The use of honeypots resembling vehicles on the APN network is a promising suggestion as it proposes a solution that could limit the risk of real vehicles being compromised while still collecting interesting data. Additionally, this is a solution where the vehicle OEM owns the whole implementation and does not need to place the honeypot in a vehicle owned by someone else. This is an interesting option compared to implementations where the honeypot is incorporated in a truck that is no longer owned by the OEM. Therefore, this is a solution we recommend for further research and exploration.

5.5 Future Development

A lot is unfamiliar about the use of honeypots in vehicles as well as about what potential cyber threats vehicles could be facing in the future. Due to this, it is difficult to foresee to what extent a honeypot could be useful before it is implemented. Therefore, when an initial honeypot is deployed it might change our view of the use and need for both honeypots and other security mechanisms in the vehicles. If the honeypot is successful in capturing attacks, that could tell us that a more interactive honeypot could be useful in the next iteration to gain more data and information for analysis.

When it comes to the placement of the honeypot, we cannot motivate a recommendation for placing a honeypot in more critical zones further in the architecture. This is partially due to the security limitations of the CAN protocol and the possibility of gaining access to the whole network by compromising a single ECU. It could be interesting to see if an attacker can make it that far into the system, however, there is always a significant risk in adding a component close to safety-critical systems that could potentially be exploited in itself and become a vulnerability. Therefore, the risk of adding a honeypot in the protected or critical zone outweighs the motivation for it. However, even if we at this point can not recommend a honeypot further into the system, it could still be an interesting subject for further research and other conclusions could be drawn in the future.

6 Discussion

In this chapter, we discuss the results and the method through which they were obtained. We do this by, to the extent it is possible, evaluating and analyzing both the result and the method as well as considering different aspects of how changes in the method could have affected the results.

6.1 Cybersecurity in Industry

There is a complexity in researching cybersecurity for industry use as information about the security practices and mechanisms actually in use is not often publicly available. This is logical, as if the security tools are known some of them will lose their value. It does however make it rather difficult to research concepts like a honeypot for industrial use. Most of the published papers about honeypots describe a solution that is either a proof of concept or has been in use for a limited time. This makes them less applicable to an industry context as many of the features and conditions are not interchangeable between research and industry. It also makes it impossible to learn from and expand on honeypots that have been proven useful in other companies for industrial use as they are unknown. Additionally, this implies that our perception of the security scene in the vehicle industry as a whole is heavily based on assumptions. At the same time, vehicle cybersecurity is a very relevant topic with the previously mentioned UNECE R155 soon becoming active.

6.2 Results

As described in the aim of the study we aimed for well-substantiated conclusions and recommendations about the use of honeypots in vehicles. These results are not very tangible and therefore difficult to evaluate. The substantiation of the results is based on the literature review and the interviews. We have reached the results aimed for, however, as there is a limited amount of related work it is difficult to compare our results with other sources, and this makes them difficult to verify. Proving or evaluating the results was therefore not defined as a condition and was never planned to be done within this study.

6.3 Recommendations

The recommendations presented in Chapter 5 are based on the research done in this study. We deem them useful for the industry as guidelines and relevant to future research. They are however quite broad. Similar to our results, the recommendations cannot be evaluated or verified more than through the method. Worth noting is also that several of the interviewees were involved in the CyReV project, and we also used the CyReV reference architecture, which could have affected our conclusions by introducing a bias in our interview data.

This thesis was written in collaboration with Volvo Trucks, who provided a lot of insight and knowledge to the study. While the recommendations were written to be applicable generally within the industry, they are likely somewhat biased toward Volvo Trucks.

6.4 Method

The limited amount of published work on honeypots in vehicles made the literature review somewhat challenging. As mentioned in the method in Chapter 2, we instead had to focus on adjacent research areas, honeypots and vehicle cybersecurity separately. These two areas did provide an adequate foundation for research for this thesis. However, the limited amount of related work in combination with a rather large research scope has realistically affected the outcome of the thesis. A more narrow scope or a focus on a limited number of aspects could have resulted in more detailed or precise, and thereby potentially more useful, conclusions.

The interviews conducted were very valuable and made up a significant part of the research. The candidates for the interviews all had different backgrounds and varied knowledge about honeypots in vehicles, but all worked worked with, or in the vicinity of, vehicle cybersecurity. The varied backgrounds of the candidates were highly useful as they gave a broad perspective. Many of the candidates, however, were either employees at the Volvo Group and/or related to the CyReV project. The fact that the thesis was done in collaboration with Volvo Trucks enabled the interviews with the Volvo employees, which was truly beneficial to the research. It might however have provided a partial view. We were able to interview some candidates from other companies, which added greatly to the project. However, an even broader group of interview candidates with more diverse employments could have given more conclusive results. Moreover, as the interviews proved highly valuable, more interviews could have been conducted for even better results. For example, other actors in the security industry could have been interviewed. Potential candidates could have been companies providing IDSs or other security solutions, preferably to the vehicle industry. This was discussed as an option but due to time constraints, they were not attempted. Another way that could have made the interviews even more beneficial would have been to do them in iterations. That way a first iteration could have been done to narrow the scope and further iterations of interviews could have

provided deeper insights with slightly different questions between iterations. This would however have required more time or the interviews to have started earlier in the project.

The interviews were constructed as semi-structured, as described in Chapter 2. The manuscript that contains the basis for the questions asked in the interviews can be found in Appendix A and follow-up questions were asked depending on the answers as well as the candidates' background and expertise. Some additional questions were also added to the manuscript after a few interviews as we realized they would also be useful. Examples of these were questions regarding the logging of data as well as the use of a honeypot emulating a fake vehicle on the network. The questions were asked in a way aimed to get the interviewees' honest opinions but were perhaps formulated with the assumption that a honeypot would prove to be useful in vehicles, as this was the hypothesis behind this thesis. As previously mentioned, this is a very uncharted area in research and perhaps it would have been interesting with even more open-ended questions.

Despite the lack of previously published sources in the field of vehicle honeypots, the literature review of the neighboring areas turned out to be useful. It provided highly relevant knowledge specifically regarding honeypots in general. This was used as a basis for both our results and recommendations, together with data from the interviews. As this gave us a broad foundation to base our results on, we believe the methods used were a good approach to fulfill the aim of this thesis.

7 Conclusion

This thesis has aimed to present recommendations about how honeypots best can be implemented in a digitized and connected vehicle architecture, anchored in a thorough theoretical investigation into vehicle honeypots. That means that the current cybersecurity threat landscape, the current design of vehicle architecture, and the current level of detection and prevention measures in vehicles have been taken into account. This was done through a combination of literature studies and interviews with candidates from the automotive industry.

This study provides apparent scientific contribution, as the research in this area to date has been decidedly limited. As far as we know, there has been no previous research into honeypots placed in the vehicle architecture, the kind of honeypots we have studied in this thesis. While there have been some studies into research areas in proximity to ours, even that has been limited.

This study has been performed in collaboration with the department for Cybersecurity at Volvo Group Trucks Technology. The proposal of this project partly came from work being done towards compliance with the UN regulation UNECE R155 and the international standard ISO/SAE 21434 [8] [9]. These regulations and standards have been introduced following a fast increase in the connectivity of vehicles to make sure corresponding cybersecurity measures are put in place. The UNECE R155 is a regulation proposed by the United Nations for cybersecurity management systems of wheeled vehicles whose first phase comes into effect in the summer of 2022; the ISO/SAE 21434 is an international standard for cybersecurity risk management in road vehicles. The idea of a honeypot placed in the vehicle is seen as a possible step towards making sure vehicles are secure and resilient against remote cyber attacks. A honeypot can collect data about the frequency of attempted attacks and potentially even aspects like skill levels of attackers through an analysis of the kind of exploits they attempt. This kind of information can then guide the design of additional intrusion detection and prevention systems in vehicles.

The results of this study can be summarized as outcomes and conclusions within four main areas, as listed below. The first three give a broader overview of different possible implementations of vehicle honeypots. The fourth are our recommendations on the most suitable honeypot implementation at this point in time in the vehicle cybersecurity landscape, specifically tailored towards commercial vehicles.

The first outcome is a set of requirements for a functional honeypot. We have

identified these as key in ensuring a honeypot is effective and safe, and we suggest these are handled before any implementation of a vehicle honeypot occurs. The requirements are formulated specifically for vehicle honeypot implementations but are relatively general in their application. These include: being isolated from the rest of the system so as not to become a vulnerability, being tempting enough to be attacked but still resembling a normal component of the system, that logging of data has to be handled to ensure usability, and that there has to be a plan of how to handle the honeypot if/when it is discovered.

The second outcome is a set of aspects to consider before deciding to implement a vehicle honeypot. These include: the advantages, challenges and risks that need to be considered before implementing a vehicle honeypot. One main advantage is the kind of threat intelligence that can be obtained. An example of the challenges that need to be taken into account before implementing a honeypot are the maintenance and handling of the collected data. One risk is the honeypot itself becoming a vulnerability to the system, particularly if it deliberately contains known vulnerabilities in order to bait attackers. Another is that it inadvertently could give away information about how the system is designed or imply what components the owner thinks are most important through what is presented as bait.

The third outcome is a set of aspects to consider in the design stage of implementing a vehicle honeypot, such as interaction level and placement in the vehicle architecture. These cover suggestions of the kind of content that could be emulated by a honeypot or that can be used as bait in it, an analysis of the preferred level of interaction of a vehicle honeypot, how to handle the data logging of the information collected by the honeypot, and the placement in the vehicle architecture.

The fourth outcome is a set of recommendations for the most suitable designs of vehicle honeypots at this point. These are made up of a subset of the earlier presented data and are specific to the current state of cybersecurity measures in the industry. They are tailored towards commercial vehicles, as this thesis was carried out in collaboration with Volvo Trucks, but from the input we have collected from the rest of the industry, we believe the conditions are relatively similar across the industry and that the recommendations are quite general in their application.

In conclusion, we believe vehicle honeypots can be a valuable asset to the automotive industry in the continued work towards further increasing the cybersecurity protection measures of vehicles. As a starting point, we believe the recommendations we have presented in this study could help guide the industry towards a safe and appropriate implementation at this point in time in the vehicle cybersecurity landscape. And in the future, as presented in our results, there is a multitude of ways that vehicle honeypots could be designed, depending on what new information is desired to be collected, and the degree to which other IDS and IPS systems have been implemented.

7.1 Future Work

Several potential future endeavors could follow this study, both within the automotive industry and within the research community.

We hope that both Volvo Trucks and other automotive OEMs can use our recommendations to guide the continued work towards future implementations of vehicle honeypots. If conditions change or other areas are of interest than the ones we have proposed, other suggestions from the results can be used to formulate new recommendations.

More research into vehicle honeypots would also doubtlessly be of interest. Our results are structured in such a way that it should be possible to identify specific details that are interesting to look further into, for example, a specific placement in the vehicle architecture or a specific service to emulate.

Bibliography

[1] ESCRYPT and KPMG, *Whitepaper: Cybersecurity full speed ahead - How digitalization and automation present automotive manufacturers and suppliers with new security challenges*, ESCRYPT GmbH, 44789 Bochum, Germany, 2021. [Online]. Available: https://www.escrypt.com/sites/default/files/2020-11/201021_ESCRYPT_KPMG_Whitepaper-WP29_EN_screen.pdf.

[2] S. Parkinson, P. Ward, K. Wilson, and J. Miller, "Cyber threats facing autonomous and connected vehicles: Future challenges," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 11, pp. 2898–2915, 2017. DOI: 10.1109/TITS.2017.2665968.

[3] Upstream Security Ltd., *2022 Global automotive cybersecurity report*, Upstream Security Ltd. All Rights Reserved, 2022. [Online]. Available: https://upstream.auto/2022report/.

[4] S. McQuate, *UW and UC San Diego researchers honored for their work discovering that someone could hack a car*, University of Washington News, Sep. 2021. [Online]. Available: https://www.washington.edu/news/2021/09/22/uw-uc-san-diego-researchers-honored-discovering-someone-could-hack-car/.

[5] K. Poulsen, *Hacker disables more than 100 cars remotely*, WIRED, Mar. 2010. [Online]. Available: https://www.wired.com/2010/03/hacker-bricks-cars/.

[6] A. Greenberg, *Hackers remotely kill a Jeep on the highway - with me in it*, WIRED, Jul. 2015. [Online]. Available: https://www.wired.com/video/watch/hackers-wireless-jeep-attack-stranded-me-on-a-highway.

[7] ——, *Thousands of trucks, buses, and ambulances may be open to hackers*, WIRED, Mar. 2016. [Online]. Available: https://www.wired.com/2016/03/thousands-trucks-buses-ambulances-may-open-hackers/.

[8] *UN regulation no. 155 - cyber security and cyber security management system*, Addenda to the 1958 Agreement (Regulations 141-160), Document symbol: E/ECE/TRANS/505/Rev.3/Add.154, 2021. [Online]. Available: https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security.

[9] *Road vehicles — Cybersecurity engineering*, International Standard ISO/SAE 21434:2021(E), 2021. [Online]. Available: https://www.iso.org/standard/70918.html.

[10] I. Mokube and M. Adams, "Honeypots: Concepts, approaches, and challenges," New York, NY, USA: Association for Computing Machinery, 2007, ISBN:

9781595936295. DOI: 10.1145/1233341.1233399. [Online]. Available: https://doi.org/10.1145/1233341.1233399.

[11] L. Zobal, D. Kolář, and R. Fujdiak, "Current state of honeypots and deception strategies in cybersecurity," in *2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, 2019, pp. 1–9. DOI: 10.1109/ICUMT48472.2019.8970921.

[12] V. Verendel, D. K. Nilsson, U. E. Larson, and E. Jonsson, "An approach to using honeypots in in-vehicle networks," in *2008 IEEE 68th Vehicular Technology Conference*, 2008. DOI: 10.1109/VETECF.2008.260.

[13] S. Panda, S. Rass, S. Moschoyiannis, K. Liang, G. Loukas, and E. Panaousis, "Honeycar: A framework to configure honeypotvulnerabilities on the internet of vehicles," *arXiv preprint arXiv:2111.02364*, 2021. DOI: 10.48550/arXiv.2111.02364.

[14] S. Sharma and A. Kaul, "A survey on intrusion detection systems and honeypot based proactive security mechanisms in vanets and vanet cloud," *Vehicular communications*, vol. 12, pp. 138–164, 2018.

[15] P. Patel and R. Jhaveri, "A honeypot scheme to detect selfish vehicles in vehicular ad-hoc network," in *Computing and Network Sustainability*, Springer, 2017, pp. 389–401.

[16] D. Gantsou and P. Sondi, "Toward a honeypot solution for proactive security in vehicular ad hoc networks," in *Future Information Technology*, Springer, 2014, pp. 145–150.

[17] R. Joshi and A. Sardana, *Honeypots: A new paradigm to information security*, 1st Ed. Distributed by CRC Press, Boca Raton, FL.: Science Publishers, Enfield N.H., 2011, ISBN: 9780429061905. DOI: https://doi.org/10.1201/b10738.

[18] J. Franco, A. Aris, B. Canberk, and A. S. Uluagac, "A survey of honeypots and honeynets for internet of things, industrial internet of things, and cyber-physical systems," *IEEE Communications Surveys Tutorials*, vol. 23, no. 4, pp. 2351–2383, 2021. DOI: 10.1109/COMST.2021.3106669.

[19] M. Björklund and U. Paulsson, *Academic Papers and Theses*, 1st Ed. Denmark: Studentlitteratur, 2014, ch. 4: Method awareness, ISBN: 9789144093765.

[20] K. E. Barajas, C. Forsberg, and Y. Wengström, *Systematiska Litteraturstudier i Utbildningsvetenskap: Vägledning vid Examensarbeten och Vetenskapliga Artiklar*, 1st Ed. Stockholm: Natur & Kultur, 2019, ch. 2: Olika Typer av Litteraturstudier, ISBN: 9789127134119.

[21] V. Waller, K. Farquharson, and D. Dempsey, *Qualitative Social Research: Contemporary Methods for the Digital Age*, 1st Ed. London, UK: SAGE, 2016, ch. Six: Interviewing, pp. 75–82, ISBN: 9781473913554.

[22] B. Sangchoolie, *Cyber resilience for vehicles*, RISE Research Institutes of Sweden, 2019. [Online]. Available: https://www.ri.se/en/what-we-do/projects/cyber-resilience-for-vehicles.

[23] AutoSec, *Automotive security and privacy*, Hosted by RISE Research Institutes of Sweden, 2022. [Online]. Available: https://autosec.se/.

[24] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16–24, 2013.

[25] O. Y. Al-Jarrah, C. Maple, M. Dianati, D. Oxtoby, and A. Mouzakitis, "Intrusion detection systems for intra-vehicle networks: A review," *IEEE Access*, vol. 7, pp. 21 266–21 289, 2019.

[26] L. Spitzner, *Honeypots: tracking hackers*. Addison-Wesley Reading, 2003, vol. 1.

[27] W. Fan, Z. Du, and D. Fernández, "Taxonomy of honeynet solutions," in *2015 SAI Intelligent Systems Conference (IntelliSys)*, 2015, pp. 1002–1009. DOI: 10.1109/IntelliSys.2015.7361266.

[28] A. Golshan, C. Sandberg, N. Nowdehi, and T. Rosenstatter, "Deliverable D2.1 CyReV reference architecture," CyReV - Cyber Resilience for Vehicles, Tech. Rep., 2021, DRAFT - Under documentation.

[29] P. Carsten, T. R. Andel, M. Yampolskiy, and J. T. McDonald, "In-vehicle networks: Attacks, vulnerabilities, and proposed solutions," in *Proceedings of the 10th Annual Cyber and Information Security Research Conference*, ser. CISR '15, Oak Ridge, TN, USA: Association for Computing Machinery, 2015. DOI: 10.1145/2746266.2746267. [Online]. Available: https://doi.org/10.1145/2746266.2746267.

[30] M. Hashem Eiza and Q. Ni, "Driving with sharks: Rethinking connected vehicles with vehicle cybersecurity," *IEEE Vehicular Technology Magazine*, vol. 12, no. 2, pp. 45–51, 2017. DOI: 10.1109/MVT.2017.2669348.

[31] *Road vehicles — Unified diagnostic services (UDS) — part 1: Application layer*, ISO 14229-1:2020, 2020. [Online]. Available: https://www.iso.org/standard/72439.html.

[32] *The universal measurement and calibration protocol*, ASAM MCD-1 XCP, 2017. [Online]. Available: https://www.asam.net/standards/detail/mcd-1-xcp/.

A Appendix: Interview Information and Questions

Elin Eriksson
Lisa Fahlbeck

Investigating the Use of Honeypots in Vehicles

A Brief Introduction to Our Project and to Honeypots in General

We are two students from Chalmers University of Technology doing a masters in computer systems and networks with a previous bachelors in software engineering. We are currently writing our master thesis at Volvo Group Trucks Technology Cybersecurity about the use of honeypots in vehicles, looking at how they can be implemented and used specifically in trucks for increased security.

Honeypots are a tool used in cybersecurity to gain information about potential adversaries and attacks. The honeypot as a component doesn't add functionality to the system and doesn't generate traffic on its own. This makes it a useful tool as all identified traffic on the honeypot is obtained clear of any legitimate traffic on the network. Honeypots act as traps for attackers in order to collect information about existing threats to the system or network by exposing potential vulnerabilities and gaining information about attackers and the way they operate. With the intelligence gained from honeypots, security efforts to counteract the identified vulnerabilities can then be developed and implemented in focused efforts.

Below are a few questions we would like to ask you. We understand all questions might not be within your field of expertise and general thoughts and interesting ideas are as valuable as definite answers.

1. What potential cyberthreats do you see to vehicles/trucks today?

2. What advantages do you identify in using honeypots specifically in vehicles?

3. What challenges and/or risks do you identify in using honeypots specifically in vehicles?

4. What would you say is the most important purpose of a honeypot - prevention or research?

5. What would you say are the most critical areas that we would like to capture intelligence about through the use of honeypots? (Services, safety critical functions, etc)

6. Do you think a honeypot would be most beneficial if used to target remote or physical access attacks?

7. Do you have any initial thoughts on where in the vehicle architecture you would place a honeypot?

8. What are the best sets of assets to include in a honeypot as bait?