DEGREE PROJECT IN TECHNOLOGY,
FIRST CYCLE, 15 CREDITS
STOCKHOLM, SWEDEN 2019

A Study on Vulnerabilities in Connected Cars

MELEK GÜLSEVER

KTH ROYAL INSTITUTE OF TECHNOLOGY
SCHOOL OF ELECTRICAL ENGINEERING AND COMPUTER SCIENCE

A Study on Vulnerabilities in Connected Cars

MELEK GÜLSEVER

Bachelor in Computer Science
Date: June 7, 2019
Supervisor: Robert Lagerström
Examiner: Örjan Ekeberg
School of Electrical Engineering and Computer Science
Swedish title: En studie av sårbarheter i uppkopplade personbilar

Abstract

This report researches the state of cyber security in connected cars. Specifically, common vulnerabilities and trends related to security issues in connected passenger cars are identified.

The study is conducted through a systematic review of publicly reported vulnerabilities and incidents related to computer systems in connected cars. Some of the largest manufacturers in the automotive industry are researched along with common automotive suppliers. In addition, systems and devices used in connected cars are identified to further extend the reach of the study.

The scope of this thesis is limited to publicly available material from two types of sources. The first source is the repository of cyber security company Upstream, which monitors automotive incidents in real-time. The second source is the National Vulnerability Database, NVD.

The most common types of vulnerabilities linked to connected cars were found to be predominantly related to remote keyless systems (RKS), mobile applications, infotainment systems and the OBD port. A vast majority of the found vulnerabilities were remotely exploitable. The most common weakness was related to failure or lack of protection mechanisms.

Sammanfattning

Denna rapport undersöker cybersäkerheten i uppkopplade bilar. Studien identifierar vanliga sårbarheter och trender relaterade till säkerhetsproblem i uppkopplade personbilar.

Studien utförs genom en systematisk granskning av offentligt rapporterade sårbarheter och incidenter relaterade till system i uppkopplade bilar. Några av de största tillverkarna inom bilindustrin granskas samt underleverantörer till dessa. Dessutom identifieras system och enheter som används i uppkopplade bilar för att ytterligare utöka studiens räckvidd.

Omfattningen av denna rapport är begränsad till offentligt tillgängligt material från två typer av källor. Den första källan tillhör cybersäkerhetsföretaget Upstream och består av en sammanställning av incidenter relaterade till cybersäkerhet i bilindustrin som uppdateras i realtid. Den andra källan är National vulnerability database (NVD) och är en amerikansk databas över sårbarheter.

De vanligaste typerna av sårbarheter för uppkopplade bilar visade sig vara relaterade till nyckellösa låssystem, mobilapplikationer, infotainment-system och OBD-porten. En stor majoritet av de funna sårbarheterna kunde exploateras via trådlösa uppkopplingar. Den mest förekommande svagheten var relaterad till bristande skyddsmekanismer.

Contents

Chapter 1

Introduction

The automotive industry is undergoing extensive change, transforming the entire industry and with it the development process of vehicles. What was once a predominantly mechanical industry is now made up of software and hardware development as an integral part of the production. This is naturally reflected in the end product; a modern day connected car could be considered to be a system of computers, with millions of lines of code [1]. These advancements come with great improvements in nearly all aspects of a car's functionality, ranging from fuel efficiency to many safety features and increased comfort, enhancing the overall user experience.

Many car manufacturers provide smartphone application services which enable the user to remotely control and track the car [2], and advanced driver assistance systems (ADAS) that aim to eliminate the human error by implementing several safety features to assist the driver [3]. While computer systems and electronic control units (ECUs) account for these new innovations they also come with a whole new set of challenges new to the automotive industry, namely those related to computer systems.

Modern cars consist of many interconnected subsystems and computers which control every aspect of the car's functionality. A software malfunction in a car could in a worst case scenario not only lead to substantial brand damage and loss of revenue for the manufacturer, but also risk the lives of the users and pose a risk to their environment. Consequently, robust systems are crucial. With the help of automotive grade components, different types of extremes can be handled as well as an extended life expectancy for the product in question. These robust systems must, however, also be durable in other ways than merely physical. Just like computers, cars are now also at risk of malicious attacks. Vulnerabilities can be exploited which can lead to software or

hardware malfunction, data leaks or a variety of other results, the worst case being life threatening situations.

Increased and added amount of connectivity in vehicles makes way for new innovations but simultaneously increases the attack surface and risk of malicious exploits [4]. These challenges are a part of every abstraction level of the car, ranging from mobile application services provided by the manufacturer down to the very chips making up one of many subsystems.

Security researchers have performed several demonstrations of car hacking to make aware the industry and the public of the many serious implications vulnerable systems can have. The infamous example of a Jeep being remotely overtaken by white hat hackers [5], resulting in a recall of 1.4 million vehicles is just one of many cases [6].

While many companies choose not to publicly disclose details or even the presence of vulnerabilities, recent industry developments have led to some companies adopting different strategies working with cyber security, some of which even encourage white hats to find vulnerabilities by giving out rewards [7].

Secure ICT systems are paramount in the automotive and transportation industry where a failure can lead to critical situations. The future holds many challenges which must be addressed, calling for new methods in product development as well as increased collaboration across entire industries.

1.1 Problem Statement

To better understand the current state of the automotive industry and what the challenges are related to commercial connected cars in terms of cyber security this thesis aims to answer the following questions:

- What are the common vulnerabilities for connected cars?
  - What weaknesses are these found vulnerabilities related to?
  - What are the impacts of the most common vulnerabilities?
- What trends can be found in security issues of cars?

By answering these questions a summary of common vulnerabilities and attack vectors will be one of the end results, providing a foundation for future studies.

1.2 Scope

This thesis aims to evaluate the most common vulnerabilities found in connected vehicles. The vehicles considered are commercial connected passenger cars. The research is carried out through observations of publicly available reports of attacks and vulnerabilities, strictly limited to two sources: the vulnerability database NVD [8] and the incident repository of cyber security company Upstream [9]. All vulnerabilities directly connected to and with the potential of impacting the system of a car are considered, meaning vulnerabilities of type: software, hardware and firmware. Vulnerabilities in aftermarket products with the ability of affecting a car's system are also examined.

It is not within the scope of this thesis to simulate or model attacks on cars. Neither does this thesis intend to investigate or measure certain manufacturers' and service providers' level of security compared to others.

1.3 Thesis Outline

Chapter 2 presents background information related to the study. This includes definitions of systems used in this paper, related work and an overview of the connected car anatomy. Chapter 3 follows with a description of the methodology and methods used. Chapter 4 presents the results and chapter 5 provides a discussion involving the findings and background information. Lastly, chapter 6 ends with the conclusions that were drawn in the study.

Chapter 2

Background

This chapter introduces key concepts to this study and the methods being used. In 2.1 the term *connected car* is defined. Section 2.2 proceeds with a presentation of the typical connected car anatomy. Section 2.3 continues with an introduction of the concept of vulnerability databases and associated concepts such as: the scoring system used to measure severity of vulnerabilities and the categorization system for weaknesses. Lastly, 2.4 provides a background in the contributions of previous work done in the field.

2.1 The Connected Car

The usage of the term *connected car* is often wide and inclusive of several different types of connectivities, often refering to e.g. Bluetooth and internet. Uhlemann [10] provides the definition of a car to be connected when it has components enabling connection of devices, services and networks, all of which can be either internal within the car and/or external, allowing short and/or long range communication. Although there are different types of connectivities within the various abstraction layers of a car many of the systems are interconnected, with some units being used for multiple purposes. One example of such an interconnection is the widespread functionality of remotely being able to start and control certain functions of a car from mobile applications, e.g. the BlueLink service provided by Hyundai [2]. A simplified description of such a connection path would for instance start from a phone, go through an internet connection or a radio signal, be received by one of the car's antennas, go through the ECUs and down to the mechanical processes of the car.

The reasons for adding connectivity to a car are many. As mentioned in

chapter 1, there are countless ways in which the user experience can be enhanced. Connecting a car to it's environment generates large amounts of data. A McKinsey study suggests that cars process up to 25 gigabytes of data per hour [11], n.b. that the article was published in 2014 and it is therefore reasonable to assume that the numbers are higher today due to the increase of connected devices in cars.

The data generated and processed in cars can be used for several purposes, e.g. real-time diagnostics, making maintenance of vehicles more efficient [12] or in ADASs for e.g. driver drowsiness detection [13][3].

Despite the positives, it should be emphasized that introducing connectivity to a car is the equivalent of exposing the system to the outside world; introducing new and increased numbers of attack vectors and threats of remote exploits of vulnerabilities. In a recent press release, cyber security company Karamba Security presented the results of a study where automotive ECUs had been exposed to the internet. Each of the ECUs had been subject to a staggering number of 300 000 attacks per month in average [14].

2.2 Connected Car Anatomy

When studying computer system weaknesses and the vulnerabilities that follow, it is important to understand what the associated attack vectors and surfaces are. This section therefore provides an overview of relevant systems in the connected car anatomy.

2.2.1 Electronic Control Unit (ECU)

Electronic Control Unit (ECU) is the general term used to describe an embedded system which is responsible for one or multiple subsystems in a car, where many functions require actions from multiple ECUs [15]. ECUs are microcontroller based systems, each having sensors and actuators, which process input and output data from various sources. The ECUs are part of a complex interconnected system and are linked to nearly every aspect of a car's functionality where some units may have connection to the external environment via e.g. Bluetooth. The ECU consists of hardware and software based on the type of functionality and designated area of application. Some examples of common types of ECUs and their functions can be seen in table 2.1.

The number of ECUs in vehicles are rapidly increasing, the modern car having an average of 50 to over 100 ECUs according to Möller [16]. In addition, the embedded software in the ECUs is also growing, leading to an overall

increase in system complexity. A 2014 study illustrates the magnitude by giving an estimation of 100 million lines of code in a car [11].

The steady growth of these modules result in an increased amount of nodes in the systems. These factors combined make the cars even more susceptible to threats and vulnerabilities as the attack surfaces are continuously growing.

Table 2.1: Examples of ECUs and their functions

ECU type	Function
Electronic Brake Control Module (EBCM)	Controls the braking system based on multiple inputs (e.g. speed)
Door Control Unit (DCU)	Controls the electronic functionalities of a door
Engine Control Module (ECM)	Manages engine performance based on input from multiple sensors
Telematic Control Unit (TCU)	Consists of GPS, GSM for mobile communications, LTE radio

2.2.2 In-Vehicle Networks

The in-vehicle networks are responsible for the communication within the internal systems of a car. As mentioned in 2.2.1 the ECUs are responsible for processing important data to control the car's systems. This data can for instance be generated by other ECUs, sensors and user input. Many functions require interaction between several ECUs to execute tasks, therefore, stable communication is key.

There are several vehicular network types used in cars which are implemented depending on the area of application. The Controller Area Network bus (CAN bus) standard is the most prevalent automotive network type [16]. The CAN bus is a central message based networking system, enabling communication between all ECUs without a host computer. Each ECU can send and receive messages, also called frames, but not concurrently. Messages sent have IDs which enable the system to prioritize tasks by communicating the level of urgency [17]. A model of a message being sent in a CAN bus can be seen in figure 2.1.

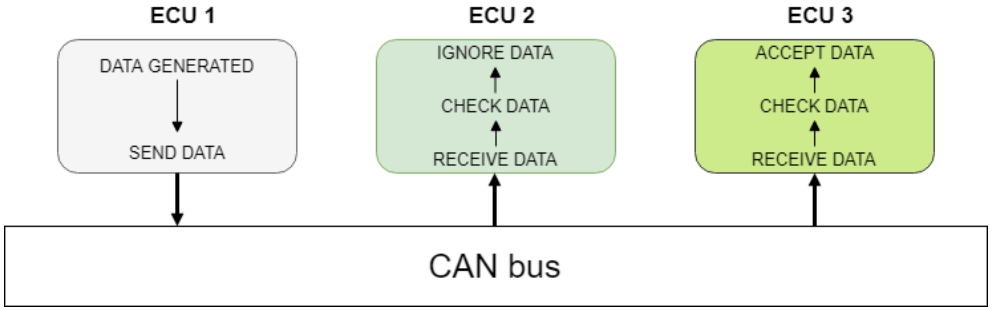

Figure 2.1: Model of ECUs communicating through a CAN Bus

The CAN protocol is a low level standard without security features, examples being that the messages sent are not encrypted and due to the format of the messages not having a field for authentication, it is possible to send fake frames to other nodes in the network [15]. There have been several hacking incidents where a compromise of ECUs has made it possible to inject messages into the CAN bus, giving the hackers control of car systems. The famous Jeep hack which is mentioned in the introduction made use of this method to take over a car [5].

The CAN protocol issues has been addressed with suggestions of implementing ECU software monitoring to analyze messages, or setting up CAN bus firewalls to filter messages. However, a study from 2017 reports that the CAN standard itself has vulnerabilities allowing attacks to bypass all of the suggested security mechanisms undetected [18].

It is not uncommon for cars to have multiple CAN buses which are isolated. One plausible hypothesis would be that the intention of isolation is to separate critical systems from others due to reasons related to security. This is, however, not the case and the separations are often due to bandwidth and concerns with integration rather than security [19]. Certain modules have more time-critical functions than others and are therefore connected to a high speed CAN bus, while some units are connected to low speed buses [15]. A model of a vehicular network with two CAN buses is shown in figure 2.2.

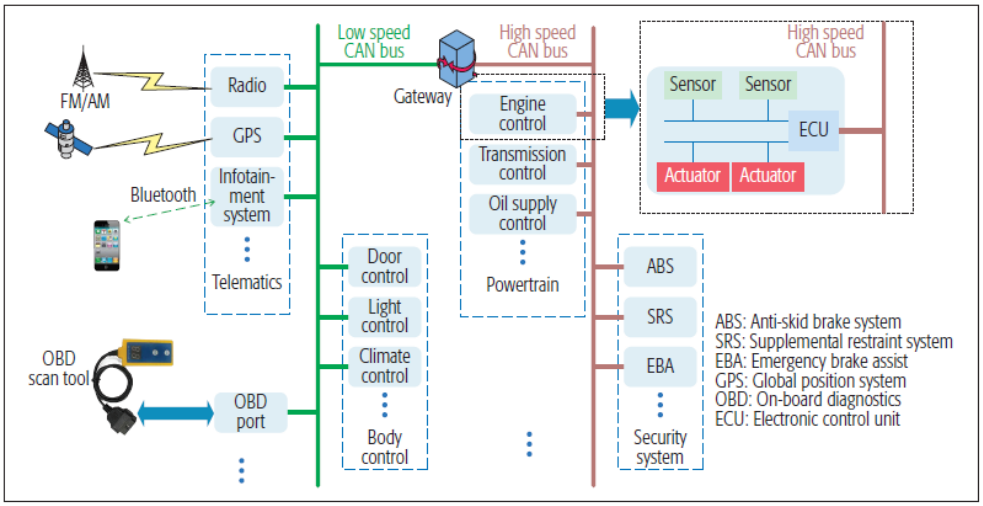

Figure 2.2: Model of a vehicular network by Liu et al. [15]

2.2.3 In-Vehicle Infotainment (IVI) and TCU

As implied by the name, infotainment is a combined system of information and entertainment technologies. The make up of the systems are mostly brand and model specific, though many provide similar functionalities.

Vehicular infotainment systems require operating systems and have interfaces for user interaction, e.g. a screen located on the dashboard and control units on a steering wheel, and often have support for smartphone pairing via Bluetooth. Some infotainment systems also have physical ports, enabling connection to peripherals such as USB devices. Furthermore, the system is integrated with the Telematic Control Unit (TCU) which is briefly explained in table 2.1 in section 2.2.1. The TCU enables connection to the outside world by providing systems for GPS navigation, GSM for mobile communications and LTE [16]. A model of a TCU can be seen in figure 2.3.

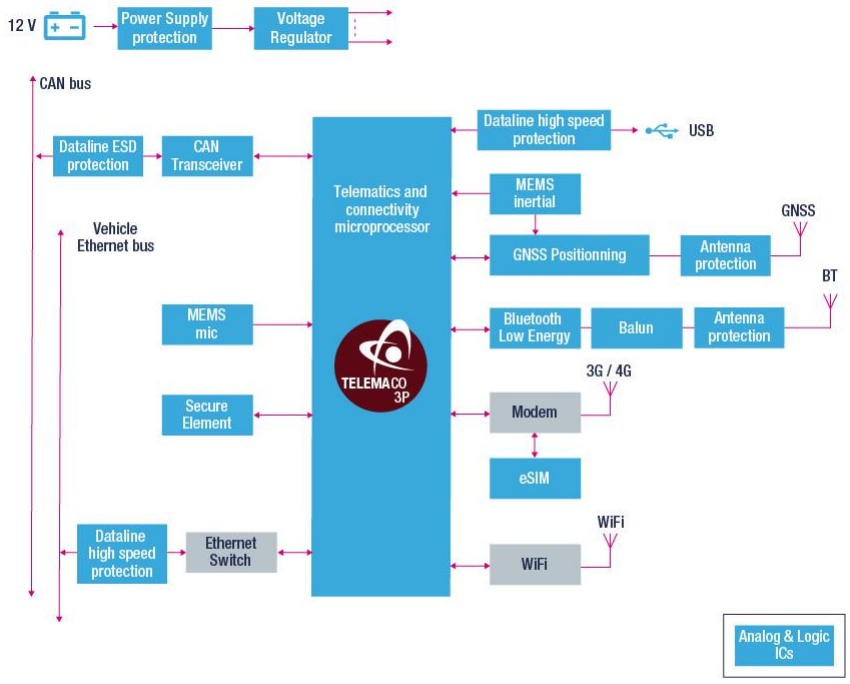

Figure 2.3: Model of a TCU by STMicroelectronics [20]

2.2.4 On-Board Diagnostics (OBD)

On-Board Diagnostics (OBD) monitors the systems of a car in real-time to detect various types of system failures and anomalies. The OBD is connected to the ECUs and buses of a vehicle, and has priviliges to read and reset code in the system.

The system was originally developed to reduce emissions by monitoring the engine [16] and has since become a standard which is even regulated by law in the EU [21]. The OBD-II is the improved standard specifying the connector of the OBD port which is used by service technicians in vehicle troubleshoots and repairs.

The OBD adapter, sometimes called OBD dongle, is a common aftermarket product which allows vehicle owners access to information which was previously only available to mechanics [22]. However, the OBD and associated aftermarket products have been used in several hacks where the diagnostic system has been compromised to gain access to the CAN buses, allowing hackers to inject messages into the internal network. An example of this is the BlueDriver hack which allowed unrestricted Bluetooth pairing [23].

2.2.5 Remote Keyless Systems (RKS)

The remote keyless system (RKS) is an electronic lock that allows users to remotely lock and unlock cars. There are two types of RKS, where one is called active, for instance requiring the press of a button, the second type is passive (PKE) and unlocks the car when the key is within proximity [24]. When the button is pressed on an active RKS, the key fob which contains a microcontroller, sends a stream to its transmitter which then sends an encrypted radio signal through a small antenna to the receiver in the car [25]. However, if the system is passive, the communication is bidirectional with a transceiver on both ends. In such a system the car continuously sends out a signal which the key picks up and responds to if it is within proximity. The car is unlocked if the signals are compatible. A model of a remote key can be seen in figure 2.4.

Initially, the increase of remote key technology managed to significantly reduce the number of cars stolen [26]. The numbers have since started going the opposite direction, with new types of car thefts being reported which instead bypass the technologies used. The General German Automobile Club (ADAC) recently tested 237 different keyless cars of which an alarming 234 turned out to be susceptible to keyless hacks [27].

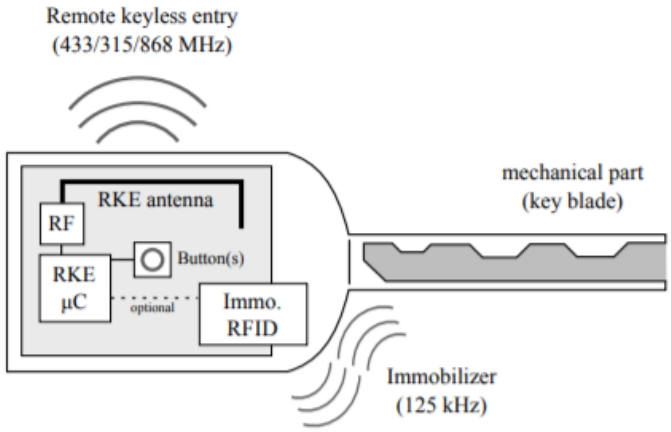

Figure 2.4: Model of a remote vehicle key with a mechanical part [25]

Common types of hacks on RKS involve copying and replaying the signal (replay attack/eavesdropping). To prevent eavesdropping, a Rolling Code protocol is often used, which provides new code for each authentication [28]. Another common hack for PKE is the Signal Amplification Relay Attack (SARA), which makes use of a relay device that boosts the signal from the car, tricking the key to unlock the car [29].

2.3 Vulnerability Databases

Vulnerability databases are commonly used tools in software security management with the aim of facilitating software vulnerability mitigation. Generally, when a flaw is reported the affected organizations are notified before information about the vulnerability is publicly disclosed in the databases [30]. Ideally, this enables the vendors to patch the affected software before any potential malicious exploits can take place. However, this not always the case and sensitive information about detected vulnerabilities can be leaked, sometimes with malicious intent. Similarly, there is the additional risk of the vendors being too slow in regards to patching the software. This in turn means that a malicious actor may be able to exploit the vulnerability before it is patched.

The National Vulnerability Database (NVD) [8] is a software vulnerability database launched by the U.S. government. NVD is one of the most commonly used vulnerability databases and has been shown to be one of the most trustworthy in previous comparative studies [31].

2.3.1 Common Vulnerabilities Scoring System

The Common Vulnerabilities Scoring System (CVSS) [32] provides a standardized tool through which software vulnerabilities can be assessed and labeled with a score. This score is called the base score and ranges from 0.0 to 10.0, where a high number indicates a critical vulnerability. Thus, CVSS enables organizations to address vulnerabilities based on priority level. The system also provides a contextual framework which can be used regardless of application type.

The score is set based on three metric groups that generate a number through an equation which can be found in the CVSS specification [32]. The metric groups are: Base, Temporal, Environmental, which also have own sets of metrics. The system takes several parameters into account when calculating the score. The attack vector is one example, referring to the context by which a vulnerability is exploitable. The possible values are: network, adjacent, local, physical. Due to a remote attack vector allowing anyone with access to the network to exploit the vulnerability, the risk of attacks is higher and therefore also the score generated by that specific value. A physical attack vector could for instance be a peripheral such as a USB drive.

2.3.2 Common Weakness Enumeration (CWE)

The Common Weakness Enumeration (CWE) is a categorization system for software weaknesses. Entries in vulnerability databases are labeled with a CWE ID based on characteristics. CWE lists the following three points to highlight the purpose of the system, which is to:

- Serve as a common language for describing software security weaknesses in architecture, design, or code.
- Serve as a standard measuring stick for software security tools targeting these weaknesses.
- Provide a common baseline standard for weakness identification, mitigation, and prevention efforts. [33]

2.4 Related Work

Many reports have been published on the subject of connected cars and the issue of cyber security. An experimental approach is common, where researchers test systems, e.g. [34]. It is also important to note that security research overall, especially with an experimental approach, is *not* limited to traditional academic environments. Many independent security researchers continuously test systems and publish their own reports in different formats and forums. Security companies also make significant contributions, e.g. the security company Computest with the Volkswagen/Audi hack [35].

One study had the objective of creating a vulnerability catalogue for connected cars by mapping out and linking car components to corresponding threats associated with the parts [36]. This study is, however, entirely based on previous work and not collection of reported vulnerabilities per se. Bécsi et al. [37] also have a similar approach but with the primary focus being how the connected features change the vehicles and what the related vulnerabilities in regards to the connectivity.

Based on the extensive research carried out in this study, no reports were found to share the same combination of objective and method within the field of connected cars. The study by Välja et al. [38] does, however, share one of the methods used in this paper to study another area of embedded systems, namely vulnerabilities in power networks. Vulnerability data is collected from databases to analyze trends and related weaknesses.

There is also research on the methods which are used in this thesis. Though CVSS and NVD have been demonstrated to be trustworthy enough in [31], a study by Allodi et al. [39] shows that black market monitoring has the potential of outperforming traditional methods such as CVSS and NVD by providing an average of 20 % reduction of expected attacks.

Chapter 3

Method

This chapter describes the methods used in this thesis. The goal of this study is to identify common vulnerabilities in connected cars, therefore, a systematic review is a well suited approach.

The work process can be divided into three steps. The first step was a pre-study, with the focus of mapping out common features of a typical connected car, then continue with a study of the automotive industry to find common tier ones and relevant aftermarket products. This was done by studying information from manufacturers, reports and news sources. The second step consisted of extracting relevant vulnerability data (which is specified in 3.1) from a vulnerability database, NVD [8]. This research was based on the information gathered in step one. Collection of vulnerability data was also the focus of the final step, however, the information was gathered through an additional platform, Upstream, which monitors and publishes cyber security related incidents from the automotive industry in a repository [9]. Lastly, the findings are analyzed based on characteristics, trends (e.g. over time periods), commonalities and origins.

The main motivation behind conducting the research through said database and platform is the capability of studying vulnerabilities in a systematic and quantitative manner. Both of the sources mentioned provide information in a concise standardized template format. An additional important motive is the difference in content, where these methods combined manage to compile relevant information in one place. While NVD and Upstream both provide information about distinct, detected vulnerabilities, Upstream also publishes multiple reports regarding incidents which may involve the same vulnerability being exploited on several occasions. This gives the study yet an important dimension which NVD alone fails to provide. Although NVD rates vulnera-

bilities based on severity it does not address the frequency of exploits. In this regard, the combined use of the two sources makes it possible to analyze *what* the known vulnerabilities are, *how/if* they are being exploited, what the associated *consequences* are and finally draw conclusions regarding any potential trends. Furthermore, vulnerability databases are commonly used tools in software security management and therefore considered relevant to this thesis. A similar approach of collecting vulnerability data from NVD has also been used in previous studies, e.g. [38].

3.1 Vulnerability Database: NVD

The database used in this study is the National Vulnerability Database, NVD. While there are other similar vulnerability databases, NVD has been reviewed as a security tool in prior studies, one example being a study conducted by Johnson et al. [31] which explores the credibility of CVSS data in different vulnerability databases. The paper comes to the conclusion that NVD is indeed the most trustworthy in comparison to other leading databases.

NVD has a standardized format for each vulnerability entry in the database. An example of this can be found in figure 3.1.

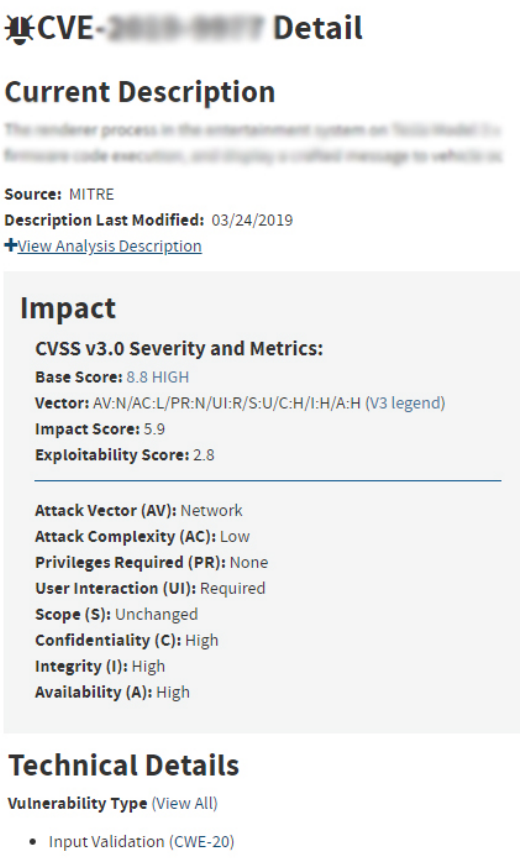

Figure 3.1: Example of a vulnerability entry in NVD

Information corresponding to the thesis objective was gathered from each separate vulnerability and were determined to be the following: vulnerability ID (CVE ID), date reported, base score, attack vector (AV) and vulnerability type (CWE). The data was manually collected from the database and saved in a data sheet.

In order to study vulnerabilities related to computer systems found in cars through a vulnerability database the search terms are key. These were found during the pre-study phase where the automotive industry was researched to gather a list of relevant manufacturers, devices, domain specific terminology and technologies to examine in the database. This was done by firstly going through a list of car manufacturers [40]. Specifications of car models were then studied along with the automotive supply chain and common features/devices used in connected cars, resulting in additional component manufacturers being found. The component manufacturers were then browsed to further extract data from NVD. All of the search terms were documented and the full list can

be found in table A.1 in appendix A, where the list is sorted in two columns, *OEM* and *MISC*, OEM being the car manufacturers and MISC (miscellaneous) containing various relevant keywords, e.g. tier one suppliers' names, domain specific vocabulary and common technologies used.

In order to differentiate devices used in the automotive industry from similar but non-automotive devices, the suppliers and their specifications were reviewed parallel to the collection of data from NVD.

3.2 Security Incident Repository: Upstream

Upstream is a cyber security company which monitors incidents related to security in the automotive industry in real-time [9]. Sources of published posts consist of media outlets, scientific reports, blog posts, industry reports etc. Entries are posted in a repository in chronological order, starting in the year 2010.

The incidents published by Upstream cover a wide scope, examples ranging from automotive manufacturers being subject to server side attacks to cyber vulnerabilities found in trains. Thus, it was required to filter out entries in order to find those within in the scope of this thesis. Specifically, vulnerabilities which have the potential of impacting the functionality of the connected passenger car's system were collected. This was done manually, where each entry was evaluated separately. The entries which were in the scope of this paper were selected and collected in a data sheet.

An example of how entries are presented in the Upstream repository can be seen in figure 3.2.

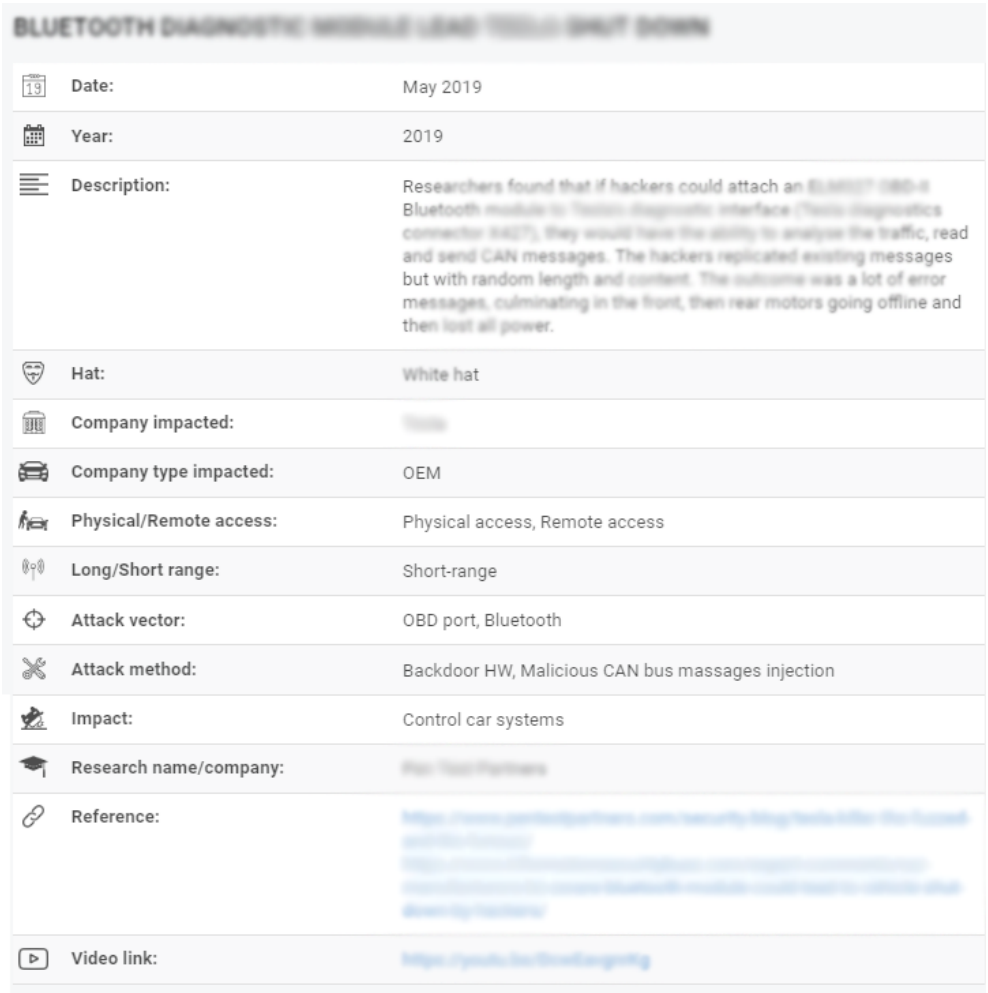

Figure 3.2: Example of an entry in the Upstream repository

The information that was obtained from each selected entry were the following: date, hat, company impacted, company type impacted, physical/remote access, long/short range, attack vector, attack method, impact and reference.

Chapter 4

Results

This section presents the results from the study. The data from NVD and Upstream are presented separately. Both sections begin with a presentation of the complete findings to give an overview. The following parts present information about attack vectors, from which the vulnerabilities have been exploited, with additional information about what type of access is needed to exploit the said vulnerabilities. Due to difference of content of the two sources the results are presented accordingly.

4.1 National Vulnerability Database

A total of 104 search terms were used for extracting data from NVD, see table A.1 in appendix A. A total of 36 different vulnerabilities linked to computer systems in connected cars were identified. The 36 vulnerabilities were distributed over 17 distinct CWE categories with one vulnerability missing a CWE. Each unique vulnerability is counted once, though some vulnerabilities appear in multiple groups of devices and affect several manufacturers.

Table 4.1: A complete list of the CWE found in NVD

CWE ID	Description	Count
CWE-693	Protection Mechanism Failure	7
CWE-119	Buffer Errors	4
CWE-200	Information Leak / Disclosure	4
CWE-20	Input Validation	3
CWE-264	Permissions, Privileges, and Access Control	3
CWE-310	Cryptographic Issues	2

Table 4.1 continued from previous page

CWE ID	Description	Count
CWE-287	Authentication Issues	1
CWE-77	Command Injection	1
CWE-19	Data Handling	1
CWE-284	Improper Access Control	1
CWE-295	Improper Certificate Validation	1
CWE-347	Improper Verification of Cryptographic Signature	1
CWE-74	Injection	1
CWE-59	Link Following	1
CWE-306	Missing Authentication for Critical Function	1
CWE-798	Use of Hard-coded Credentials	1
CWE-327	Use of a Broken or Risky Cryptographic Algorithm	1
-	Unspecified	1

Table 4.1 shows a complete list of all the weaknesses which the found vulnerabilities are associated to and figure 4.1 shows the number of vulnerabilities reported per year.

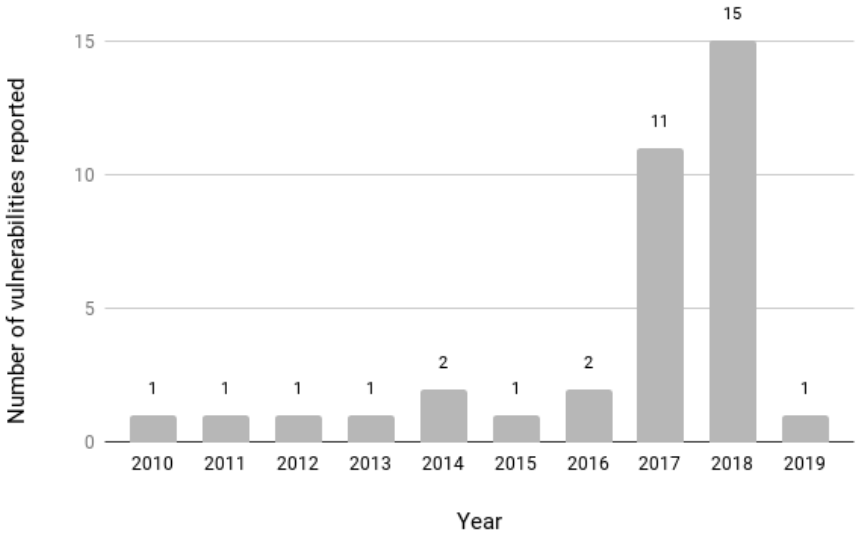

Figure 4.1: Total number of vulnerabilities reported per year

The searches based on car manufacturers alone (OEMs) resulted in 22 unique vulnerabilities from seven different brands. A total of 58 different car brands were examined of which the remaining 51 car brands had no information available in the database.

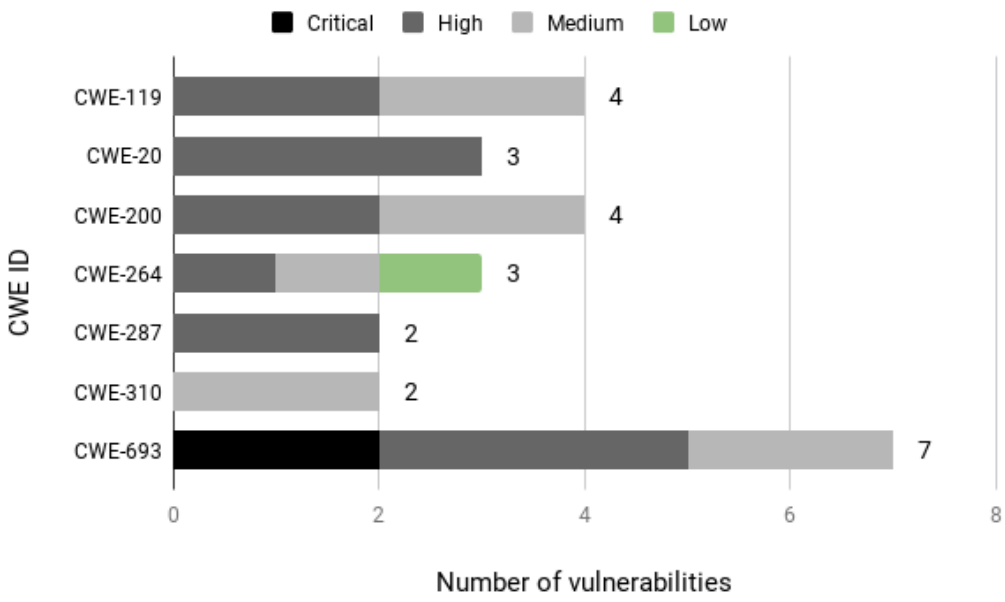

Figure 4.2: Distribution of vulnerability base scores over most common CWEs

4.1.1 Attack Vectors

The attack vector values from which a vulnerability can be exploited are shown in figure 4.3, where 37.8 % of the vulnerabilities can be remotely exploited through a network and 29.7 % through e.g. a short range network.

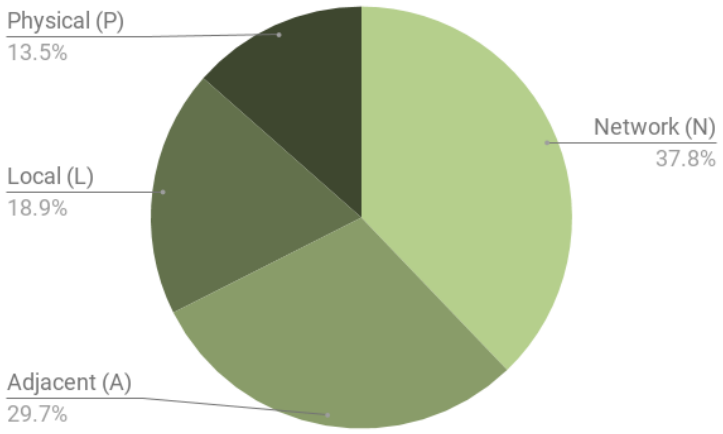

Figure 4.3: Distribution of attack vector values

Table 4.2: Attack vectors from vulnerabilities in NVD

Attack Vector (AV)	Count
Infotainment	10
Mobile app	8
CAN	8
TCU	5
Cellular network	4
USB port	4
Bluetooth	3
OBD port	3
Wi-Fi	3
Chip	2
OBD dongle	2
Servers	1
Gateway	1
Remote keyless entry system	1

Table 4.2 shows the attack vectors which could be identified from the reported vulnerabilities. Some of the attack vectors were combined in single vulnerabilities. This includes all vulnerabilities that were found.

4.2 Upstream Repository

A total of 187 vulnerabilities and exploits related to connected cars were collected from the Upstream repository. As mentioned in chapter 3, only reports of immediate impact on a car's system were collected.

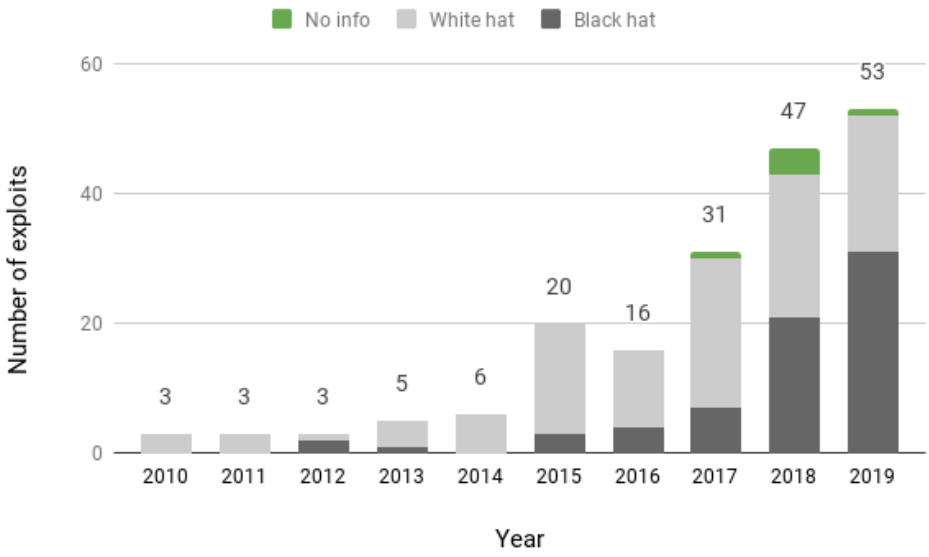

Figure 4.4: Total number of exploits reported per year

Figure 4.4 presents the entire collected data set, distributed over time and the origins of attacks (black hat/white hat).

4.2.1 Attack Vectors

A total of 25 unique attack vectors were identified in the collected data. The most prevalent ones can be seen in table 4.3 which shows the top half of the found attack vectors, with the number of times the attack vectors have been utilized in an exploit together with the origin of attacks. Several attack vectors may have been combined in single hacks. Table B.1 in appendix B shows the full list of attack vectors found.

Table 4.3: Top half of AVs used in exploits and their origins

Attack Vector (AV)	Count	Black hat	White hat
Remote Keyless System (RKS)	77	73%	25%
OBD port	27	19%	81%
Mobile app	22	14%	73%
Infotainment	21	5%	95%
Servers	16	19%	56%
Wi-Fi	12	0%	100%
Bluetooth	9	0%	100%

Table 4.3 continued from previous page

Attack Vector (AV)	Count	Black hat	White hat
OBD dongle	9	0%	100%
CAN bus	8	0%	100%
Sensors	8	12%	88%
Cellular network	7	0%	100%
USB port	7	0%	100%
ECU	6	0%	100%

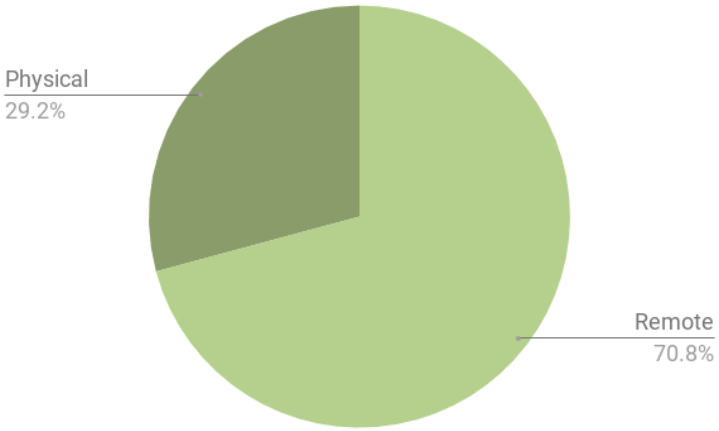

Figure 4.5: Remotely vs. physically exploitable vulnerabilities

Figure 4.5 shows the distribution between remotely versus physically exploited vulnerabilities, with remote attacks being 70.8 %. Remote includes both short range and long range connections.

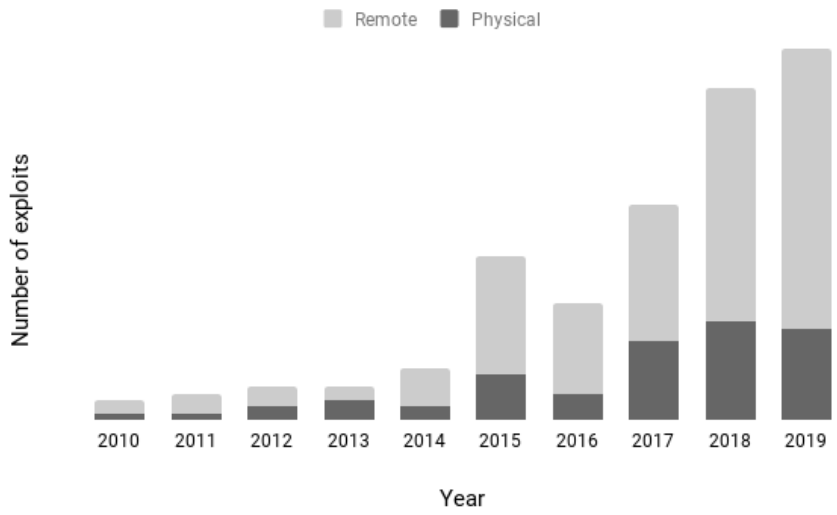

Figure 4.6: Remote vs. physical exploits per year

4.2.2 Impact

The attack vectors are presented with reported impacts in table 4.4. The table follows the same order as table 4.3, arranged by most frequently reported attack vector in descending order.

Table 4.4: Attack vectors and their reported impacts

Attack Vector (AV)	Impact
Remote Keyless System (RKS)	- Car theft - Theft of valuables in cars
OBD port	- Car theft - Data breach - Location tracking
Mobile app	- Car theft - Data breach - Control car systems - Theft of valuables in cars
Infotainment	- Control of car systems - Data breach - Location tracking - Malware

Table 4.4 continued from previous page

Attack Vector (AV)	Impact
Servers	- Car theft - Data breach
Wi-Fi	- Car theft - Control car systems - Location tracking
Bluetooth	- Control car systems - Data breach
OBD dongle	- Control car systems - Data breach - Location tracking
CAN bus	- Control car systems - Manipulate car systems

Chapter 5

Discussion

To answer the research questions a literature review was combined with a systematic review and collection of data from reported vulnerabilities. A vulnerability database was used (NVD) as well as a repository of automotive incidents from a security company (Upstream).

While NVD provides data of unique vulnerabilities which have been detected, the Upstream repository contains multiple counts of exploits which may involve the same vulnerabilities being exploited on several occasions. Upstream therefore provides an important additional aspect in regard to trends and the current state of connected cars.

Elements in the connected car anatomy which are affected when adding connectivity to a car are presented in the background, section 2.2. The overall results from the data gathered show presence of vulnerabilities in each of these presented modules, see table 4.2 in section 4.1.1 and table 4.3 in section 4.2.1. This can be explained by the extensive interconnection in the architecture of a connected car with few systems being isolated. It should also be noted that the presented attack vectors are not always isolated in exploits and that an attack path can consist of multiple vectors, also being a consequence of interconnectivity. When taking into account the most common type of weakness found in NVD, CWE-693 Protection Mechanism Failure [41], this could imply that overall sufficient protection mechanisms may be missing, such as isolation of systems based on security. This weakness also accounted for the most critical vulnerabilities, see figure 4.2.

The introduction of connectivity is in itself a significant factor of vulnerability. The vulnerabilities from NVD show that 67.5 % of the reported vulnerabilities can be remotely exploited (including short range and long range connection types, see figure 4.3). The Upstream results show similar numbers

with 70.8 % of vulnerabilities being remotely exploitable (see figure 4.5).

The Upstream data also shows the origins of reported exploits (black hat vs. white hat, table 4.3). These numbers only reflect the collected data and are unlikely to be a fully accurate description of reality. White hats, or security researchers, aim to actively report and bring awareness to their findings to help secure a system. Whereas exploits by black hats have other intentions and go unrecorded if they are not detected. These numbers do, however, show an interesting distribution between the different types of attack vectors. All types but one are dominated by white hat reports, the RKS.

The RKS and related hacks are presented in the background, section 2.2.5. An exploit of a RKS often results in a car theft or theft of valuables in cars (see table 4.4). While the numbers of RKS hacking incidents stand out in relation to the rest of the findings, it is important to emphasize that car theft has long been a persistent problem, and that there has been a significant decline in recent years [42]. New technologies have made it increasingly difficult to steal a car (e.g. tracking and remote disabling of a system) but have also introduced new ways of stealing. The remaining types of impacts which are presented are results of the technologies and therefore relatively new (e.g. remote control of car systems), with potential exploits possibly having other intentions than auto theft, an example being political motives.

Furthermore, it is interesting to comparatively analyze the results from NVD and Upstream. While the type of information provided is not equivalent between the two sources, they do contain several similarities. There are similarities in regard to the attack surfaces of vulnerabilities, and the majority of vulnerabilities being remotely exploitable as mentioned above. Both of the sources also display a trend over time with reported vulnerabilities continuously increasing, this can be attributed to the computerization of cars together with the increase of connectivity.

5.1 Limitations

Although a trend analysis of vulnerabilities in connected cars based on reports from NVD and the repository of Upstream is relevant within the given objective, there were a number of limitations that need to be addressed.

Firstly, the research based on NVD heavily relies on the keywords used to extract data. Even though an extensive pre-study was carried out to cover as many relevant vendors and technologies as possible, there is a risk of inaccuracy and misrepresentation in data based on the searches made.

The second issue related to the data from NVD is the question of transparency in the automotive industry. Not all manufacturers have a transparent approach in regard to public disclosure of vulnerabilities, resulting in few reported vulnerabilities. Certain brands and types of devices make up a larger portion of the data that was collected. This does not necessarily mean that they are more prone to having vulnerabilities, rather it points to a different business approach regarding vulnerability detection and disclosure.

An additional disadvantage of NVD is how some vulnerabilities are reported. Certain vulnerabilities occur in a wide group of devices, spanning across multiple industries but appear in the databases with only one entry and ID. This system does not manage to represent the full amplitude and impact of such a vulnerability.

The limitations of the Upstream repository were mainly linked to inconsistency. This refers to both the lack of information about the methods used by Upstream to monitor automotive incidents, and inconsistency in certain entries posted where common vulnerabilities sometimes have incorrect labels. The overall use of Upstream as a source is also debatable.

5.2 Future Work

The connected car is still in its early stages, a similar study would therefore also be of interest in a few years. Other suggestions for future work include research on the life cycle of modern cars. Systems require maintenance, for how long will cars continue to be patched by vendors? Another suggestion is to further investigate the possible risks of widespread industry standards, e.g. when a standard turns out to have a critical flaw, e.g. the CAN standard [18] or the Spectre/Meltdown hacks [43].

Chapter 6

Conclusions

The results clearly illustrate the significant impact of introducing connectivity to a car. The data retrieved from both sources show that vast a majority of the vulnerabilities related to connected cars can be remotely exploited with dire consequences.

The most common vulnerabilities found were related to the RKS (e.g. the SARA hack). Mobile applications, the infotainment system and the OBD port were also frequently used attack vectors. Due to the highly interconnected architecture of the system of a car, many of the attack vectors mentioned can be combined as attack paths to compromise systems. Exploits can result in car theft, data breach, control of car systems and location tracking. The most common types of weaknesses linked to these vulnerabilities were related to failure or lack of protection mechanisms, buffer errors and information leaks.

The results show trends both in regard to the interfaces used in exploits, as mentioned above, and in the growing number of vulnerabilities being reported per year as a result of the increasing number of connected cars. In conclusion, the automotive industry needs to continuously work on cyber security as an integral part of product development and maintenance. Standards need to be developed further, collaboration across industries must increase and the law must keep up with new technology to be able to target the challenges.

Bibliography

[1] TE Connectivity. *The Car in the Age of Connectivity: Enabling Car to Cloud Connectivity*. Sept. 2018. URL: https://spectrum.ieee.org/telecom/wireless/the-car-in-the-age-of-connectivity-enabling-car-to-cloud-connectivity.

[2] *Hyundai Blue Link | 3 Years Complimentary Blue Link*. URL: https://www.hyundaiusa.com/bluelink/index.aspx.

[3] Eric A. Taub. *Sleepy Behind the Wheel? Some Cars Can Tell*. Mar. 2017. URL: https://www.nytimes.com/2017/03/16/automobiles/wheels/drowsy-driving-technology.html.

[4] Argus Cyber Security. *Vehicle Hacking*. Jan. 2019. URL: https://argus-sec.com/car-hacking.

[5] Charlie Miller and Chris Valasek. "Remote exploitation of an unaltered passenger vehicle". In: *Black Hat USA* 2015 (2015), p. 91.

[6] Andy Greenberg. *After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix*. Jan. 2018. URL: https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/.

[7] Dana Hull. *Tesla Offers a Model 3 as 'Bug Bounty' for Anyone Who Can Hack Into It*. Jan. 2019. URL: https://www.bloomberg.com/news/articles/2019-01-14/tesla-offers-model-3-as-bug-bounty-for-cybersecurity-researchers.

[8] *General Information*. URL: https://nvd.nist.gov/general.

[9] *SMART MOBILITY CYBER ATTACKS REPOSITORY*. URL: https://www.upstream.auto/research/automotive-cybersecurity/.

[10] E. Uhlemann. “Introducing Connected Vehicles [Connected Vehicles]”. In: *IEEE Vehicular Technology Magazine* 10.1 (Mar. 2015), pp. 23–31. ISSN: 1556-6072. DOI: 10.1109/MVT.2015.2390920.

[11] *What’s driving the connected car*. Sept. 2014. URL: https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/whats-driving-the-connected-car.

[12] William Drier. *The Rise of Connected Vehicles Is Changing the Approach to Vehicle Maintenance*. June 2018. URL: https://www.navigantresearch.com/news-and-views/the-rise-of-connected-vehicles-is-changing-the-approach-to-vehicle-maintenance.

[13] A. Shaout, D. Colella, and S. Awad. “Advanced Driver Assistance Systems - Past, present and future”. In: *2011 Seventh International Computer Engineering Conference (ICENCO’2011)*. Dec. 2011, pp. 72–82. DOI: 10.1109/ICENCO.2011.6153935.

[14] *Autonomous and Connected Vehicles Face 300,000 Attacks Per Month, According to Karamba Security*. Jan. 2019. URL: https://karambasecurity.com/press/2019-01-08-autonomous-connected-vehicles-face-300000-attacks-per-month.

[15] J. Liu et al. “In-Vehicle Network Attacks and Countermeasures: Challenges and Future Directions”. In: *IEEE Network* 31.5 (2017), pp. 50–58. ISSN: 0890-8044. DOI: 10.1109/MNET.2017.1600257.

[16] Dietmar P.F. Möller and Roland E. Haas. *Guide to Automotive Connectivity and Cybersecurity: Trends, Technologies, Innovations and Applications*. eng. Computer Communications and Networks. Cham: Springer International Publishing, 2019. ISBN: 978-3-319-73511-5.

[17] Marco Di Natale et al. *Understanding and Using the Controller Area Network Communication Protocol: Theory and Practice*. eng. New York, NY: Springer New York, 2012. ISBN: 9781461403135.

[18] *The Crisis of Connected Cars: When Vulnerabilities Affect the CAN Standard*. Aug. 2017. URL: https://blog.trendmicro.com/trendlabs-security-intelligence/connected-car-hack/.

[19] Stephen Checkoway et al. “Comprehensive experimental analyses of automotive attack surfaces.” In: *USENIX Security Symposium*. Vol. 4. San Francisco. 2011, pp. 447–462.

[20] *Telematics and Networking*. URL: https://www.st.com/en/applications/telematics-and-networking/telematics-and-connectivity-control-unit.html.

[21] *Lex Access to European Union law*. URL: https://eur-lex.europa.eu/eli/dir/2014/45/oj.

[22] Eric Ravenscraft. *How to Make Your Car Smarter with an OBD-II Adapter*. May 2017. URL: https://www.howtogeek.com/304155/how-to-make-your-car-smarter-with-an-obd-ii-adapter/.

[23] *CVE-2016-2354 Detail*. URL: https://nvd.nist.gov/vuln/detail/CVE-2016-2354.

[24] Margaret Rouse. *What is passive keyless entry (PKE)? - Definition from WhatIs.com*. URL: https://whatis.techtarget.com/definition/passive-keyless-entry-PKE.

[25] David F. Oswald. "Wireless Attacks on Automotive Remote Keyless Entry Systems". In: *Proceedings of the 6th International Workshop on Trustworthy Embedded Devices*. TrustED '16. Vienna, Austria: ACM, 2016, pp. 43–44. ISBN: 978-1-4503-4567-5. DOI: 10.1145/2995289.2995297. URL: http://doi.acm.org.focus.lib.kth.se/10.1145/2995289.2995297.

[26] *Car industry declares victory in war on thieves*. June 2011. URL: https://www.bbc.com/news/uk-13787442.

[27] *Hundreds of popular cars 'at risk of keyless theft'*. Jan. 2019. URL: https://www.bbc.com/news/business-47023003.

[28] Jeffrey Cashion and Mostafa Bassiouni. "Robust and Low-cost Solution for Preventing Sidejacking Attacks in Wireless Networks Using a Rolling Code". In: *Proceedings of the 7th ACM Symposium on QoS and Security for Wireless and Mobile Networks*. Q2SWinet '11. Miami, Florida, USA: ACM, 2011, pp. 21–26. ISBN: 978-1-4503-0899-1. DOI: 10.1145/2069105.2069110. URL: http://doi.acm.org.focus.lib.kth.se/10.1145/2069105.2069110.

[29] Vince Tabora. *Signal Amplification Relay Attack (SARA)*. Aug. 2018. URL: https://hackernoon.com/signal-amplification-relay-attack-sara-609ce6c20d4f.

[30] *The National Vulnerability Database Explained*. Dec. 2018. URL: https://resources.whitesourcesoftware.com/blog-whitesource/the-national-vulnerability-database-explained.

[31] P. Johnson et al. "Can the Common Vulnerability Scoring System be Trusted? A Bayesian Analysis". In: *IEEE Transactions on Dependable and Secure Computing* 15.6 (Nov. 2018), pp. 1002–1015. ISSN: 1545-5971. DOI: 10.1109/TDSC.2016.2644614.

[32] *CVSS v3.0 Specification Document*. URL: https://www.first.org/cvss/specification-document.

[33] *Common Weakness Enumeration*. URL: https://cwe.mitre.org/about/index.html.

[34] S. Jafarnejad et al. "A Car Hacking Experiment: When Connectivity Meets Vulnerability". In: *2015 IEEE Globecom Workshops (GC Wkshps)*. Dec. 2015, pp. 1–6. DOI: 10.1109/GLOCOMW.2015.7413993.

[35] *Car Hack project Volkswagen/Audi*. Feb. 2019. URL: https://www.computest.nl/en/knowledge-platform/rd-projects/car-hack/.

[36] S. Strobl et al. "Connected cars — Threats, vulnerabilities and their impact". In: *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*. May 2018, pp. 375–380. DOI: 10.1109/ICPHYS.2018.8387687.

[37] T. Bécsi, S. Aradi, and P. Gáspár. "Security issues and vulnerabilities in connected car systems". In: *2015 International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS)*. June 2015, pp. 477–482. DOI: 10.1109/MTITS.2015.7223297.

[38] Margus Välja, Matus Korman, and Robert Lagerström. "A Study on Software Vulnerabilities and Weaknesses of Embedded Systems in Power Networks". In: *Proceedings of the 2Nd Workshop on Cyber-Physical Security and Resilience in Smart Grids*. CPSR-SG'17. Pittsburgh, PA, USA: ACM, 2017, pp. 47–52. ISBN: 978-1-4503-4978-9. DOI: 10.1145/3055386.3055397. URL: http://doi.acm.org.focus.lib.kth.se/10.1145/3055386.3055397.

[39] L. Allodi, W. Shim, and F. Massacci. "Quantitative Assessment of Risk Reduction with Cybercrime Black Market Monitoring". In: *2013 IEEE Security and Privacy Workshops*. May 2013, pp. 165–172. DOI: 10.1109/SPW.2013.16.

[40] *All Car Brands List and Car Logos By Country A-Z*. Jan. 2015. URL: https://www.globalcarsbrands.com/all-car-brands-list-and-logos/.

[41] *CWE-693: Protection Mechanism Failure*. URL: https://cwe.mitre.org/data/definitions/693.html.

[42] *Crime statistics*. URL: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Crime_statistics#Car_thefts_down_by_36_.25_between_2008_and_2016.

[43] Nael Abu-Ghazaleh, Dmitry Ponomarev, and Dmitry Evtyushkin. "How the spectre and meltdown hacks really worked". In: *IEEE Spectrum* 56.3 (2019), pp. 42–49. DOI: 10.1109/mspec.2019.8651934.

Appendix A

NVD Search Terms

Table A.1: Search terms used to extract data from NVD

OEM	MISC
ACURA	ADAS
ALFA ROMEO	AIRBAG
ALPINE	AIRBIQUITY
ASTON MARTIN	ANDROID AUTO
AUDI	AUTOLIV
BAIC	AUTOMOBILE
BENTLEY	AUTOMOTIVE
BMW	BLUETOOTH
BUGATTI	CAR
BUICK	CARLINK
CADILLAC	CARPLAY
CHANGAN	CONTROLLER AREA NETWORK
CHEVROLET	CRUISE
CHRYSLER	DELPHI
CITROËN	DENSO
DAIMLER	DRIVESYNC
DODGE	ECU
DONGFENG	ENFORM
FERRARI	FLEXRAY
FIAT	FREESCALE
FISKER	INFOTAINMENT
FORD	LEMUR
GEELY	LIDAR

Table A.1 continued from previous page

OEM	MISC
GENERAL MOTORS	MBRACE
GMC	MOBILEYE
GREAT WALL	MOST
HONDA	OBD
HYUNDAI	PANASONIC
INFINITI	PASSENGER
JAGUAR	PIONEER
KIA	QNX
KOENIGSEGG	RADAR
LAMBORGHINI	RENESAS
LAND ROVER	SAFETY CONNECT
LEXUS	SENSOR
MASERATI	SUNNY
MAZDA	TAKATA
MCLAREN	TELEMATIC
MERCEDES	TEXAS INSTRUMENTS
MITSUBISHI	TIRE
NISSAN	TPMS
OPEL	ULTRASONIC
PAGANI	VEHICLE
PEUGOT	VEONEER
PORSCHE	XILINX
PSA	ZUBIE
RENAULT	
ROLLS ROYCE	
SAAB	
SAIC	
SKODA	
SSANGYONG	
SUBARU	
SUZUKI	
TATA MOTORS	
TESLA	
TOYOTA	
VOLKSWAGEN	

Appendix B

Vulnerabilities

B.1 Upstream Repository

Table B.1: A complete list of the attack vectors found and their origins

Attack Vector (AV)	Count	Black hat	White hat
Remote keyless entry system	77	73%	25%
OBD port	27	19%	81%
Mobile app	22	14%	73%
Infotainment	21	5%	95%
Servers	16	19%	56%
Wi-Fi	12	0%	100%
Bluetooth	9	0%	100%
OBD dongle	9	0%	100%
CAN bus	8	0%	100%
Sensors	8	13%	88%
Cellular network	7	0%	100%
USB port	7	0%	100%
ECU	6	0%	100%
TCU	6	0%	100%
Gateway	4	0%	100%
GPS navigation system	2	0%	100%
Instrument cluster	2	100%	0%
Ignition keyhole	2	100%	0%
Immobilizer	2	0%	100%

Table B.1 continued from previous page

Attack Vector (AV)	Count	Black hat	White hat
Connected security and control system	1	0%	100%
Ethernet port	1	0%	100%
OTA update	1	0%	100%
CD player	1	0%	100%
Mechanics tools	1	0%	100%
Intelligent Transportation System (ITS)	1	0%	100%

TRITA-EECS-EX-2019:396