



Turun yliopisto
University of Turku

ANALYSIS OF AUTOMOTIVE CYBERSECURITY

Attack surfaces and users' privacy concerns

Master's Thesis
in Information Systems Science

Author (s)/Student number:
Saikat Asaduzzaman - 506681

Supervisors:
D.Sc. (Econ. & Bus. Adm.)
Matti Mäntymäki

30.04.2016
Turku



Turun kauppakorkeakoulu • Turku School of Economics

Table of contents

1	INTRODUCTION	7
1.1	Background and motivation	7
1.2	Research Gap	8
1.3	Study aim and research question	9
1.4	Research limitation and scope	10
1.5	Research strategy and structure	10
1.5.1	Research methods	12
1.5.2	Structure of this report	13
2	MODERN AUTOMOBILE'S ARCHITECTURE	14
2.1	ECU components	14
2.2	Controller Area Network Bus or CAN Bus	18
2.3	Potential vulnerabilities in CAN bus architecture	19
3	ATTACK TAXONOMY	21
3.1	Attack Phases	21
3.2	Attack surface	22
3.2.1	Indirect Physical	22
3.2.2	Short-range wireless access	23
3.2.3	Long-range wireless	24
3.2.4	Firmware-Over-The-Air (FOTA)	24
3.3	Attack methods	25
3.3.1	Data stealing	25
3.3.2	Control override	26
3.3.3	Vehicle degradation	26
3.3.4	Data falsification	27
3.3.5	External sensor attack	27
3.3.6	Attacking TPMS	28
3.3.7	Ethernet attacks	28
3.3.8	Attacking key fobs and immobilizer	28
3.3.9	Passive keyless entry and start	29
3.3.10	Keypad entry	29
3.4	Types of attack	30
3.4.1	Side channel attacks	30
3.4.2	Timing attacks	30
3.4.3	Fault injection and reverse engineering attack	31
4	RELATED WORKS	32
4.1	Related works on Intrusion Detection	32
4.2	Related works on Penetration Testing	34
4.3	Related works on Standards and Frameworks	35
4.4	Related works on Vulnerability analysis	38

4.5	Related works on Information Privacy	41
5	RESULT ANALYSIS	46
5.1	Information privacy	45
5.2	Attack surfaces	55
5.3	Awareness among consumers	59
6	CONCLUSIONS	62
6.1	Discussions on hypotheses	62
6.2	Future work	64
7	REFERENCES	65

List of figures

Figure 1: Finding the research gap for this thesis	8
Figure 2: Level of knowledge of privacy rights among Canadians from 2001 till 2014	9
Figure 3: The modified IUIPC scale from the original	11
Figure 4: Standard CAN packet	18
Figure 5: Extended CAN packer (Koscher 2014)	19
Figure 6: NHTSA Risk Management Framework	36
Figure 7: Comparison of GIPC, CFIP and IUIPC scale (Malhotra et al 2004)	44
Figure 8: Original IUIPC scale model (Malhotra et al 2004)	45
Figure 9: User responses: Question on Control 1	47
Figure 10: User responses: Question on Control 2	48
Figure 11: User responses: Question on Awareness 1	49
Figure 12: User responses: Question on Awareness 2	49
Figure 13: User responses: Question on Collection 1	50
Figure 14: User responses: Question on Collection 2	50
Figure 15: User responses: Question on Collection 3	51
Figure 16: User responses: Question on Errors 1	52
Figure 17: User responses: Question on Unauthorized personal use 1	53
Figure 18: User responses: Question on Improper access 1	53
Figure 19: User responses: Question on Global information privacy concern 1	54
Figure 20: User responses: Question on usage of Bluetooth	55
Figure 21: User responses: Question on usage of TPMS	55
Figure 22: User responses: Question on usage of In-built GPS/Navigator	56
Figure 23: User responses: Question on usage of DVD player/Music system	56
Figure 24: User responses: Question on usage of Lane changing assistance / Automatic parallel parking	57
Figure 25: User responses: Question on mobile phone integration	57
Figure 26: User responses: Question on usage of Third party devices	58
Figure 27: User responses: Question on awareness 1	59
Figure 28: User responses: Question on awareness 2	60
Figure 29: User responses: Question on awareness 3	60

List of tables

Table 1: Common Wireless network technologies in cars	16
Table 2: Comparison between different automotive protocols	17
Table 3: Attack surface capabilities	39

1 INTRODUCTION

1.1 Background and motivation

Automobiles these days are no longer mechanical tools; they are embedded computers running on wheels. The high demand of technologies by the consumers is pushing them to be more computerized each day. Nearly hundred percent of new cars have wireless technologies that are vulnerable to intrusion and lack privacy measures (Markey 2015, 3). The new technologies in cars are lucrative to use, they brought a large number of technological processes together and as a result opened numerous attack surfaces. Car security research gained a significant number of public attentions because most of the people owns a car and has clear idea of the damage it can cause if not functioned properly (Miller & Valasek 2015, 5). It is indeed a huge risk if a situation arises where a high speed car loses its brakes due to intrusions and alterations. A majority of the auto manufactures are unaware of such vulnerabilities and could not recall any hacking attempt in the past. Nevertheless they are collecting vast amount of data on car performance and driving history in order to improve the customer experience (Markey 2015, 14).

Since the invention of automobiles, cars were mere mechanical devices for almost eighty years, until sophisticated technologies are integrated to them (Koscher 2014, 26-29). Day by day the complexity grew and now it is believed that a recent car has an average of 100 million lines of software code (Charette 2009). According to Alfred Katzenbach, the director of IT management in Daimler, the radio and telematics of Mercedes Benz itself has more than 20 million lines of code. In this midst of codes, lie unknown vulnerabilities. The number of functionalities in automobile systems allows user to connect various devices such as mobile phones and iPods via networking technologies such as Wi-Fi, Bluetooth or near field communication (NFC). On top of that, it is also possible to connect a car to the cellular systems to get navigation data and even software updates. Tesla Motors already introduced a feature called Over-The-Air update where a user can connect his/her car to the home wireless network and is able to download any software update via the interaction module on the dashboard. When an update is available for a specific model of car, the center display will give the option to download it now or later. (Software updates Tesla Motors 2015.)

The tragic death of American journalist Michael Hastings in 2013 also brings back a lot of questions. Michael was killed in a car crash in California and there are many conspiracy theories behind his accident. Former counterterrorism adviser Richard Clarke mentioned that the attack might be an automobile cyber-attack and a similar demonstration was conducted by Defence Advanced Research Projects Agency (DARPA) in the United States. This was followed by the security and privacy report issued from the Senator Ed Markey's office and it was clear that the "Drivers are at risk". (Papenfuss 2015.) Although it was not confirmed that if Michael's car was actually hacked or not for the crash, but it shows that there is enough attack surface and opportunities for intruders to damage an automobile's infrastructure and anybody's fate can be like Michael if the attack surfaces are not mitigated properly. These attack surfaces and privacy findings motivated the author to perform his research on this area.

1.2 Research Gap

Comparing to other research areas in information systems, automobile vulnerabilities and privacies are a very new branch. Not many works have been done in the past and hence there is an ample rooms for research and development. The three most common areas which can be overlapped with this research topic are:

1. Consumer's privacy scale and model
2. Vulnerability analysis (including penetration testing) in automobile and embedded systems and
3. Possible solutions to mitigate the vulnerabilities in automobile systems.

This research looks into the vulnerabilities in automobile systems and analyses its attack surfaces. In addition to that, it seeks if the automobile consumer's privacy fits into any privacy scale and model. No work has been done yet in this topic and hence it elevates a research gap in the literature.

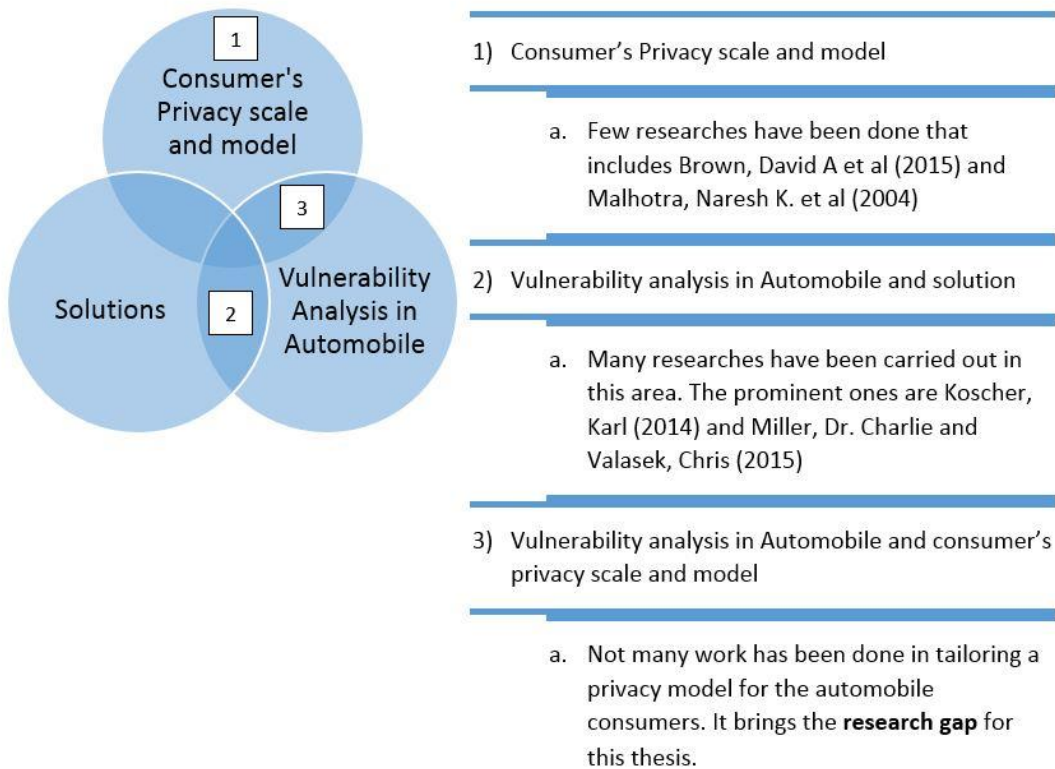
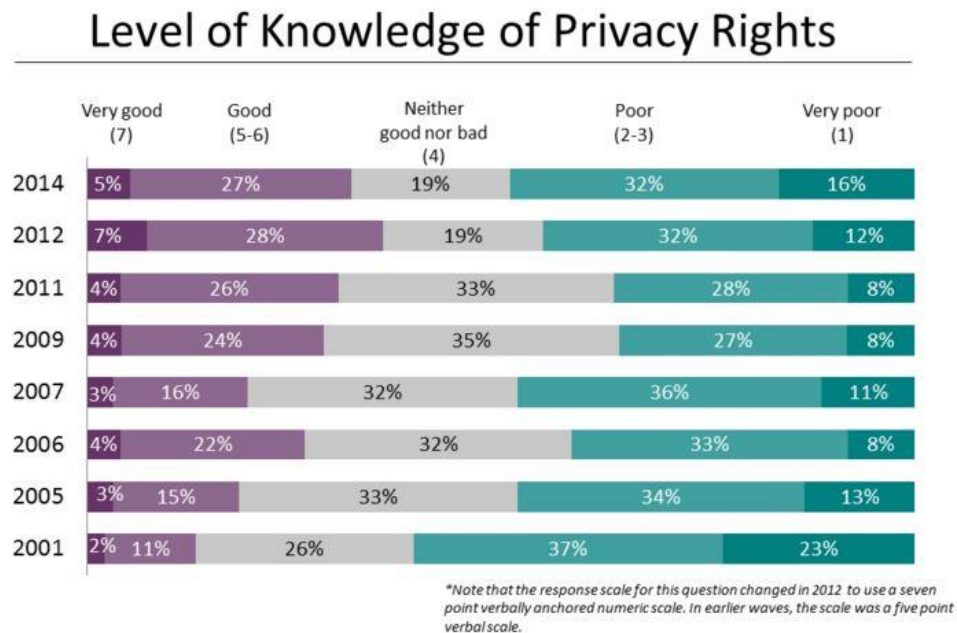


Figure 1 Finding the research gap for this thesis

1.3 Study aim and research question

This thesis studies the attack surfaces in an automotive system and seeks to find a proper privacy scale and/or model for the automotive consumer privacy. Measuring privacy is always been a difficult job in digital world as entities can be copied and reused several times, like in physical world. As for an example, a paper money is one entity and it holds its values which is related to one object. Whereas if there is a lack of regulatory bodies (or public ledger) for Bitcoins, it can be used many times with a same entity and value (Murphy – Murphy – Seitzinger 2015). On top of that public awareness towards consumer privacy has developed very recently. The below diagram about the level of knowledge of privacy rights among Canadians gives a good idea about other developed countries as well. It can be seen that in 2001 the good and very good knowledge of privacy rights were only 13% combined which is about 33% combined in 2014.



Q: How would you rate your knowledge of your privacy rights under the various laws protecting your personal information? (7-point scale)

Figure 2 Level of knowledge of privacy rights among Canadians from 2001 till 2014 (2014 Survey of Canadians on Privacy)

The research questions this thesis is aim to study are:

1. What are the attack surfaces and methods in automotive systems and network? How many of them are currently used by automotive consumers? (R1)
2. In which consumer's privacy scale and/or model do automotive consumer privacy falls? (R2)

This study is divided into two parts, the first part does an extensive research to answer R1 and the second part tried to tailor a known privacy scale model to match the automotive

consumer privacy preferences. An internet based survey was conducted using Google forms and 142 respondents were recorded. 20 questions were asked among the audiences and almost half of the questions were focused on the different technologies and appliances used by the consumers which have an attack surface. The rest of the questions were related to privacy in connected cars and were intended to match a known consumer privacy scale model.

1.4 Research limitation and scope

Automotive cybersecurity is a vast field with major opportunities to research. There can be a number of subcategories where the concentration could be given. But due to the time and resource limitation, the scope of this research has been determined.

This research has only performed a theoretical studies about the attack surfaces in an automotive network. Concentration and priorities has been given to controller area network or CAN Bus architecture as it is one of the most common one in cars today. CAN bus is a vehicle bus network that is used by the microcontrollers and devices to communicate to each other. No practical experiments has been done with the components of the cars. The privacy discussed in this research are solely consumer's privacy which are exposed (or maybe exposed) due to connected cars. Although the privacy part of this research has been tailored with the Internet Users' Information Privacy Concerns (IUIPC) privacy scale (Malhotra – Kim – Agarwal 2004) but the covariates of the original scales such as Sex, age, education, internet experiences are not included in this research. Although the solutions of automotive cybersecurity are touched briefly but only the attack surfaces, methods and privacy in connected cars are mostly discussed.

1.5 Research strategy and structure

A strategy is “a method or plan chosen to bring about a desired future, such as achievement of a goal or solution to a problem” (Business Dictionary 2015). It is the step by step plan to reach to a goal of fulfilling something. The strategy of this research is to study the attack surfaces and methods of automotive systems and infrastructure. After that, match the existing IUIPC consumer's privacy scale model with the privacy concern of the automotive consumers. Side by side there was a survey questionnaire to analyse and support the research.

The original IUIPC scale model was modified little bit to support the findings of this research. The covariates were excluded as they were the limitations of data collections. Besides that, the survey questionnaires are based on 5-point scale instead of original 7-point scale of IUIPC scale model.

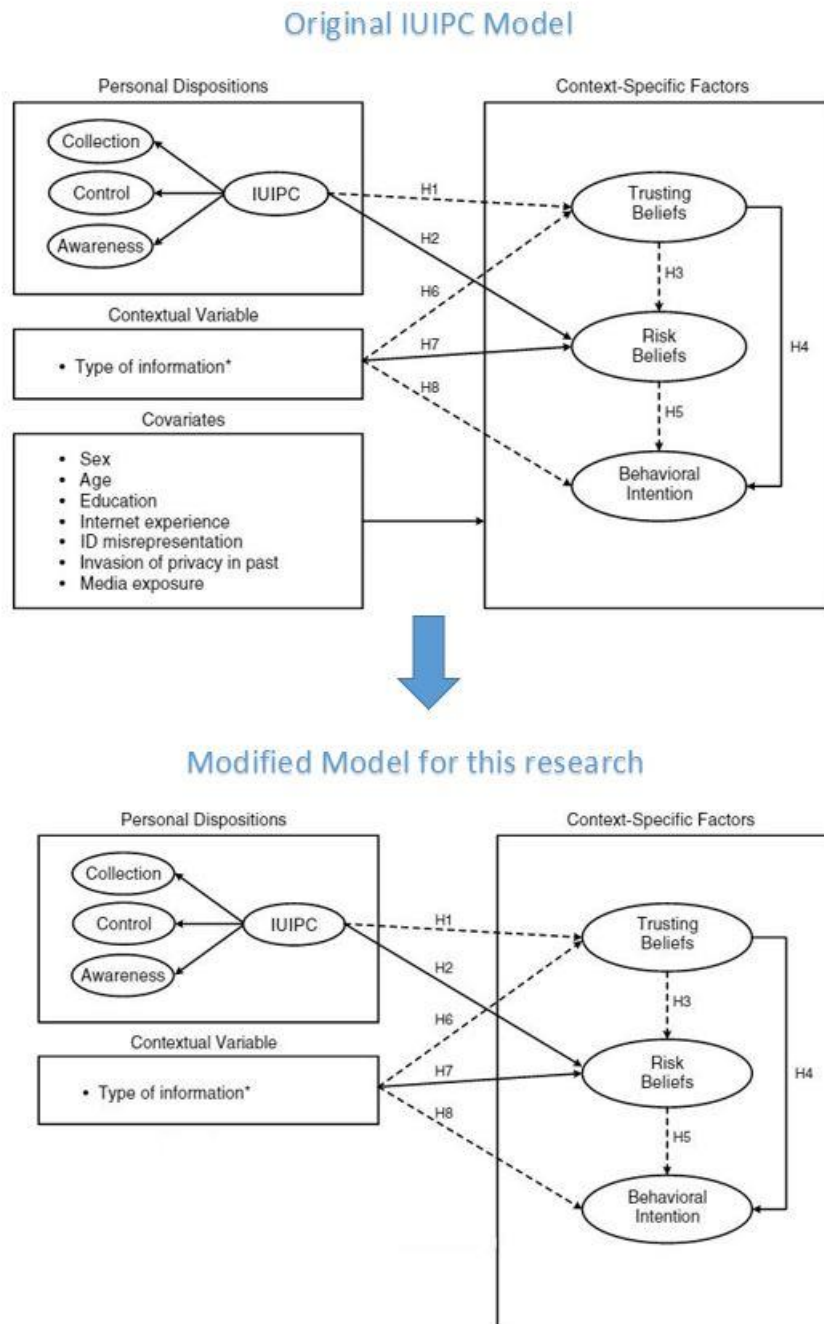


Figure 3 The modified IUIPC scale from the original (Malhotra et al 2004)

The hypotheses of original IUIPC scale model have also been altered to fit the consumers' privacy in automotive securities. Modification are made to tailor the original IUIPC model to blend with the privacy concerns of automotive consumers. The main modifications are changing the generalized "Internet users" to "Automotive users" and "marketers" to "automotive manufacturers and third parties". The IUIPC scale model is a good for this study because the hypotheses and privacy concerns in IUIPC are similar to the proposed research methodologies of this thesis. The modified hypotheses are:

Hypothesis 1: Automotive users' information privacy concerns will have a negative effect on trusting beliefs.

Hypothesis 2: Automotive users' information privacy concerns will have a positive effect on risk beliefs.

Hypothesis 3: Trusting beliefs will have a negative effect on risk beliefs.

Hypothesis 4: Trusting beliefs will have a positive effect on intention to reveal personal information.

Hypothesis 5: Risk beliefs will have a negative effect on intention to reveal personal information.

Hypothesis 6: An automotive manufacturer or third party's request for more sensitive information will have a negative effect on trusting beliefs.

Hypothesis 7: An automotive manufacturer or third party's request for more sensitive information will have a positive effect on risk beliefs.

Hypothesis 8: An automotive manufacturer or third party's request for more sensitive information will have a negative effect on intention to reveal personal information.

1.5.1 Research methods

The study of information system is a comparatively new field of applied science, it was only emerged in 1960s (Myers – Avison 2002). The substantial growth of information systems in the last half century has opened a lots of rooms for new researches and developments. Choosing a research method is indeed one of the most important factors for applied science researches (Bhattacharjee 2012). A proper research methods are needed that is well structured and has suitable ways for data analysis. The main two types of research analysis are Quantitative and Qualitative researches. The quantitative research analysis mostly deals with numbers, frequencies and try to figure out the quantitative value out of a system. It is a statistically reliable results which can be generalizable as well. A problem is viewed and quantified according to the analyzed data. On the other hand, qualitative research analysis mostly focused on the quality of the data and depends on exploratory research. The insight of an applied issue is studied in order to uncover social and cultural phenomena (Pickard 2012). The philosophical perspective of qualitative research is the "assumption of knowledge and how it can be obtained" (Myers et al 2002). Generally hypotheses are assumed and studies are done to conclude in either accepting or rejecting the hypotheses. There are many philosophical perspective of qualitative researches, one of them is Positivist research. Positivist research usually assume that "reality is objectively given and can be described by measurable properties which are independent of the observer (researcher) and his or her instruments." (Myers et al 2002).

Positivist research observes the social phenomena and view of reality in order to deduce generalized patterns (Bhattacharjee 2012). The popular positivist methods are laboratory experiments and survey researches. Positivist research is an increasingly common research method in information systems literature and it is efficient to build a process oriented phenomenon. This research uses positivist research methods to perform its analysis. Survey analysis are done through online survey as a tool for data collections.

1.5.2 Structure of this report

The structure of this report is divided into chapters. The elaboration of the chapters are explained below:

Chapter 2 Modern automobile's architecture: The internal architecture of automobile systems are explained here. The architecture of network packets, infrastructure are also studied in detail. The word "automotive", "automobile" and "car" have been used interchangeably.

Chapter 3 Attack taxonomy and phases: The attack surfaces and various methods are studied in this chapter.

Chapter 4 Related work: Researches and related work of automotive cybersecurity are explored in this chapter.

Chapter: 5 Result analysis: The survey results in this research are studied into three sections 1) Information privacy 2) Attack surfaces 3) User awareness.

Chapter 6 Conclusion: This chapter discussed and validated the hypotheses of this research and concluded its goals.

2 MODERN AUTOMOBILE'S ARCHITECTURE

Since the beginning of car production until 1970, the electronic components in cars were very limited to the spark plugs and radio systems. The major functions and operations were mainly mechanical processes (Vyleta 2014). The Clean Air Act was introduced in 1970 where electronics were introduced in order to design an efficient combustion system. The Clean Air Act was looking for lower emission engine and as a result the carburetors were quickly replaced by Electronic Fuel Injection (EFI) engines with more effective combustions (Rogers 1990). The combustions were effective because electronic control units (ECU) can adjust the fuel/oxygen mixture before combustion in an efficient way (Koscher 2014). Thus the era of car computerization began. Today most of the old mechanical systems such as steering control, anti-lock braking systems or parking brakes are replaced by drive-by-wire. It is a process of transforming mechanical linkages in cars into a form of electromechanical systems (Wolf – Weimerskirch – Paar 2004). Safety was expanded in drive-by-wire after the introduction of different car features such as Electronic stability control, parking assistance and adaptive cruise controls.

The in-vehicle network architecture can be compared with a SCADA (Supervisory Control and Data Acquisition) system (Carsten – Andel – Yampolskiy – McDonald 2015). This kind of system collects and monitors data from a number of sensors and use a control unit to process it. These control units are alternately called electronic control units or engine control units (ECUs). A typical car can have about 50-70 ECUs depending on the number of functionalities it offers (Nilsson – Phung – Larson 2014). Each ECU is responsible for its own functionality that varies from controlling the washer fluid to apply adaptive braking in cruise control when there is an obstacle in front.

2.1 ECU components

An ECU is a printed circuitry which has many electrical components run by firmware (Prathap – Rachumallu 2013). The ECU can be compared with modern desktop computers as they both have similar basic components. ECU has input and output functionalities and it sends or receives data from sensors or actuators. The sensors convert the physical and mechanical data such as temperature and speedometer readings into electronic forms that can be read by the ECUs. On the other hand, actuators do the opposite. It receives data from the ECU and converts them to mechanical reading that is understandable by the respective components in the vehicle. The processor speed in an ECU is lesser than a desktop computer. Typically it can have a 32 bit 40 MHz processor cable capable to perform its functionalities. If we compare the processing capability of this processor with a desktop computer, it will be much lower and cheaper as well. Since each ECU has their own tasks unlike central processing units in desktop computers, they are able to work efficiently with less power. There are two types of memory in a typical ECU, a flash memory and a RAM memory. (Prathap et al 2013.) The flash memory is non-volatile where the RAM memory is not. Anything stored in flash memory will stay when the ECU

is powered off whereas the contents in RAM memory will be erased. The bootloader also has two parts, a primary bootloader (PBL) and a secondary bootloader (SBL). The flash memory cannot be overwritten as it has the PBL which is necessary for starting up the ECUs. When an ECU is powered on, the PBL is executed to load the SBL into RAM memory. Then the RAM memory is used to modify any program code in the ECUs.

All of these ECUs inside a car use some kind of communication system or bus to transfer data between each other (Koscher 2014). This networked system also varies from each other, there can be proprietary buses as well as non-proprietary with different designs and specifications (Koscher 2014).

Local Interconnect Network (LIN): LIN protocol was designed to be a low cost, low powered network for task that are not mission critical to the system. It was first specified in 1999 and it was the “silicone implementation based on common UART/SCI interface hardware” (LIN Consortium 2006). It is a single wire subnetwork which mostly depends on the Controller Area Network (CAN). LIN is much cheaper to implement and used for processes where other heavily network such as CAN is not fully required. LIN is capable to have collision free communication to maximum of 16 hosts using its single master mechanism. The validations of the LIN packets are set by its parity bits and checksum. LIN can go to sleep mode when necessary and hence saves on power. LIN has an average data rate of 20 kilobit per second.

Controller Area Network (CAN): It is one of the most popular standards used in most of the cars and also one of the oldest protocol. With the ability to transfer data with a rate of up to one megabit per second, CAN is an event triggered serial bus system (Prathap et al 2013). CAN was first published in 1986 by Robert Bosch GmbH (Vyleta 2014). It was designed with reliability in mind and it can also work when some nodes are defective due to its multi-master architecture. Error protection is done using cyclic redundancy check and also by using the parity bits. An addressing scheme is not used in CAN protocol, however it works on broadcast mechanism. CAN packets are broadcast to all the nodes and the appropriate node acts accordingly by examining the message type. Packets with high priority are sent and they are processed with urgencies, and hence CAN is most suitable for critical systems such as brakes and steering.

Media Oriented Systems Transport (MOST): This is a high speed serial bus mainly used for transmitting multimedia such as audio and video inside the car. Due to the heavy load of multimedia and control data, the transfer speed of this bus is high as well. It has the capability to transfer a rate of 24 Megabit per second for synchronous and 14 Megabit per second for asynchronous transmission. Unlike CAN packets, the MOST packets contains both the sender’s and receiver’s information. MOST uses either a ring, star or bus topology which can connect up to 64 plug and play devices. (Prathap 2013.)

FlexRay: Originally developed by joint effort of BMW and DaimlerChrysler, the development of FlexRay was started in 2000 and was supposed to be the successor of CAN bus. It is an error tolerant and reliable high speed but which was standardized as ISO 17458 in 2013 (Vyleta 2014). It has speed of 10 megabit per second and robust enough

to handle safety critical situations with its redundant mechanism. The error tolerance is guided through channel redundancy, checksum calculation and independent bus guardian to minimize logical errors (Prathap et al 2013). Time division multiple access (TDMA) method is used in FlexRay for handling the priority in various transmission. TDMA is a mechanism to slice up a single channel into time slots and each time slot is used to transmit a portion of the data in logical format (Frenzel 2013).

Ethernet: Ethernet is one of the most popular protocol in computer networking and now has been used in cars too. The first car with Ethernet based parking camera was present in BMW X5 in 2013 (Yoshida 2013). A direct comparison of Ethernet protocol can be done with MOST as both of them operates in the Open Systems Interconnection layers and Ethernet said to be much efficient (Vyleta 2014). Ethernet is an established protocol which is also 100 times faster than CAN bus (Sauerwald 2014) but still it was not a lucrative options for the automakers due to its limitations. It was unable to meet the requirement of automotive market, especially the OEM EMI/RFI (Automotive Ethernet: An Overview 2014). A standard achieved through proper shielding and filtering (Lish 2015). Ethernet has too much latency and is susceptible to radio frequency noises from its own and also from other devices.

Wireless: Wireless networking protocols has been readily used in modern cars in various ways. It is possible to pair mobile phones to cars via Bluetooth technologies. Tire pressures can be displayed on the dashboard in real time via near field communications (NFC). Even the modern cars can be locked/unlocked or remotely start via wireless fobs. The wireless protocol and technology used varies and so does the properties. Recently an important concept in wireless technology has been developed, which is known as C2X, which can be categorized to C2C (car to car) or C2I (car to infrastructure) communication (Drive C2X). It is believed that by creating an ad-hoc network between cars will help to safeguard the cars and make them more efficient. It is to be note that most of the consumer electronics and entertainment system in modern cars operate based on wireless technologies. A comparison of these wireless network technologies are shown in the following table:

Table 1 Common Wireless network technologies in cars (Vyleta 2014)

Technology	Purpose	Range
Tire Pressure monitoring systems (TPMS)	Safety and convenience	Meters
Bluetooth technology	Entertainment	Meters
Keyless entry system	Comfort, security	Couple of meters
Wi-Fi	Entertainment	Couple of meters
3G	Entertainment, navigation	Unlimited

Table 2 Comparison between different automotive protocols (Prathap et al 2013)

Bus / Network	LIN	CAN	FlexRay	MOST	Ethernet	Wireless
Suitable for	Low level Subnets	Soft Real time	Hard Real time	Entertainment systems	Soft Real time	External communication
Application example	Door locks, power windows, sunroof control	Engine control, automatic parking	Steer-by-wire, Emergency systems	Navigation, Information services	Back camera	Bluetooth phone integration, Wireless Hotspot
Architecture	Single-Master	Multi-Master	Multi-Master	Multi-Master	Multi-Master	Multi-Master
Transfer mode	Synchronous	Asynchronous	Synchronous and Asynchronous	Synchronous and Asynchronous	Synchronous and Asynchronous	Synchronous and Asynchronous
Data rate	20 kBit/s	1 MBit/s	10 MBit/s	24 MBit/s	Usually 100 MBit/s for cars. Highest is 100 GBit/s	Varies. For Bluetooth: 720 kBit/s
Redundancy	None	None	2 channels	None	None	Varies. For Bluetooth: 79 frequencies
Error protection	Checksum, parity bits	CRC, parity bits	CRC, bus guardian	CRC, system service	CRC, checksum, parity bits	CRC, FEC
Physical layer	Single-wire	Dual-wire	Optical fiber, dual-wire	Optical fiber	Single/Dual-wire, optical fiber	Air
Key features	Low cost and weight	Reliability	Speed, reliability	Speed	Speed, lower cost and weight	Wire free, easy to use
Introduced Standard	1999 ISO 17987	1986 ISO 11898	2006 ISO 17458	2005 -	1980 IEEE 802.3	1994 (Bluetooth) IEEE 802.15.1

2.2 Controller Area Network Bus or CAN Bus

Although there are a number of protocols to implement on vehicle bus, but starting from 2008, all cars sold in U.S. are required to have CAN bus architecture (Koscher 2014). Ultimately most of the dominant automakers such as BMW, Ford, GM, Honda, and Toyota gradually shifted to CAN bus and hence it is the most common bus architecture present in cars today. The CAN packets used in CAN bus has certain properties that might be similar to transmission control protocol (TCP) or internet protocol (IP) packets. Two types of CAN packets are standard and extended packets.

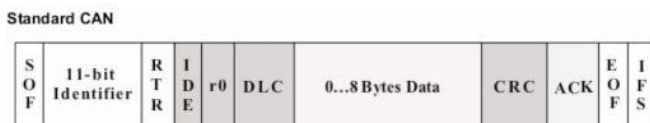


Figure 4 Standard CAN packet (Corrigan 2008)

The packet consists of segments with different purposes:

Start of frame (SOF): The start-of-frame header, it is 1 bit.

Identifier: This identifier is used to prioritize the packet, the lower the value, the higher is the priority. Moreover it is indicate which ECU can process the information. It is 11 bit in length.

Remote transmission Request (RTR): Although the packet is distributed to all ECU nodes, this RTR bit indicates when an information is required from a specific node. It is also 1 bit.

IDE (short for identifier): It is a single bit that distinguishes between a standard and extended CAN packet (Carsten et al 2015).

R0: This is also a single bit which is currently not in use, it is reserved for future use.

Date Length Code (DLC): This is a 4 bit segment to indicate the length of the data to be transmitted.

Data: the actual data to be transmitted. It can be up to 8 bytes (64 bits) in length.

Cyclic Redundancy Check (CRC): This 16 bit segment is used to validate the packet and contains the checksum value.

Acknowledge (ACK): Initially this 2 bit segment is set to zero. The receiving node check for errors in the packet and if it is error free, then ACK bit is flipped to one.

End of frame (EOF): The end of frame flag is 7 bit long. It is also used to identify bit-stuffing.

Inter-frame space (IFS): the flag represents the time which the controller used to move the frame into the buffer, it is usually 7 bit long.

The extended CAN bus packets come with a 29 bit identifier flag instead of the 11 bit standard identifier. The rest of the bits are used for an alternate version of RTR and extra space for the identifier (Carsten et al 2015). A sample extended packet is shown below (Koscher 2014).

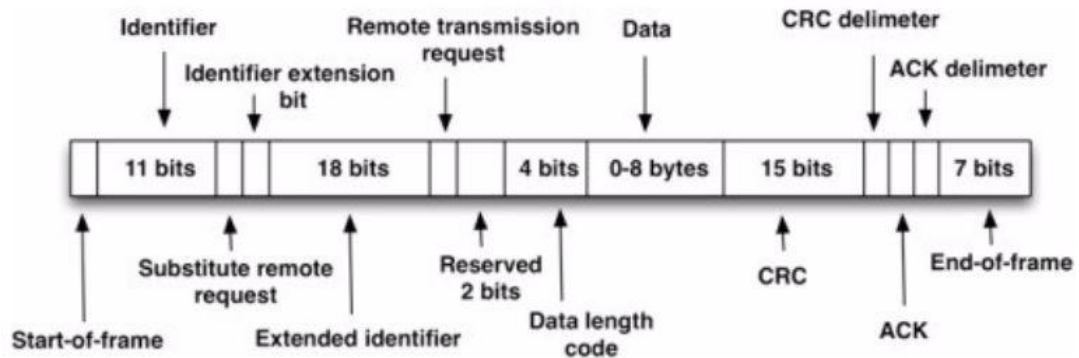


Figure 5 Extended CAN packer (Koscher 2014)

2.3 Potential vulnerabilities in CAN bus architecture

CAN bus has a number of weaknesses that was inherited from its earlier versions. Some of the common vulnerabilities are discussed below.

CAN packets are broadcast in nature: CAN protocol works in a broadcast manner. When a packet needs to be send to any of the ECUs, it is send to all of the nodes and the specific node accepts it and the rest drops it. It gives room for the malicious attackers to snoop CAN packets if somehow the attacker becomes part of the network where the packets are send in. After capturing live packets from the network the attacker can reverse engineer and retrieve further information to portray his attack.

Vulnerable to Denial of Service: CAN bus are very vulnerable to denial of service attacks. If a flood of high priority packets are send it can push a node to act “dominant” and hence other nodes will back off and service denial will occur. (Koscher 2014.)

Lack of authenticator fields: Another disadvantages of CAN packets is the lack of authenticator fields in the packets. It is not possible to know the sender's address and hence any nodes can send any packets to any other nodes, including nodes that are compromised by attackers. Thus an attacker has the ability to spoof a packet and disguise the destination ECU.

Weak access control: One of the pillars in information security is confidentiality and access control is a major part of it (Smith 2015). There is no legitimate access control for CAN bus and it is very easy to access it via On-board diagnostics with the help of special

tools. However there are challenge response mechanism for re-flashing the ECU and for memory protection (Koscher 2014).

3 ATTACK TAXONOMY

Common terms are needed in computer and network security to understand a same scenario. Howard et al. introduced a set of terms that can be used seamlessly to describe attack scenarios. These are general terms to structure an incident in a logical manner. A typical attack consists of Tools, Vulnerability, Action, Target and Unauthorized results. (Howard & Longstaff 1998) The tools are the software, application or instruments used by attacker to exploit the vulnerabilities in an automotive system. Vulnerabilities are the flaws and weaknesses that are present in a system and which the attackers take advantages. Actions are the process or steps taken to exploit those vulnerabilities and it is usually directed towards the target. Target is the victim or subject of the attack and unauthorized results are the outcome of a successful attack and the fruits of the whole process (Prathap et al 2013). On top of that there are two more keywords used to distinguish an attack, they are events and incidents. An event is a single activity or state of change in a system and a group of events can be categorized as an incident. An attack happens when there is an incident towards a target using tools to exploit its vulnerability to outcome unauthorized results.

3.1 Attack phases

Cyber-attack can be categorized into seven phases according to InfoSec Institute (Stoneff 2015). Automotive networks are somewhat similar and can also be expressed into same phases:

Reconnaissance: This is the initial phase where an attacker set a target and start gathering information about the system. It can be visual observation of the system or trying to connect to the system, getting reply back from the system and analysing the results. The attackers tries to get as much information as possible about vulnerable areas of the car such as open ports, outdated software etc. Various monitoring tools are used hook into the car system and analyse the data packets.

Scanning: This is the phase where the attacker already set the target and in the process of infiltrating the system. Vigorous scanning tools are used to find open ends to the system. Different vulnerability tools are used to penetrate vulnerable entry points in the car. Usually this process takes time as an attacker might have limited time to get exposed to a vehicle to try its scanners.

Access and Escalation: In this phase the attacker already identified the weakness in the system and now trying to break into it. He may use rainbow table or similar tools to brute force and gain access through the vulnerable entry point(s). The hacker would like to have privileged access so that he has the freedom to move around and alter things. When the attacker has the privileged access to a system, it can be said that the system is “owned” by the attacker. Owned (also written as poned or pwned) is an urban slang used in hacker and gamer community to get control of a device against one’s will (Gil 2013).

Exfiltration: At this phase the attacker has privileged access to the car system and hence he is able to hop in from network to network. The attacker now can extract private data about the car and the driver as well as analyse and reverse engineer CAN Bus packets for further attacks.

Sustainment: The attacker also needs to hide himself from getting exposed. In this phase the attacker configured a stealth process to access the car network from time to time and also not getting noticed by the user. He may also configured multiple access points to enter to the car's network.

Assault: This is the phase where things get nasty. Maliciously tailored CAN Bus packets are pushed into the system that may result in catastrophic outcomes. The driver may experience denial of services, malfunctioning of the devices at motion that can result in life threatening accidents. The assault and damage done to a car system can vary in various ways depending on the motto of the attacker.

Obfuscation: This is the last phase where the attacker tries to hide his identity. This is done by erasing the traces or footprints the attacker made in the last few phases. The reason behind it is to spoof the forensic personnel to trace back to the attacker. Sometimes the attacker wants to know the victim of its art and can leave traces intentionally as tokens. It is called "calling card" which is used to boast about the ability to own a system and exploit it.

3.2 Attack surfaces

Attack surfaces or attack vectors are the number of ways an attacker can get into a system. It is described as all the different gateways attackers can get data out of the system (OWASP 2015). In modern automobiles, the attack surface is broad as there are several physical devices which are either directly or indirectly connected to the internal systems of a car (Checkoway - McCoy - Kantor - Anderson - Shacham - Savage - Koscher - Czeskis- Roesner - Kohno 2011).

3.2.1 *Indirect Physical*

The most straightforward approach is using the OBD-II port (Carsten et al 2015). On-Board diagnostic or OBD has been introduced in early seventies for manufacturers to connect electronically to the engine and later in mid-nineties the more sophisticated version, OBD-II was introduced. OBD-II is a universal access port and it is widely used to check if a car is maintaining its OEM standard for emission. The port is located right at the bottom of the steering wheel. All cars which are built after January 01, 1996, should supposed to have an OBD-II port. (OBD-II Home page 2011.) When a car is taken to a service station, this port can be commonly used by the mechanic or other service person-

nel such as customer service representatives or helpers. Hence a full physical attack surface exist within the OBD-II ports. Few years ago it was still specialized handheld tools which were needed to access these OBD-II ports. Technicians would use tools like Ford's NGS or Nissan's Consult II to diagnose the car via the OBD-II port (Checkoway et al 2011). But a PC-centric trend has been going on since then and there were a tendency for connecting personal computer at ease with the ports. Nowadays the modern vehicle can be connected to computers via the OBD-II ports with the help of specialized software. These software are specially written to analyse data from the ports in order to diagnose it efficiently. Usually the port does not have a safety cap or lock and it can be readily available for anyone who has access to the car for a shorter time. It is possible to attach a third party device to the OBD-II port unnoticed and transmit CAN Bus packets to an intruders' destination.

Another physical attack surface for the modern cars is the entertainment system. Almost all of the cars have some sort of entertainment functionalities that allows user to play an audio disc, connect mobiles phones or iPod to the system and play music from there. There is possibility for attacker to disguise a user with CD encoded with malware instead of music. Hence when the user plays it into his system, the entertainment system can be corrupted. Although a compromised audio system can be considered as limited threat but the overlapping of vehicles network architecture always keeps an open door for attacker to infiltrate further.

3.2.2 *Short-range wireless access*

Although Bluetooth is considered to be the mostly used wireless access technology in automobiles (Checkoway et al 2011) but there are few others which are used almost equally. The common ones are the remote keyless entry, RFID, tire pressure monitoring systems (TPMS) and Wi-Fi. Most of the manufacturers are shipping modern cars with remote keyless entry. It allows the user to lock, unlock cars from a short distance. Some cars also has remote start ability which comes in handy during winter times. There are RFID enabled car keys which even do not need a button to push. The car will automatically unlock itself when the user comes to a close proximity to the car. The TPMS uses external sensors inside the tire to monitor and send tire pressures and has the ability to communicate with the vehicle's internal systems. Short ranged 802.11 Wi-Fi has been introduced by BMW earlier to monitor its backup cameras (Murray 2013) and more and more manufacturers are planning to embed Wi-Fi as well. Wi-Fi hotspot has been offered by major manufacturers that would allow users to bridge its 3G data link to be used as a Wi-Fi hotspot inside the car. Ford offered this capability in its Ford Focus back in 2012 (Checkoway et al 2011). A not yet fully implemented technology known as Dedicated Short Range Communications (DSRC) is also been developed which will actively support the vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) from safety point of view (Walton 2015). DSRC is a two-way short to medium range communication which

has the ability to transmit data in a very fast pace. If the external nodes for these entertainment systems are not guarded well, then there can be possibilities to compromise a system and traverse to the core vehicle system and plot damage.

3.2.3 Long-range wireless

Modern vehicles are also equipped with long-range wireless communication technologies which usually has a range of more than a kilometer. Those technologies can be categorized into two types: broadcast channels and addressable channels. Broadcast channels are more generic in nature and they are not focused on particular vehicles, but they can be “tuned into” by receivers if needed (Checkoway et al 2011). If a broadcast channel is compromised, then there is the possibilities of mass infections of a number of cars at a given time. A typical use of broadcast channel technologies can be using auto manufacturer provided Global Positioning System (GPS), satellite radio or Traffic Message Channel (TMC). Although the range of these signals absolutely depends on the power of the transmitter but an average range of a 1.2 kbps signal can come with a range of up to 10 km. This gives the attacker a safer and wider area to carry on an attack and not get caught. Addressable channels are more customized and there is a dedicated connection with continuous connectivity between a provider and a vehicle. These channels can be used for more personalized services such as sending crash reports to service providers, remote shutdown of the car engine in case of theft, and convenience such as hands free and driving directions. Popular remote telematic systems that use addressable channels are Ford’s Sync, GM’s OnStar and Chrysler’s UConnect.

3.2.4 Firmware-Over-The-Air (FOTA)

The car industry is going forward to the same direction as the mobile phone industry, which encountered it thirteen years ago (Red Bend Ltd 2011). The increasing number of software maintenance and the demand of amending the firmware is pushing the industry towards faster, efficient and reliable methods. Over-the-air (OTA) technologies has been used in mobile phone industries since the last decades and is getting its attention towards the automotive industries due to its quicker and simplistic ways of reducing the warranty cost for the manufactures, increase the number of software recalls in a given amount of time and also increasing the customer satisfactions (Bird 2016). When the updates are installed over the air, the manufacturers do not need specialized tools and dedicated personnel for serving a single car. Sometimes over the air updates can be setup for multiple number of cars at the same time. Thus an Auto manufacturers can service more vehicles in a shorter time during the process of a software recall. Hence customers have to spend less time in the service stations. Firmware are the set of instructions or programs specialized to run a hardware device, mostly an embedded system (Tech Terms 2016). Firmware-over-the-air is a method which is yet to be popular in the automobile industry but it is

the idea of updating or upgrading the ECUs firmware over the air i.e. without any physical touch with a device. FOTA works in three stages of updates, 1) Generating the update, 2) managing and delivering of the update and 3) performing the update (Red Bend Ltd 2011). In the first stage, based on the vehicle identification number (VIN), the required update is sorted out. Then a connection is established between the vehicle and the computer in the service center, the update is transferred to the car via wireless technology and then the update is verified for errors. The last stage is the update being installed in the car systems and the system restarts with the new updates. Audi, BMW and Tesla has been announced to update the in-built navigation systems over the air, Hyundai and Ford already has proof of concept for over the air updates. Infotainment software application has been already in the process of OTA by quite a few manufacturers. And estimated of 1.3 million vehicles has been released in 2015 which has the ability to update infotainment systems over the air and professionals are expect this number to increase to 17.6 million by 2022. (Bird 2016.) Telematic control units such as General Motor's GM OnStar and Verizon's telematic systems (available in many cars in the US) has the capability to get update over the air. Updating the core ECU is still in the process of acceptance by most of the automotive manufacturers but Tesla already has it in place. Tesla model S regularly receives software update over the air and it takes approximately 45 minutes to complete (Tesla Motors 2016). Although OTA and FOTA bring convenience and efficiency in the automotive industries but it also opens up a wider range of attack surfaces for the modern connected cars. There can be numerous possibilities to attack in over the air technologies if they are not secure enough.

3.3 Attack methods

3.3.1 Data stealing

The basic and easiest attack that is possible on an automotive network is data stealing (Carsten et al 2015). CAN bus architecture is broadcast in nature and hence the CAN data packets are send to each and every node in the vehicle network. The expected node will accept it and the rest will discard the packet. It gives the opportunity for any compromised host to listen to every packets in the network and get necessary information and pass it to the attacker. Insurance company such as The Personal and Desjardins are offering an app called Ajusto will can be installed in one's cell phone and can monitor the driving behavior. Before the insurance company used to offer a device that can be attached to the OBD-II slot. It collects the driving data such as acceleration and braking behavior of a driver, bridge it to the cell phone, and use the cell phone network to transmit it to the service provider. They say a driver can save up to 25% in auto insurance by driving properly (Saltzman 2015). The device is now not offered anymore, instead the cell phone app has become much 'cleaver' and can do the job itself. The app is offered in both iOS and Android platform and with the user consent, it collects the driving behavior based on the

movement of the phone's accelerometer. Accelerometers are used to measure the displacement of a device and are able to calculate the velocity, motion and movement of a person, hence the car as well. Ajusto app calculated the driving behavior of the driver based on certain conditions and score the person in a scale of 1-100. The current insurance drops based on how good is the driving behavior. Almost twenty five percent of customers have been already enrolled in this program which is offered for the last two years (Saltzman 2015). This rises a great deal of privacy as lots of personal data has been sent to the service providers, that includes where the driver is going, is he using his cell phone while on the road and other user behaviors. If an attacker can compromise one of the attack surface, such as the cell phone or the insurance app, then he can get hold of all these personal data.

3.3.2 Control override

This is a serious type of attack. A scenario can be described as driving at 70 miles per hour and suddenly the steering took a sharp right turn and the vehicle crashes (Pagliery 2014). This is the type of scenario come to anyone's mind when they think their car is hacked. This is the control override where an attacker can take over the control of a driver and manipulate the car against the driver's will. Currently this attack is possible to certain extent. As we know that CAN packets are broadcast to all the nodes in a vehicle network and the packets with high priority are always serves first. So if an attacker compromised a node in the network and flood the network with high priority packets, then a denial of service scenarios can happen. Some specific nodes can be halt by spoofing that it is busy with high priority packets. Either the nodes will be unresponsive or responds in the manner the attacker wants. A team of researchers were able to control override a vehicle which was moving at a 40 mph speed (Koscher 2014). They were able to honk the horns, blasting the heat and kill the engine of the car while in motion. The driver was restricted to restart the car. The team was also able to interact with the Electronic Brake Control Module (EBCM) and manipulate it accordingly. In the expensive report of Valasek and Miller (2015) they mentioned that this types of brake override is only possible with certain conditions to be fulfilled. The car has to be in hacker's favorable state and a number of CAN bus needs to be override. However they have shown that the brakes can be bleed with manipulating some other diagnostic commands. The team was able to own the brake of a 2014 Jeep Cherokee and guide it to a ditch at a speed of 5 mph.

3.3.3 Vehicle degradation

Vehicle degradation is the process of harming the vehicle with the help of compromised CAN bus packets. When a vehicle is low of supply such as engine oil, fuel or even radiator water, it shows the warning on the dash board. The driver notices the warning and take necessary measures to maintain the optimum level of supplies in the vehicle. Is has been

shown by the researcher to falsify the CAN packets and not show the actual condition of the vehicle. By doing that, medium to severe degradation of the vehicle is possible. Valasek and Miller (2015) was able to circulate a diagnostic packet in the network that will sense lack of fuel in the car and prevent the car from starting. Until and unless the packet is roaming in the system, it was not possible to start the car at all. In manual transmission cars, the gear shift is necessary after a certain RPM of the engine. RPM is a unit that gives the number of rotation of motor in the engine and it's linked to the gear shifting of the vehicle. Damage can happen to the transmission system if high RPM is obtained and the car is still in the lower gear. It is possible for attackers to spoof the RPM information on the dashboard and hence disguising the driver to shift on time.

3.3.4 Data falsification

Data falsification is the process of showing or giving wrong data to the user from the vehicle network. Modern cars have Airbag control system which checks the working airbags and informs the driver about their conditions. According to Yoshida (2013) it is possible to generate CAN packets that will falsify those data even in case there is no airbag in the vehicle at all (Hoppe – Kiltz – Dittmann 2010). The researchers show that old information of the airbag can be displayed in the system and disguise the driver that there are working airbags in the car. On the other hand, Valasek and Miller (2015) showed that it is possible to falsify the reading of speedometer and odometer in a vehicle. By showing a lesser value on the speedometer the driver is exposed to legal issues as well as falsified on his driving habits. Odometer changing can be a very big issue for used car sales market. The prices of a used vehicle directly depends on the number of kilometers it ran before. So if someone can decrease or change the numbers on the odometer, he can sale a vehicle for a substantial price.

3.3.5 External sensor attack

Modern vehicles are loaded with external sensors these days. These external sensors are used in various operations in the vehicle. Starting from adaptive braking system (ABS) to automatic parking assist, these external sensors are the vital sources of information for day to day operations. If an attacker manages to compromise an external sensors, it will be very easy for him to plot a physical attack with the mobility of the vehicle. Which using adaptive braking system, if the sensors are compromised, a car can hit another car in miscalculations. Proximity warning could be misled by the attacker which the driver is performing a parking with automatic parking assistance.

3.3.6 *Attacking TPMS*

Tire pressure monitoring system (TPMS) is a small device which resides inside the tire. It connects information such as the tire's air pressure, temperature and rotational speed and report to the car ECU (Smith 2014). The device is registered with the car's ECU with a 32-bit unique identifier. Normally the TPMS device is in sleep mode and wakes up in two ways. Either the car needs to run at a speed of 40 mph or a radio frequency device wakes the TPMS sensors. The radio frequency needs to be 125 kHz low frequency in order to wake up the TPMS. Few possible attack on TPMS can be:

- **Tracking the vehicle:** An attacker can track a vehicle based on its unique ID in a certain route. Specific sensors should be place in the possible route of the vehicle in order to track it. The TPMS usually broadcast in every 60-90 seconds and low frequency amplifier can be used to strengthen the receiving sensors and amplify its range.
- **Triggered events:** Theoretically it is possible to trigger an event when a vehicle with unique identifier is near a triggering sensors. So it is possible to open a garage door while the vehicle is near and it can also be possible to blow up a bomb when a vehicle passes a certain path and comes near to a sensor. This can be a devastating attack if vehicle id of a VIP or politically important person is exposed to terrorist groups.
- **Spoofing:** It can also be possible to damage the tires by spoofing the data received from the sensor and not putting any warning lights on the dashboard.

3.3.7 *Ethernet attacks*

Ethernet has been the de-facto standard for most of the computer network but it is yet to be seen in mass for automotive networks (Yoshida 2013). Ethernet was not used much in automotive network due to its lack of standards with the OEM EMI/RFI requirements as well as its high latency in data transfer rate (Ixia Worldwide Inc. 2014). But some of the leading auto manufacturers already using Ethernet technology in some part of its systems such as backup camera. BMW released its model X5 with Ethernet based 360 degree parking assistance backup camera (Yoshida 2013). Ethernet network is much familiar to the computer geeks and hacker communities and it can be easily analysed by freely available software like WireShark. When an attack get access to the Ethernet nodes of a vehicle, then it will much easier for him to tailor an attack and much efficiently drop its payload.

3.3.8 *Attacking key fobs and immobilizer*

Key fobs and immobilizers are convenient devices used to lock/unlock or remote start the vehicle from a short distance. These remote keyless systems runs at 315 MHz in North

America and in approximately 434 MHz in Asia and Europe (Smith 2014). The older model key fobs used to use infrared communication technology. There is usually a transponder which uses rolling code to authenticate with the immobilizer. The typical transponder operates at 125 KHz and communicate with the immobilizer through radio frequency identification (RFID). Potential attack on key fobs can be:

- Jamming the key fob with junk data and hence prevent the receiver to change the rolling code. Hence it will allow the attacker to see the current key sequence.
- Sometimes the key is stored in the memory of the immobilizer for a short period of time. The attacker may grab that information and start the vehicle without the key.
- Attacks are possible on older immobilizer where static keys are used instead of rolling keys.
- It is sometimes possible to dump the memory of the transponder and reverse engineer the secret key.
- Spoof the driver by jamming the car lock and giving an impression that the car was locked properly, where in real it is not. Hence the car will still be unlocked and it gives the attacker opportunity to steal items from the car.

3.3.9 Passive keyless entry and start

Passive keyless entry is quite similar to the immobilizer system but here the driver does not need to click any buttons in the device. When the driver approaches near the car with the device in his pocket, a security exchange takes places between the car systems and the key fob device and the car allows the driver to drive the car without any key. It is possible to apply relay attack on this scenario. An attacker place a device next the car and another one next to the driver. When the driver get close to the vehicle, the device relays the signals to the vehicle and back and hence the attacker has the opportunity to start the car before the driver.

3.3.10 Keypad entry

There are some vehicles which are shipped with keypad entry systems situated under the handle of the car. If an attacker has enough time to perform a permutation combination, then he can try all the possible combinations and has the potential to open the door of the vehicle. It might take about 20 minutes to unlock the car door (Smith 2014).

3.4 Types of attack

3.4.1 *Side channel attacks*

Side channel attacks are the attacks that are caused by the side channel information (Bar-El 2014). Side channel information are the data that is passed while a cryptographic analysis is done. Usually these information are not plain text nor totally encrypted as well. Side channel attacks have been a challenging issue among the security researchers who are specialized in cryptanalysis. Side channel data analysis can be of two types, simple analysis and differential analysis. In simple analysis, an attacker takes a small trace of the crypto operation inside the car and analyse it to find the secret key. In modern cryptography, public key infrastructure is a very popular approach for encryption. Here each node has its own pair of public key and private key as well. When a node needs to send an encrypted message, it uses the public key of the other node to encrypt and send the message. The destination node receives the message and decrypt it using its private key. The modern cryptographic devices are mostly designed with Complementary Metal-Oxide-Semiconductor (CMOS) gates which has data dependent power consumption (Saeedi – Kong 2014). That means there is a change of power flow in the semiconductor in accordance with the data flow. When the node access the private key to decrypt the message, electron flows in the CMOS conductor and it emits electromagnetic radiations. The attacker can guess the secret key from the source of that radiation leakage. On the other hand, differential analysis uses statistical tools to study an array of data in order to have an accurate differential power and electromagnetic analysis.

3.4.2 *Timing attacks*

These types of attack is similar to the side channel attack where the attacker focuses on the time needed to perform an operation. Different cryptographic devices need different amount of time to encrypt or decrypt a data based on the size of the data and algorithm used. It is possible for an attacker to find fixed Diffie-Hellman exponents or factor RSA keys just by measure the time taken to perform private key operations (Kocher 1996). These time analysis and measurements are fed into a statistical model, it can check correlations between time measurements and provide possible key bits based on some degree of uncertainty (Bar-El 2014). It was shown that it is possible to reconstruct the screen content of a video display unit just by analysing the electromagnetic data produced by it (Eck 1985).

3.4.3 Fault injection and reverse engineering attack

Fault injection attack is a wide spreading technique used by attacker where different factors are altered in a device. As for an example an attacker might change the power supply voltage level of a cryptographic device inside the car and see how it reacts on low power environment. Other factors the attacker can alter are injection of irregular clock signals, rise the temperature of the device or its surrounding or expose the device to intense lights (Barenghi - Breveglieri - Koren - Naccache 2012). By changing the factors, each device behaves in a different ways. The attacker notes down those differences and compare them to a fully functional device. It has been shown by researchers that it is possible to invade some cryptographic devices such as SNOW 3G and RSA to some extent using fault injection attack (Barenghi et al 2012). Reverse engineering is a process of understanding how a device or an algorithm works by reversing and analysing the procedure. Sometimes by doing so, a device can be unresponsive and cannot be used later on. By reverse engineering attack, a person can gain inside knowledge of the architecture of a device or system and hence can align with the procedure with successful disguise.

4 RELATED WORKS

A literature review in the domain of interest is the process of finding out what has been done related to a field of study (Bhattacharjee 2012). The three main reasons of literature reviews are:

- 1) Get to know the current state of knowledge in the area of the research.
- 2) To identify the prominent authors and researchers who have worked in this area and
- 3) To identify the knowledge gap in the research area.

4.1 Related works on Intrusion Detection

In the article by Hori, Sasaki, Miyamatsu and Yakura (2000, 25) Development of Intrusion Detection Sensor for Vehicle Anti-theft Systems, the researchers have experimented and demonstrated a vehicle intrusion detection system based on Radio wave. The reunification of east and West Germany and the collapse of Soviet Union lead to a sharp increase in car burglary during that time, and hence there was a high demand of vehicle anti-theft systems. Fujitsu ten was developing and marketing these devices since 1990 as an optional gadget for the cars until there was a need for adding them in the production line past 1998. The developed device that was explained in the article was designed to meet the U.K Insurers' certification requirements. Which in turn consists of two major test, an environment resistance test such as the temperature test and the actual anti-theft mechanism test with the sensors' performance. There should be a detection requirement and erroneous detection prevention. The sensor should be smart enough to alarm when there is an intruder and also ignore if a person just passing by the car. The detection technologies that are mainly used are radio waves and ultrasonic waves. An outstanding comparison of radio waves type and ultrasonic wave type sensors are done in respect to the effect on design, detection range and malfunction. The detection principle behind these waves is that, there is a transmitter and a receiver mechanism. The receiver is receiving the sinusoidal patterned waves from the transmitter and if there is any anomaly in the waves, an alert is generated.

Vestlund (2014) explained about the possible intrusion detection system (IDS) idea in his paper Intrusion Detection Systems in Networked Embedded Systems. The author pointed out the high risk of intrusion in the automotive network due to its increased networking abilities and he suggested to deploy intrusion detection systems in order to prevent it. Christian explained intrusion detection system as a "burglar alarm for computers that let someone know about the burglar". (Vestlund 2014) So the intrusion caused by the burglar is detected by a system and the system either notify the owner or does something by its own to mitigate the intrusion. IDS has been used in computing systems for quite sometimes and it has a good impact on auditing. IDS for embedded systems as car can be a vital tool for overcoming the vulnerabilities and shortfalls of the architecture of modern

cars. There are two types of IDS, host based and network based. The IDS resides in the host device in case of a host based system and the packets which are coming in or going out of the device is analysed based on some criteria. The network based IDS resides in a central position in the network where it has the ability to monitor any data packets to and fro from any of the nodes or devices. There are major two types of techniques the IDS uses for detecting intrusion: signature based or anomaly based intrusion detection. Signature based detection is similar to modern computer anti-virus tools. A set of virus or malware signatures based on hash values are stored in the databases of the IDS and it matches intrusion coming from any of those destinations whose signatures are already in the system of the IDS. Anomaly based IDS are smarter, they rely on pattern or behavior of a data packet and realize how different it is from a usual data packet of same kind. Both of these IDS techniques have limitations, they may have false positives or false negatives. False positive is tend to happen when an IDS is considering an event as a threat where in real it is not. And a false negative is other way around, an event which was passed by the IDS system which in fact is malicious. Christian suggested network based IDS for embedded systems to be hybrid IDS system based on some assumptions in his paper. He also mentioned the value in using artificial immune systems (AIS) in embedded network as it has to be lightweight and consumes less power. There are still much research needed for implementing a proper AIS in embedded IDS in automotive networks.

An applicability analysis of intrusion detection and prevention in automotive systems has been done by Fallstrand and Lindstrom (2015). The researcher surveyed the state of the art technologies available in modern cars these days and analysed the security measure proposed and implemented as well. An evaluation has been done with the current intrusion detections and prevention (IDPS) technologies and the researchers tried to portray a generic model of IDPS for the automotive industries. The IDPS systems are mostly grouped and listed with four properties (Pathan 2014):

- Scope: What entities and to what extent the IDPS protects.
- Location and distribution: The location of the system components and how are the settings.
- Detection method: what are the processes of the IDPS to detect intrusion?
- Post-detection: What will the system do in response of a detected intrusion?

Several tools and methods have been proposed, among them some are already in use and others are still in the testing phase. Among the broad categories there is message cryptography, where a CAN Bus packet is encrypted and send in the network. Architectural improvements in the vehicle network so that it is more segregated and robust towards attack and also securing the endpoint nodes. The purpose of their research was to develop a model by constructing a conceptual image of a general in-car network (Fallstrand et al 2015). The research did an in depth study about the various interconnected components of a vehicle and how they are connected. Additional considerations were taken about the hardware-imposed complexity of each nodes in the system and also about the cost. Daniel and Viktor proposed that a network-based IDPS system will be viable for automotive networks. They also mentioned that a single centralized IDPS system would be a better choice however they also talked about the data congestions that it can experience. The

team commented that anomaly based IDPS systems such as using a neural networks may increase the cost and complexity of the overall system that a traditional signature-based IDPS system. The post detection can be either passive or active. The passive detection of intrusion in the car will inform the user only whereas the active one will shut down the nodes. The authors concluded that it all depends on the criticality of the node itself. Other security measures such as network segmentations, packet filters, and use of cryptography was also discussed. The conclusion of this research paper was that, the architectural diversity and software/hardware dependencies of different automotive manufacturers is the reason for the failure of a generic model of modern automotive systems.

4.2 Related works on Penetration Testing

Penetration testing on vehicle ECUs has been discussed by Prathap and Rachumallu (2013) in their master's thesis paper. Different types of automotive networks has been discussed and attack taxonomy was well explained in context of embedded scenarios. The basic concept and principles of information security has been explained in depth, which are confidentiality, integrity and availability, which is also known as CIA Triad.

- Confidentiality is the concept that information should only be visible to groups who has the right to see the information. Privacy must exist and confidential information should only be available to intended recipients. As for an example, an individual person should only have the access to his health records and someone who he has given the permission to view, such as a doctor or health insurance personnel.
- Integrity: The information should not be changed or modified by anyone else except the owner or someone who has received the permission from the owner. The integrity of an information must be preserved when it is transmitted through a network or stored in a media. As for an example, when someone emails a recipient, the content of the mail should not be altered by anyone in the middle of the transmission.
- Availability: Information should be available at all time whenever the owner needs it, else there will be a denial of service scenario. The system must able to perform procedures to keep the information available at all times. As for an example, a user should always be able to check his email whenever there is internet services available.

Penetration testing is the process of testing the defense of a system, either from the outside or inside of the system. This is done to check the robustness of a system to external attacks. The common type of attacks are the external attacks where an attacker tries to infiltrate through the attack surface of a vehicle. In internal attack, the attacker already got access information to come inside the vehicle's network through social engineering. Some software and hardware countermeasures were suggested by the authors but due to the nature of fast paced environment and memory constraints there exist more rooms for research in this field.

Vyleta (2014) in his master's thesis Automated penetration testing in automotive industry has successfully demonstrate vulnerabilities in automotive network by a method known as Fuzzing. Fuzzing is a method which was idealized first by Barton Miller in 1988. The idea was to use random data to test in a software or application in order to find bugs in it. In this paper the author gave a holistic view of the world of penetration testing both in computing and automotive world. He compared the mostly used pen testing standards and methodologies and concluded that Open Web Application Security Project (OWASP) would be a proper choice for pen testing methodology for automotive systems. The author also introduced his fuzzing tool called Fuzzer which is based on open source fuzzing framework Peach. He proposed a method to analyse the fuzzing results obtained from the ECUs.

4.3 Related works on Standards and Frameworks

The National Highway Traffic Safety Administration (NHTSA) in USA along with the National Institute of Standards and Technology (NIST) published a cybersecurity risk management framework to modern vehicles in 2014 (McCarthy – Harnett 2014). The purposes of publishing this report is to bridge the knowledge gaps between automotive industries and cybersecurity practitioners. The current risk and threats are well explained and the security best practices are mentioned in the form of guidelines. It was mentioned that the SAE International Vehicle Electrical System Security Committee is working to identify strategies and techniques to prevent breaches in the automotive network and they are developing measures to mitigate those breaches when they happen. NIST already has a well-established risk assessment framework security lifecycle. A modified risk management framework has been developed only to support the vehicle sector.

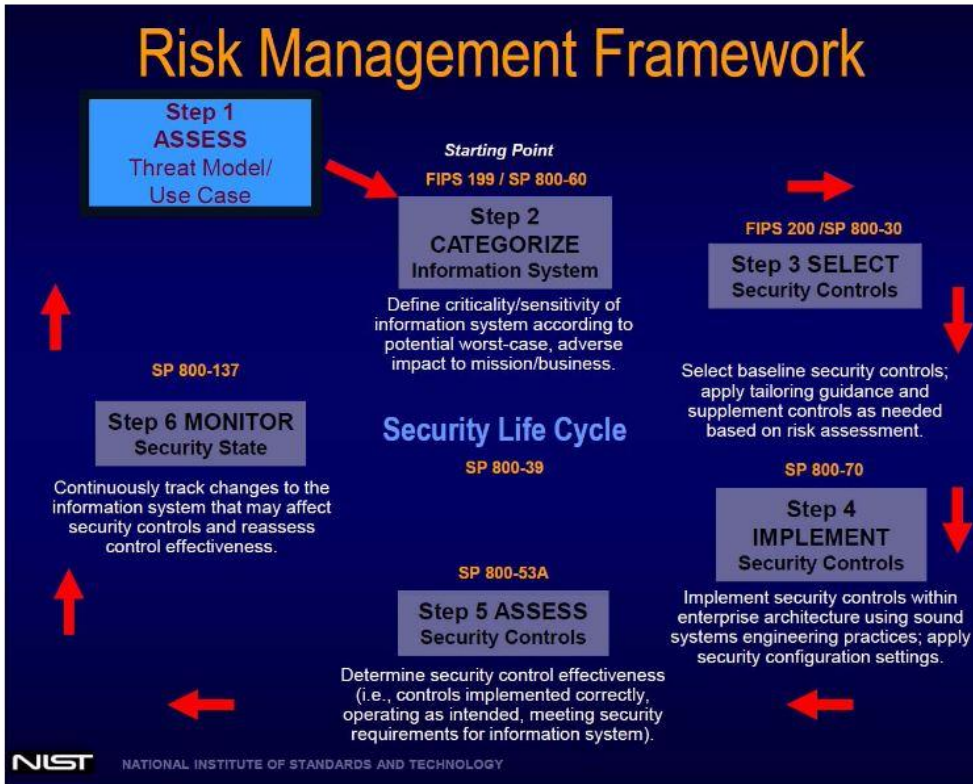


Figure 6 NHTSA Risk Management Framework (McCarthy et al 2014)

There are 6 detailed steps in the modified risk management framework for vehicles:

- Assess threat model/used case: This is the step where the threats and risks are assessed and used cases are developed to portray the scenarios. The threat sources can come from either of this three types 1) threat from cyber or physical attack on the vehicle network 2) human errors due to omission and 3) natural or man-made disasters.
- Categorize information system: The federal information processing standards (FIPS) 199 / Special Publication (SP) 800-60 discusses this step further. This is mainly to categorize the vehicle, its sub-systems as well as the impact of the attack. This categorization is mainly done by the system owner which would be the automotive manufacturers. This step will help to align the security controls and give them the right and optimum support.
- Select security control: In this step, the proper security controls are selected based on types of vulnerabilities. The vulnerabilities are identified and the likelihood of occurrence and damage is determined. The impact of the threat is also considered along with the risk impact. Finally a risk assessment report is produced who likely to have system characterization, threat areas and risk calculations. FIPS 200/SP 800-30 covers this in great details.

- **Implement security control:** The selected security controls from the previous steps are implemented here. The common control are identified and the security controls are selected. Security test and evaluation such as vulnerability assessment and/or penetration testing are introduced. SP 800-70 has it covered in depth.
- **Access security controls:** In this phase, the risk assessment results are shared with the management for review in forms of executive briefings, risk assessment reports or dashboards. The review can either be formal or informal based on the organization's policy. SP 800-53A covers this in great details.
- **Monitor Security Control:** This step is covered in SP 800-137 where the security controls are monitored. A risk factor monitoring is conduct as well the updates of the risk assessments. A monitoring strategy is developed which will be ongoing in nature and reflects the changes made time to time.

The members of the Auto Alliance and Global Automakers have developed a cybersecurity best practice framework based on NIST and other cybersecurity standards and it supposed to be a best practice guide for voluntary automotive cybersecurity operations. The document mainly touches on vehicle security by design, risk assessment and management, threat detection and protection, incidents response and recovery and collaboration and engagement with appropriate third parties (Auto Alliance). On top of that the security best practice also includes continued review of existing best practices and also prioritization of issues and identify them properly. The rooms for engagement of independent experts are also discussed as well as the participation of external stakeholders such as after-market product manufacturers, government agencies or event customers/user of the vehicle industries. They will also organize series of work sessions for engaging the industry and its people in order to understand and synchronize the industry best practices among each other. A white paper has been written by David Brown et al of Intel Security about best practices as well (Brown - Cooper - Gilvarry - Rajan - Tatourian - Venugopalan - Wheeler- Zhao 2015). In their paper recommendations for security and privacy in the ear of the next-generation car, they have talked about the privacy concerns of users' data on the vehicle network and also the risk and vulnerabilities associated with it. They have discussed the distributed security architecture and hardware security services which can be used by applications. Hardware security such as trusted execution technology, active memory protection and cryptographic accelerations were mentioned as best practices in automotive securities. A range of options about software security, network security and cloud security were also explained. Supply chain risk management such as authorized distribution channels (OEMs and third parties) and continuity of supply plans for spare parts in order to maintain the vehicle are also included. Different standards in automotive industries such as J3061 and J3101 were also touched.

4.4 Related works on Vulnerability Analysis

A Car Hacker's Manual paperback book has been written and published by Smith (2014) of Open Garages which gives an holistic approach of car hacking. The book explains the attack surfaces commonly available in modern cars, and the tricks to break into the vehicle. A list of CAN Bus inspection tools are explained in the book as well as the explanation of CAN data findings. External and internal threats are categorised well in this book and a bird's-eye view analysis was presented. The infotainment center of a car is closely linked to its internal network. Long range external nodes such as cellular or Wi-Fi can have direct access to the infotainment console. This console is associated with the internal network of the vehicle or the CAN Bus network. Hence an attacker has privilege to compromise the processes in the ECU with a tampered infotainment system. Power glitches and clock glitches were explained which can be effective if the attacker has a powerful device than the automotive counterparts by affecting the memory's read and write capabilities. To setup a test based workstation to try car hacking a researcher needs oscilloscope, logic analyzer, solder reflow station, OBD-II extension cable and CAN Bus scan tools. A list of software were also provided that will support the mentioned hardware.

Side-channel vulnerabilities in automobile network has been discussed by Saeedi and Kong (2014). This types of vulnerabilities exist among the cryptographic tools already available in automotive systems these days. The two types of side-channel analysis are the simple and differential electromagnetic analysis (SEMA and DEMA). The authors introduced Fuzzy analysis of side channel information. A differential analysis of 0-set and 1-set of the cryptographic signals are taken into considerations. They are then fed into a fuzzy engine where based on certain rule matrices, the fuzzy engine concludes if it is an improbable, unclear, probable and highly probable incident. The proposed fuzzy system works in two phases, in the first phase, the fuzzy engine analyses the side channel information and gives a secret bit based on some estimations. Then on the second phase a final decision has been made on previous phases output and considering other measurements. (Saeedi et al 2014.)

Koscher, Czeskis, Roesner, Patel and Kohno (2010) did an experimental security analysis of the modern automobile. A detail explanation of automobile architecture and the internal processes are explained here. They pointed out the potential fragility in CAN Bus network, in the telematics and also during the operations of the ECUs such as ECU couplings. This paper did not touch threat model of the vehicle in-network but explained in detail what hackers can do if they have compromised the vehicle systems through the threat models. The two most discussed threat model explained are the OBD-II physical port and the various wireless functionalities of the infotainment systems. The experiments were carried out on the bench, where there were no wheels attached to the cars, on stationary cars as well as cars which they are on the road. A software called Carshark has been developed to analyse the CAN Bus data and to manipulate with them. The inter-

vehicle network security is mostly depends on the carrier protocol which is the CAN Bus network in most of the modern vehicles. Hence the CAN security challenges such as broadcast in nature, fragility to DoS, no authenticator fields and weak access control are the main reasons for the easy attack surface in vehicle networks. The attack methodologies were packet sniffing and targeted probing with the help of Carshark, through fuzzing and also through reverse engineering. On the stationary testing, the team were able to compromise the radio and control its display. They were also able to control the instrument panel cluster and able to modify data. By reverse engineering they were able to compromise the body controller and hence could lock unlock the car doors and jam them if needed. Most of the attacks towards the engine were done by fuzzing and through that they were able to compromise the brakes, HVAC systems and also be able to generate a denial of service attack. On the road testing, the car was moving at a speed of 40 mph where the team were able to perform composite attack on the vehicle. They were able to control the speedometer, turn off all the lights in the vehicle and also exhibit a self-destruct sequence where the engine will be killed after 60 seconds of countdowns.

The threat models and the attack surfaces has been discussed in another paper by Checkoway et al (2011). The paper is titled as Comprehensive Experimental Analyses of Automotive Attack Surfaces. The paper was segmented into four sections, threat model characterization, vulnerability analysis, threat assessment and synthesis. A comprehensive attack surface capabilities has been constructed, a simplified version is shown below:

Table 3 Attack surface capabilities (Checkoway et al 2011)

Vulnerability type	Channel	Capability	Visible to User	Scale	Full control
Direct physical	OBD-II	Attack hardware plugged directly into OBD-II port	Yes	Small	Yes
Indirect physical	CD	CD-based firmware updates	Yes	Small	Yes
	CD	Special song (WMA) embedded with codes (steganography)	Yes	Medium	Yes
	PassThru	Wi-Fi or wired control to PassThru devices such as cell-phones or iPods	No	Small	Yes
	PassThru	Shell injection via Wi-Fi or wired connection	No	Viral	Yes
Short-range Wireless	Blue-tooth	Buffer overflow via cellphone which is paired and has a Trojan app	No	Large	Yes
	Blue-tooth	MAC address sniffing, PIN brute force	No	Small	Yes
Long-range wireless	Cellular	Authentication exploit, buffer overflow by the use of laptop	No	Large	Yes

Cellular	Call car, authentication exploit through iPod, audio files, ear-phones, and a telephone	No	Large	Yes
----------	---	----	-------	-----

Paul Carsten et al has discussed and analysed vulnerabilities in in-car network and also recommended few solutions in their paper *In-vehicle Networks: Attacks, Vulnerabilities, and Proposed Solutions*. The team had explained different types of communication buses available to modern cars such as CAN, FlexRay, MOST and LIN. A detailed analysis of standard CAN packet was also mentioned. Different attack methods such as data stealing, control override, vehicle degradation and data falsification are also explained in great detail. The purpose of their research was to provide some functional solutions of the current shortfalls of CAN protocol architecture. Since CAN protocol broadcasts packets to all the nodes, there might be no way for a single node to know if a packet comes from a legitimate in-car node or a malicious node. By including a hash value with the CAN packets the researchers think they can overcome the problem. Hash value is a fixed length numeric value that represents a data in a unique way (Microsoft Developer Network 2016). Hash values are generated through hash function that is only one way. The original data cannot be replicated from a hash value by going backward. Hash value gives the authenticity of a data or CAN packet in our case. The team has decided to use CAN with Flexible Data-Rate architecture instead of regular CAN architecture which was proposed recently by BOSCH. This protocol has improved features and will be able to carry a hash value within a packet. They also proposed a CAN identification number based on vehicle. So it should be something similar to a VIN which will identify that a CAN packet belongs to a specific car, and not any malicious node. Their proposed solution will use a universal clock in the car and also a hash division. The solution will be beneficial to invasion and replay attack resistance.

A database management system (DMS) was proposed by Schulze et al (2009). The team has proposed three systems which are centralized, distributed and hybrid. All the data are supposed to pass through a centralized system which will look for anomalies in the system. But the centralized system can cause a bottleneck scenarios if it breaks in the operation at any time. The distributed system strategy is to have multiple DMS throughout the in-vehicle network, but it might add much throughput and load to the existing ECUs. The hybrid system is the combination of both and may work in a desired manner. An algorithm was proposed by Ling and Feng (2012) where a monitoring system monitors the CAN packets and changes counters based on a known ID or unknown ID. Another very ambitious approach was proposed by Oguma et al in (Oguma – Yoshioka - Nishikawa - Shigetomi - Otsuka - Imai 2008). They proposed an attestation-based security where each ECU will go through an attestation and encryption process with the master ECU when the car was first started in its manufacturer's location. A verification process with all the other ECUs present in the in-vehicle system will exchange cryptographic keys and a master table will be present for the master ECU. When a vehicle is started, the master ECU sends two random numbers to all the ECUs in the car. These two numbers are used by the other ECUs in hash form to communicate further in the system.

In a technical white paper written by Miller and Valasek (2015), they have introduced the steps and tools needed for car hacking. Their research was mainly focused to reduce the barrier of other researchers or security personnel to automotive infrastructure and security. They explained and showed how to put an ECU on a bench, connect it and experiment with it. The team was able to read the ECU sensors and attack the network with CAN message injection. They admit that there are some limitation for trying out these hacking methods in actual moving vehicles. But last year the team was able to hack a Jeep Cherokee 2014 model without altering it. They explained the whole process in their report Remote Exploitation of an Unaltered Passenger vehicle. The team identified that the remote attack surface for the 2014 Jeep Cherokee are the remote keyless entry, tire pressure monitoring system, Bluetooth, radio (FM/AM/Xm), cellular and internet (through apps), as most of them use CAN C and CAN IHS communication protocol. They were able to jailbreak the Jeep's infotainment system also known as UConnect and also manage to re-flash it to get compromised updates. Among all other hacking demonstrated by them, compromising the vehicle through cellular system was the most outstanding one. One of the researcher was able to put payload into the target vehicle from 10 miles away via the Splint cellular network. The team was able to compromise the CAN messages to turn signals, lock/unlock doors, alter RPMS, kill engine, disengage brakes, and turn steering and able to direct the test Jeep into a ditch.

4.5 Related works on Information Privacy

Information privacy is getting a considerable attention in the past decades especially in law, public policy, organizational behavior and information systems (Caudill – Murphy 2000). The consumers' privacy has been segmented into three categories (Data privacy: what the consumer really thinks 2015):

- 1) Data pragmatists: These are the group of consumers who understand the risk of data privacy but they are willing to review it in a case-by-case basis. They weigh the benefits they receive with a service while exposing their private data.
- 2) Data fundamentalists: This group is very concern about their data and they oppose to share it for any cost. They are always unwilling to provide personal information for any kind of service enhancement.
- 3) Data unconcerned: As the name applies, this group of consumers are not concern at all about the privacy of their data.

In a report published by US senator Markey (2015), the security risk and privacy gaps of drivers were held focused. A set of questionnaire about data privacy and the measures taken are distributed among 16 major automobile manufacturers including BMW, General Motors, Mercedes-Benz, Toyota and Honda. The report discusses about the wide range of technologies available in today's automotive market and also portrays the responses received from these manufacturers. According to Ed Markey's report:

- The modern cars with wireless technologies in the market, 100% of them possess the risk and has the vulnerabilities to hacking or privacy violations.
- Most of the automotive manufacturers were not able to report past hacking incidence in their product nor has an idea if there were any incident happened.
- Anti-intrusion practises and procedures for remote access to a vehicle are not reliable at all, and most of the automotive manufacturers do not understand the question asked by senator Markey.
- Only two manufacturers out of sixteen replied and admit the capability of real-time intrusion detection in their vehicle.
- A large number of data about the vehicle as well as the driver has been collected by the automotive manufacturers.
- Most of the automotive manufacturers collect user and vehicle data and transfer them wirelessly to their system or third party systems. The transfer process lacks encryption and proper security measures.
- User and vehicle data are stored for unknown number of time in manufacturers' or third parties' databases and there is no specific rules on data retentions.
- Customers are sometimes not aware of the data collections and an explicit awareness is not provided by the manufacturers. There are less or close to none possibilities to opt out from data collections without giving up on valuable services such as navigations.

These findings show that there are many possible rooms for intruders or hackers to compromise an automotive systems via the manufacturer's lack of understanding of data privacy and security. There should be standards that mentions about wireless vehicle's attack surfaces and the procedures to mitigate them. There should be security systems validation and possible options for penetration testing. There should be rooms for handling real time hacking attempts and the drivers should be made explicitly aware of the amount and types of data collection done by the manufacturers.

Another concern of data privacy is the rise of "Consumer Capital". It is said to happen when customers do not think personal data is a privacy risk rather than an effective indication to their preferences for specific commodities (Data privacy: what the consumer really thinks 2012). Although most of the concentration is towards e-commerce and digital marketing, few semantic attempt has been done to control consumers' privacy in automotive system. No proven model has been developed or tested that will undergo the privacy issues in automobiles. To fill up the gaps, an online survey has been conducted and data from 142 respondents who are current automobile users (or will be automobile users in near future) have been recorded and analysed. Information privacy is defined as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others" (Westin 1967, 7). It is the personal freedom and control of own data to share with each other. The earlier studies have been done on information privacy in general and Smith et al [54] has developed a one dimensional global information privacy concern (GIPC) scale. It was a general

scale and does not contain any specific dimensions. Hence their further research and efforts in this area has finalized a multidimensional scale called concern for information privacy (CFIP). The original CFIP scale has four dimensions which are collection, unauthorized secondary use, improper access and errors. Malhotra, Kim, and Agarwal has developed another scale known as Internet Users' Information Privacy Concerns (IUIPC). The first order of this model has three factors, namely collection, control and awareness of privacy practices, they are described in detail below:

Collection: It is the process of data collections for various users' privacy concerns. It is one of the most important factors and it is known to be the degree of information and data collected and possessed by others relative to the value of benefit received. Collection is also an important factors of CFIP scale. (Malhotra et al 2004.)

Control: This is another most important components to reflect IUIPC and it is the control of personal information that are made public to the automobile manufacturers or third parties. This is the ability given to a user over his or her shared information. Numerous studies have shown that people has the tendency to have control over their data. A study done by Phelps, Nowak and Ferrell (2000) shows that 84% people wanted to have further control over their data in order to limit commercial advertisements. It has been also found that people are less worried about data privacy concern when they have the choice to opt-out from the process (Nowak – Phelps 1995). User's privacy concern will increase where there is a lack of control over their data.

Awareness of privacy practices: Researcher Foxman and Kilcoyne (1993) reasoned on the basis of literature review that information privacy happens only when a person is given control over his information he is well informed about the data collections and usages. Hence awareness of privacy practices is another important factors in IUIPC scale. The awareness factor can also be of two types: interactional and informational justice. Interactional justice is the transparency of information during the act of legislation and informational justice is the process of information disclosure (Malhotra et al 2004).

Second-order IUIPC: It has been engaged by Smith et al. (1996) that CFIP is correlated to first-order factors and their model exclude the prospect of a second-order factors governed or lead by the first order factors. However Stewart and Segars (2002) argued on that and said "CFIP leads to various subconcerns" and hence is no longer a first-order factors, it has the elements of a second order phenomenon. Based on these evidences or empirical and studies, Malhotra, Kim, and Agarwal [55] anticipated that their IUIPC scale is a second-order factor too. Several problems in structural model has been eliminated by the second-order IUIPC. As for an example, confusion between multiple factors and many research variable of interest by the researchers are phased out. On top of that, problems due to multicollinearity has been eliminated too by using the second-order IUIPC. This model is more concise, convenient and empirically justified (Malhotra et al 2004). A summary of the comparison of GIPC, CFIP and IUIPC are given below:

	GIPC	CFIP	IUIPC
Purpose	To reflect the level of information privacy concerns in general	To reflect individuals' concerns about organizational information privacy practices	To reflect Internet users' concerns about information privacy
Focus	No particular focus	Organizations' responsibilities for the proper handling of customer information	Individuals' perceptions of fairness/justice in the context of information privacy
Context	Context-independent	Mostly offline or traditional direct marketing	Mostly online environment
Communication	Both one-way and two-way communication	Mostly one-way communication	Mostly two-way communication
Dimensions	One-dimensional construct	Collection, improper access, unauthorized secondary use, and error	Collection, control, awareness of privacy practices
Representation	A single latent factor	Correlated first-order factors; Stewart and Segars (2002) argued that CFIP is better represented as a second-order factor.	Second-order factor

Figure 7 Comparison of GIPC, CFIP and IUIPC scale (Malhotra et al 2004)

A Causal Model has been developed by Malhotra and Agarwal (2004) which is based on the theory of reasoned action (TRA) and trust-risk framework. The context-Specific factors in the model are the Trusting Beliefs, Risk Beliefs and Behavioral Intention. Trust and risk play a vital role in variety of situations where there is a dependency with uncertain environments. A consumer's firm relationship can be deduced from a trust-risk model (Wulf – Odekerken-Schroder – Lacobucci 2001). Trusting belief is the degree to which a consumer trust the automotive manufacturers or third parties for taking care and protecting his information. On the other hand risk belief is the expectations of loss of privacy on consumers' information by the automotive manufacturers. Behavioral intentions is the tendency of a consumer and his intention to release information to the automotive manufacturers or third parties (Dowling - Staelin 1994). There are few hypotheses for the Causal models of second-order IUIPC (Malhotra et al 2004) which were already tested and the researchers found them supported to their theory. The hypotheses are little bit modified to meet the requirement of this thesis and are given below:

Hypothesis 1: Automotive users' information privacy concerns will have a negative effect on trusting beliefs.

Hypothesis 2: Automotive users' information privacy concerns will have a positive effect on risk beliefs.

Hypothesis 3: Trusting beliefs will have a negative effect on risk beliefs.

Hypothesis 4: Trusting beliefs will have a positive effect on intention to reveal personal information.

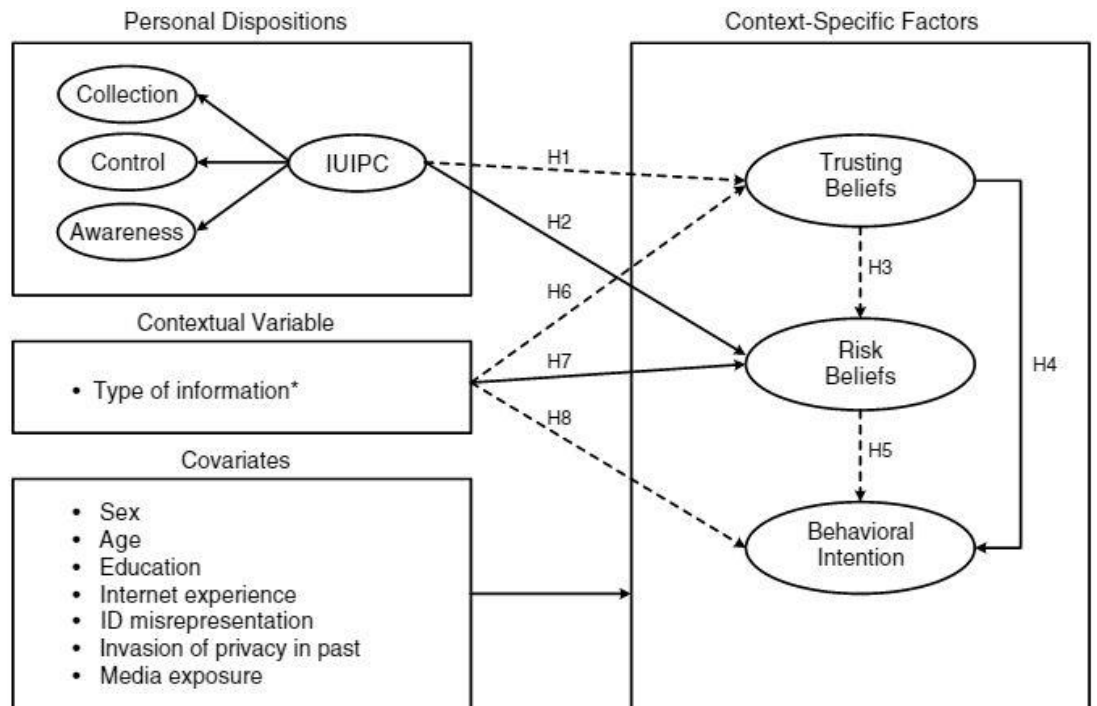
Hypothesis 5: Risk beliefs will have a negative effect on intention to reveal personal information.

Hypothesis 6: An automotive manufacturer or third party's request for more sensitive information will have a negative effect on trusting beliefs.

Hypothesis 7: An automotive manufacturer or third party's request for more sensitive information will have a positive effect on risk beliefs.

Hypothesis 8: An automotive manufacturer or third party’s request for more sensitive information will have a negative effect on intention to reveal personal information.

The Causal model of IUIPC by Malhotra et al (2004) are given below:



Notes. *Less sensitive information (0), more sensitive information (1), positive effect —→, negative effect - - - ->.

Figure 8 Original IUIPC scale model (Malhotra et al 2004)

5 RESULT ANALYSIS

5.1 Information privacy

The survey questions for this thesis have been tailored to fit in the major factors of the IUIPC scale (Malhotra et al 2004). Questions has been asked to respondents via Google forms and the answers are analysed and observed below:

Control	It is a consumer's' right to control and monitor about how their vehicle-recorded and user-introduced data from the automobile are collected, used and shared. Five point linear scale were introduced where 1=Agree, 2=Partially agree, 3=Neutral, 4=Partially disagree, 5=Disagree
	Controlling personal information is the key part of consumer privacy. Five point linear scale were introduced where 1=Agree, 2=Partially agree, 3=Neutral, 4=Partially disagree, 5=Disagree
Awareness	Automakers collecting information from the car should disclose the way the data are collected, processed and used. Five point linear scale were introduced where 1=Agree, 2=Partially agree, 3=Neutral, 4=Partially disagree, 5=Disagree
	There should be a clear and easy way to aware the consumer about information disclosure through policies or user manuals. Five point linear scale were introduced where 1=Agree, 2=Partially agree, 3=Neutral, 4=Partially disagree, 5=Disagree
Collection	It bothers me that my car is passing information to the automakers. Five point linear scale were introduced where 1=Agree, 2=Partially agree, 3=Neutral, 4=Partially disagree, 5=Disagree
	I am not comfortable with giving user-introduced data to automaker or third parties. Five point linear scale were introduced where 1=Agree, 2=Partially agree, 3=Neutral, 4=Partially disagree, 5=Disagree
	I am not comfortable with giving vehicle-recorded data to automaker or third parties. Five point linear scale were introduced where 1=Agree, 2=Partially agree, 3=Neutral, 4=Partially disagree, 5=Disagree
Errors	How important is it to have data encryption during the collection process? Five point linear scale were introduced where 1=Very important,

	2=Partially important, 3=Neutral, 4=Not so important, 5=Not important
Unauthorised personal use	Automakers should never sell personal information (e.g. information obtained from my car/driving habits) to other companies for promotional activities. Five point linear scale were introduced where 1=Agree, 2=Partially agree, 3=Neutral, 4=Partially disagree, 5=Disagree
Improper access	Automakers or third parties (independent service providers) should have a secure way to store data. Five point linear scale were introduced where 1=Agree, 2=Partially agree, 3=Neutral, 4=Partially disagree, 5=Disagree
Global information privacy concern	On a scale of 1 to 5: To what extend do you trust automakers in terms of information privacy? Such as having access to user-introduced data (e.g. GPS location) and vehicle-recorded data (e.g. how much brake fluid is left). Five point linear scale were introduced where 1=I trust them and 5= I do not trust them.

Control:

It is a consumer's' right to control and monitor about how their vehicle-recorded and user-introduced data from the automobile are collected, used and shared. Five point linear scale were introduced where 1=Agree, 2=Partially agree, 3=Neutral, 4=Partially disagree, 5=Disagree

(140 responses)

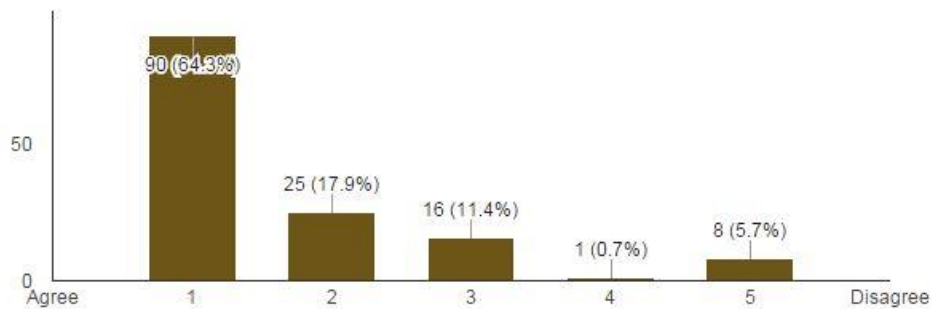


Figure 9 User responses: Question on Control 1

140 responses were recorded where 64.3% agreed to this statement and 17.9% partially agreed as well.

Controlling personal information is the key part of consumer privacy. Five point linear scale were introduced where 1=Agree, 2=Partially agree, 3=Neutral, 4=Partially disagree, 5=Disagree

(141 responses)

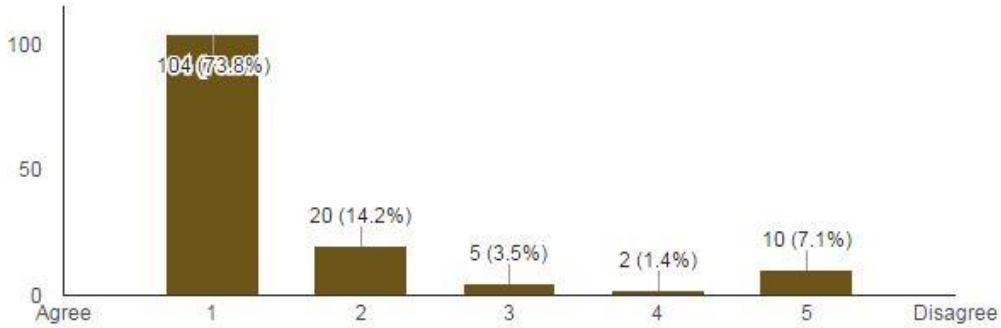


Figure 10 User responses: Question on Control 2

141 responses were recorded where 73.8% agreed to the statement and 14.2% partially agreed as well. Only 7.1% disagree with the statement.

Observation: Although all the hypotheses are mathematically proved to be supported in the Causal model (Malhotra et al 2004), our survey results also shows a similar positive effect on hypothesis 1, 2 and 3 in this case. The privacy concerns of automotive users will have a negative effect on trusting beliefs and a positive effect on risk beliefs. On top of that, trusting belief will have a negative effect on risk belief. Most of the consumers believe that they have the right to control and monitor the data that are passed to the automotive manufacturers and third parties through their vehicles. The control over their own data is the most important thing they think about information privacy. This concern of information passing will definitely increase a negative effect on the trust towards the manufacturers.

Awareness:

Automakers collecting information from the car should disclose the way the data are collected, processed and used. Five point linear scale were introduced where 1=Agree, 2=Partially agree, 3=Neutral, 4=Partially disagree, 5=Disagree

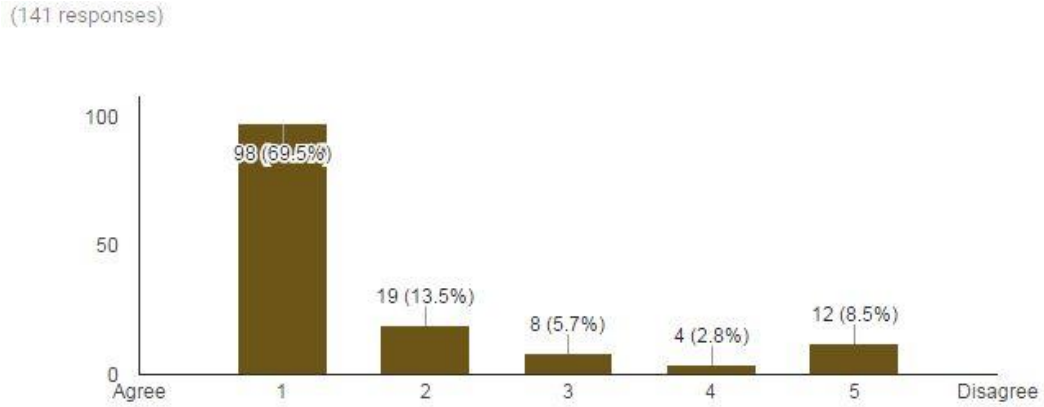


Figure 11 User responses: Question on Awareness 1

141 responses were recorded where 69.5% agreed to the statement and 13.5% partially agreed as well. Only 8.5% disagree with the statement.

There should be a clear and easy way to aware the consumer about information disclosure through policies or user manuals. Five point linear scale were introduced where 1=Agree, 2=Partially agree, 3=Neutral, 4=Partially disagree, 5=Disagree

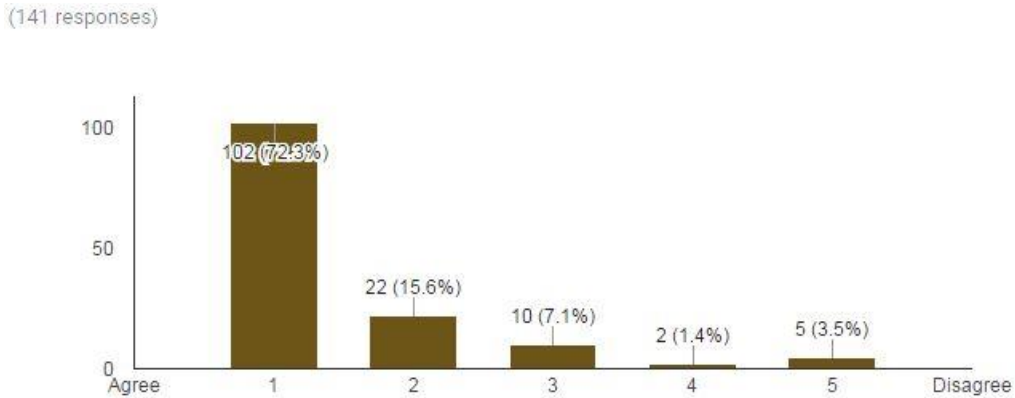


Figure 12 User responses: Question on Awareness 2

141 responses were recorded where 72.3% agreed to the statement and 15.6% partially agreed as well. Only 3.5% disagree with the statement.

Observation: The automotive manufacturers or Automakers should disclose the information that are collected from the consumers and there should be a clear and easy way to aware the consumers. This will support the hypothesis 4 and 5. If the automakers reveal what information they are collecting from the consumers and aware the consumers through a transparent method, then the trusts of the consumers towards the automakers will increase and open the intention to reveal personal information. Consumers

might disclose more information as there is transparent data collection method available and a trust exists between the automaker and consumer due to that.

Collection:

It bothers me that my car is passing information to the automakers. Five point linear scale were introduced where 1=Agree, 2=Partially agree, 3=Neutral, 4=Partially disagree, 5=Disagree

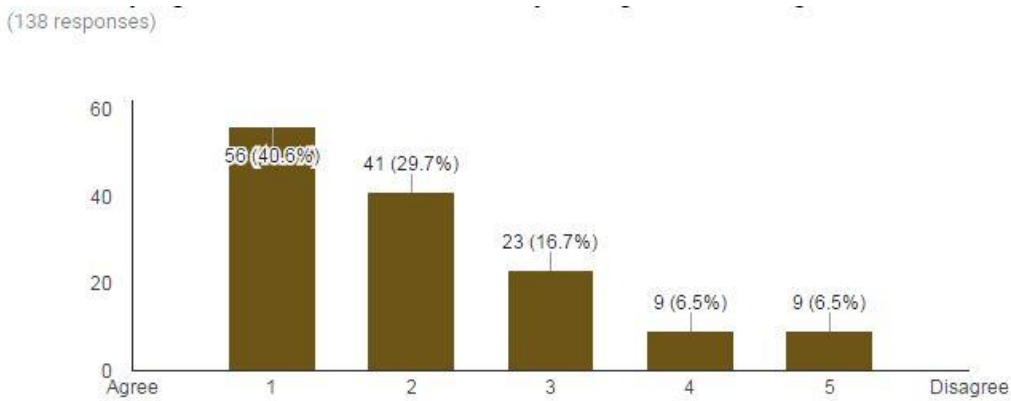


Figure 13 User responses: Question on Collection 1

138 responses were recorded where 40.6% agreed to the statement and 29.7% partially agreed as well. Only 6.5% disagree with the statement.

I am not comfortable with giving user-introduced data to automaker or third parties. Five point linear scale were introduced where 1=Agree, 2=Partially agree, 3=Neutral, 4=Partially disagree, 5=Disagree

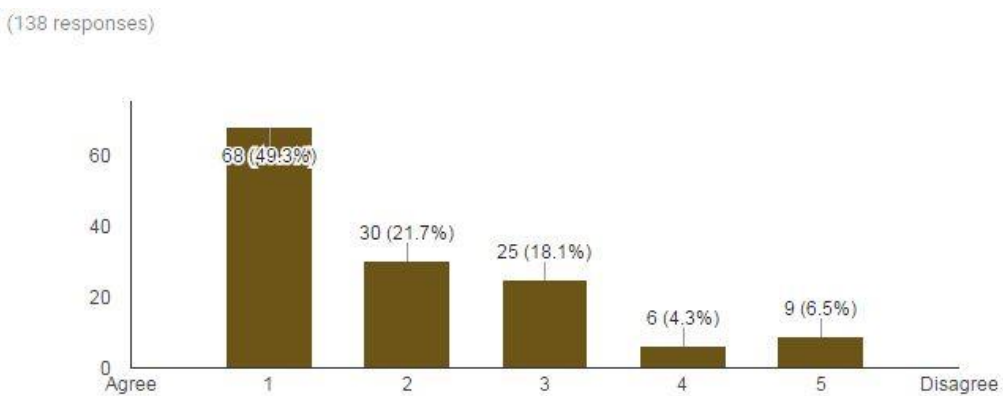


Figure 14 User responses: Question on Collection 2

138 responses were recorded where 49.3% agreed to the statement and 21.7% partially agreed as well. Only 6.5% disagree with the statement.

I am not comfortable with giving vehicle-recorded data to automaker or third parties. Five point linear scale were introduced where 1=Agree, 2=Partially agree, 3=Neutral, 4=Partially disagree, 5=Disagree

(139 responses)

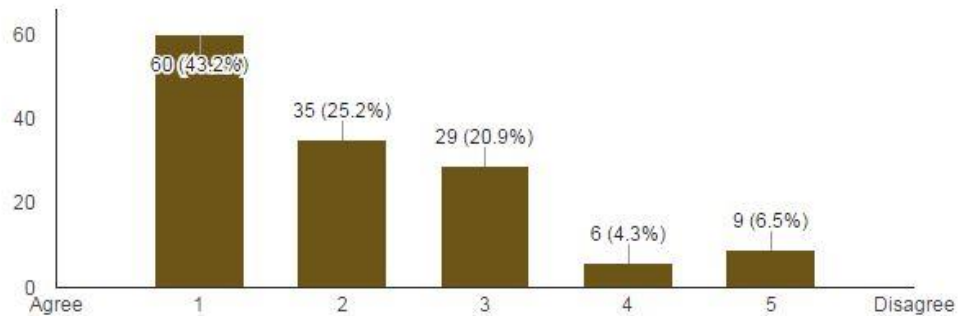


Figure 15 User responses: Question on Collection 3

139 responses were recorded where 43.2% agreed to the statement and 25.2% partially agreed as well. Only 6.5% disagree with the statement.

Observation: A positive response is recorded from responders that they are not comfortable that the car is passing information to the manufacturers and it bothers them. They are also not favorable with the fact in giving vehicle recorded or user introduced data to manufacturers or third parties. This supports the hypothesis 6 and 7, 8. So a request from the automakers or third parties for more sensitive information will decrease the trust towards them and hence will have a negative effect on trusting belief. The consumers will be more concern about the information privacy and hence their risk belief will have a positive impact. Their intention to share information with the automakers or third parties will be less and hence there will be a negative effect to reveal personal information.

Errors:

How important is it to have data encryption during the collection process? Five point linear scale were introduced where 1=Very important, 2=Partially important, 3=Neutral, 4=Not so important, 5=Not important

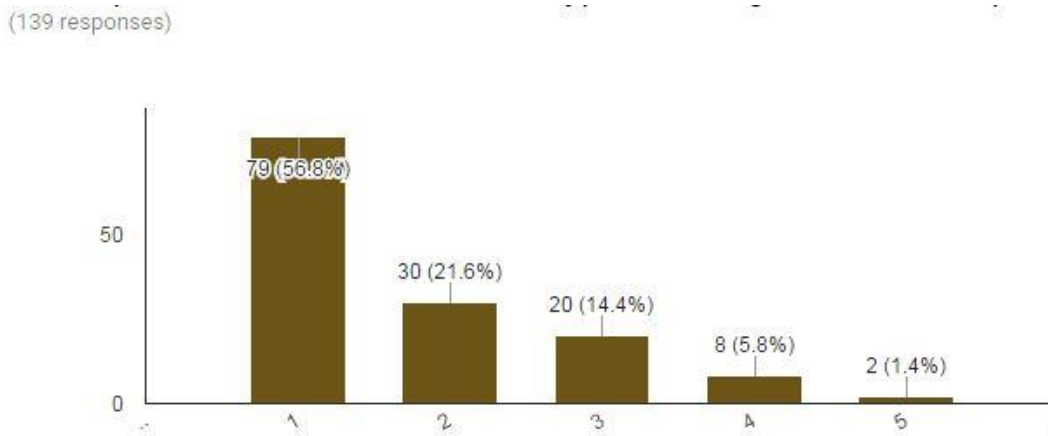


Figure 16 User responses: Question on Errors 1

139 responses were recorded where 56.8% agreed to the statement and 21.6% partially agreed as well. Only 1.4% disagree with the statement.

Observation: The lack of data encryption can have two implications in the CIA triad. The lack of confidentiality and the lack of integrity. When data is transmitted without encryption, there are number of ways intruders can read that data in plain text and modify it if needed. Thus data is no longer confidential and there is no integrity in the data as well. Most of the respondents agree that data encryption is important or partially important and it supports hypothesis 2, 5, 6. The privacy concern will have a positive effect on the risk belief of the consumers and risk belief will lead to a negative effect on intention to reveal personal information. On top of that, if the automakers ask for more information, there will be a negative effect on the trusting belief.

Unauthorised personal use:

Automakers should never sell personal information (e.g. information obtained from my car/driving habits) to other companies for promotional activities. Five point linear scale were introduced where 1=Agree, 2=Partially agree, 3=Neutral, 4=Partially disagree, 5=Disagree

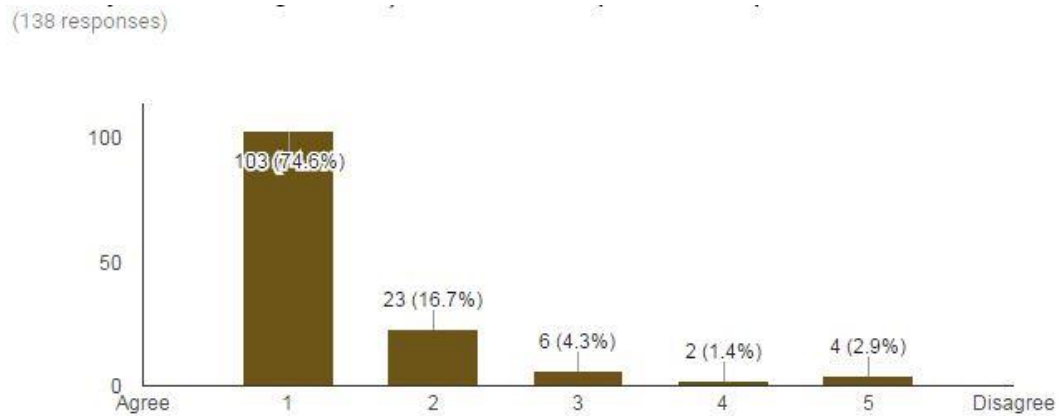


Figure 17 User responses: Question on Unauthorised Personal Use 1

138 responses were recorded where 74.6% agreed to the statement and 16.7% partially agreed as well. Only 2.9% disagree with the statement.

Observation: Most of the respondents believe that the automakers never sell those collected information to companies for promotional activities. If the automakers do so, there will be a privacy concern among the consumers and it will have a negative effects on trusting belief and positive effect on risk belief. It supports hypothesis 1.

Improper access:

Automakers or third parties (independent service providers) should have a secure way to store data. Five point linear scale were introduced where 1=Agree, 2=Partially agree, 3=Neutral, 4=Partially disagree, 5=Disagree

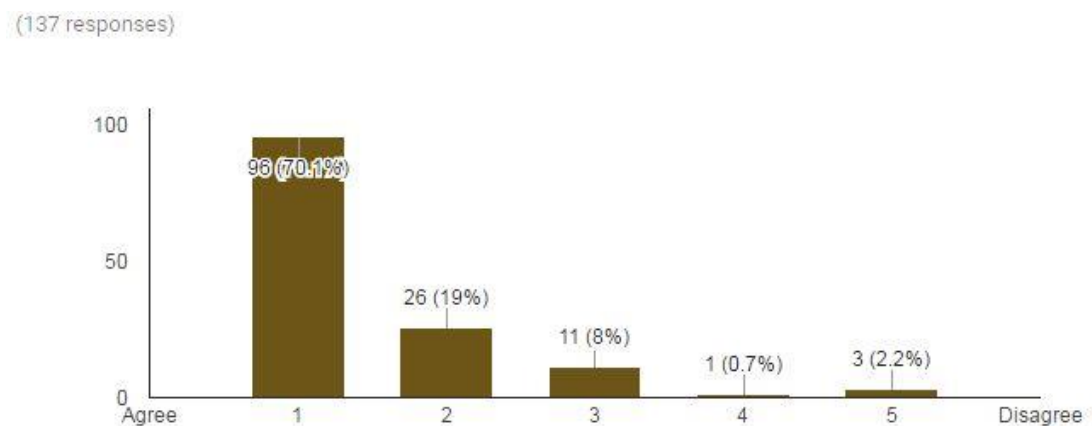


Figure 18 User responses: Question on Improper access 1

137 responses were recorded where 70.1% agreed to the statement and 19% partially agreed as well. Only 2.2% disagree with the statement.

Observation: Most of the consumers also agree that automakers or third parties should have a secure way to store data. If data is secure then there will be an increase in trusting belief hence the intention of the consumers to reveal personal information will be positive (hypothesis 5).

Global information privacy concern:

On a scale of 1 to 5: To what extend do you trust automakers in terms of information privacy? Such as having access to user-introduced data (e.g. GPS location) and vehicle-recorded data (e.g. how much brake fluid is left). Five point linear scale were introduced where 1=I trust them and 5= I do not trust them.

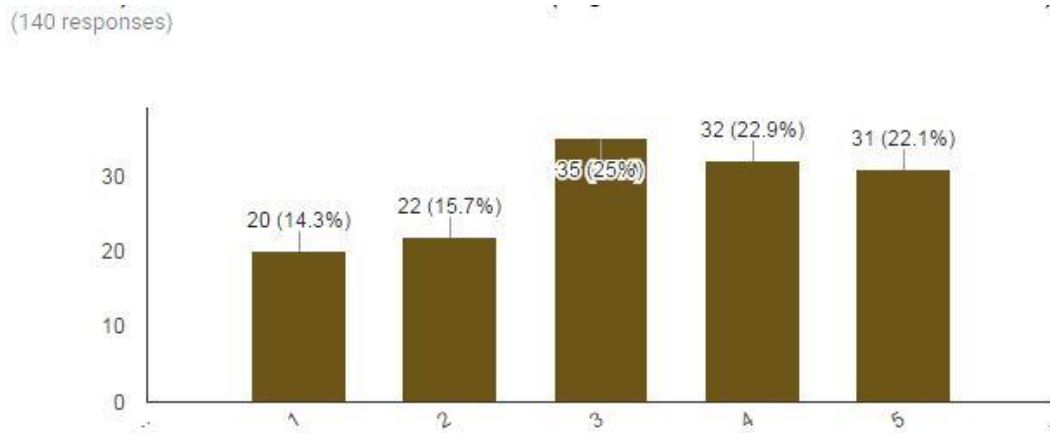


Figure 19 User responses: Question on Global information privacy concern 1

140 responses were recorded where 14.3% trust the automaker and 15.7% partially trust the automaker as well. 25% respondents were neutral and a combination of 45% (22.9% + 22.1%) respondents do not trust the automakers in terms of information privacy.

Observation: Little less than fifty percent responders do not trust their automakers or third parties in terms of information privacy. This supports hypothesis 5 where the risk belief will have negative effect on intention to reveal personal information. Also hypothesis 3, that trusting beliefs will have a negative effect on risk beliefs.

5.2 Attack surfaces

Automotive attack surfaces have been discussed in depth in the previous chapters. 5-point scale questions were asked to the respondents about their regular usages in their cars. The results are illustrated below:

How often do you connect your phone via Bluetooth or similar technologies to your car? 5-point scale where 1=Always, 2=Often, 3=Sometimes, 4=Seldom, 5=Never

(140 responses)

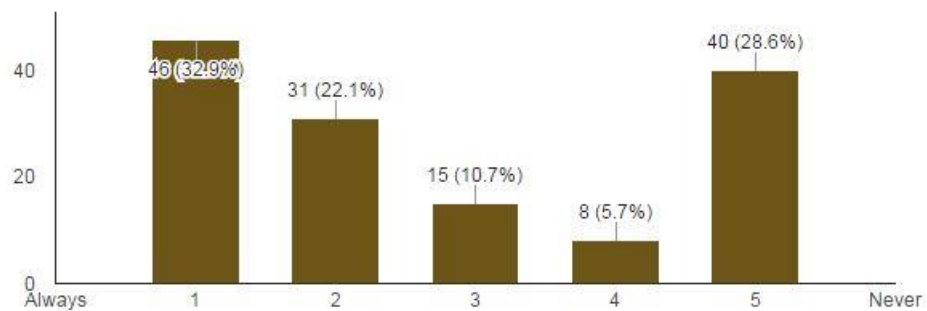


Figure 20 User responses: Question on usage of Bluetooth

140 responses were recorded using Google Forms where 32.9% uses Bluetooth or similar technologies always in their cars, 22.1% use it often and 28.6% never use it in their vehicles.

How often do you use the following features in your car? TPMS (Tire pressure monitoring system). 5-point scale where 1=Always, 2=Often, 3=Sometimes, 4=Seldom, 5=Never

(140 responses)

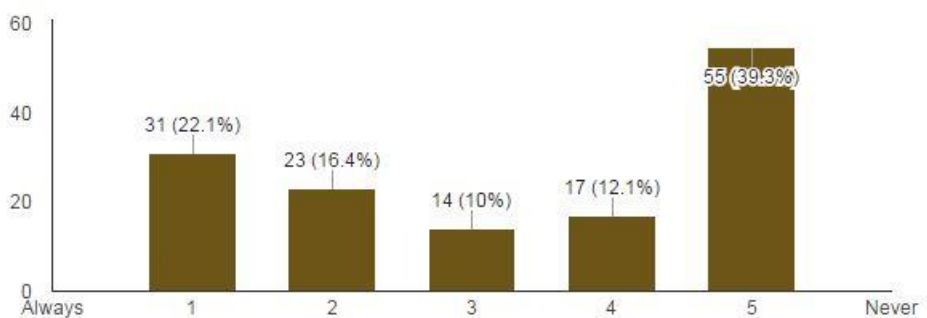


Figure 21 User responses: Question on usage of TPMS

Out of 140 responses recorded via the online questionnaire, tire pressure monitoring system or TPMS has always been used by 22.1% but almost half of the respondents (39.3 + 12.1 = 51.4%) seldom or never use it in their cars to check their tire pressure.

In-built GPS/Navigator. 5-point scale where 1=Always, 2=Often, 3=Sometimes, 4=Seldom, 5=Never

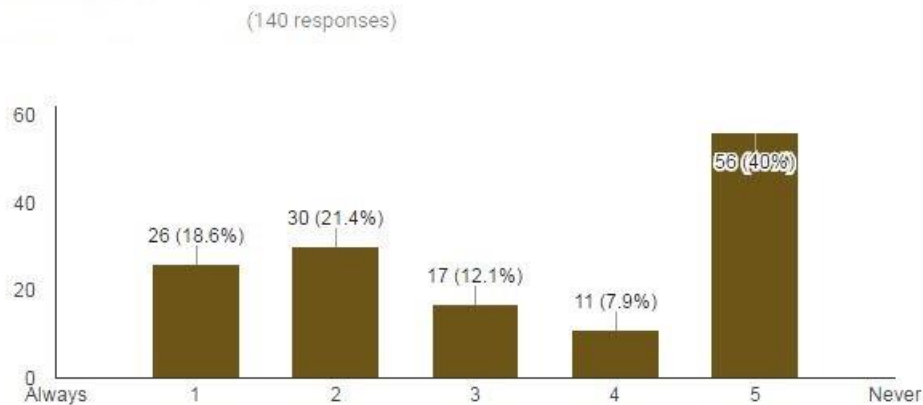


Figure 22 User responses: Question on usage of In-built GPS/Navigator

In built GPS-Navigator has been always used by 18.6% of recorded 140 respondents. 21.4% often use it and 40% respondents never use it. 12.1% respondents sometimes use the technology. It is assumed that they have it installed in their vehicle and use it when needed to.

DVD player/Music system. 5-point scale where 1=Always, 2=Often, 3=Sometimes, 4=Seldom, 5=Never

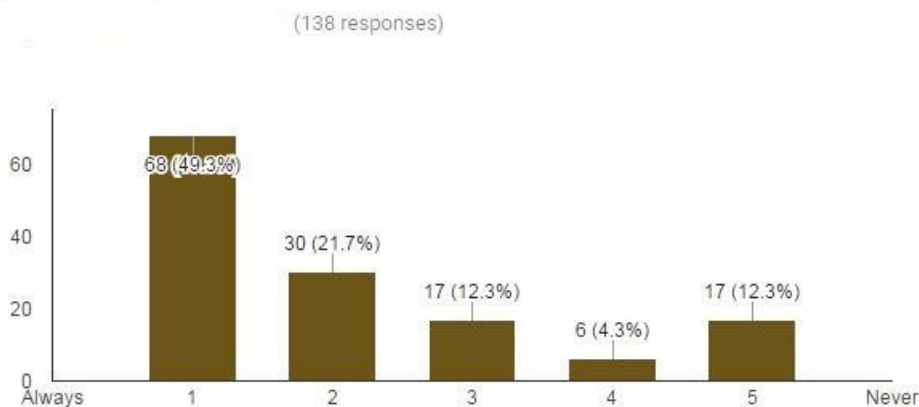


Figure 23 User responses: Question on usage of DVD player/Music system

138 responses were recorded where more than 70% respondents use their car entertainment system regularly. Only about 18% seldom or never use it.

Lane changing assistance / Automatic parallel parking. 5-point scale where 1=Always, 2=Often, 3=Sometimes, 4=Seldom, 5=Never

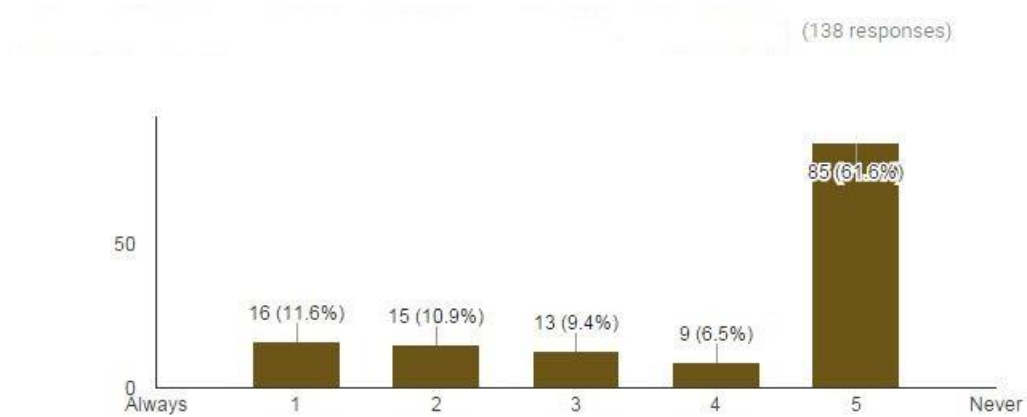


Figure 24 User responses: Question on usage of Lane changing assistance / Automatic parallel parking

Lane changing assistance and automatic parallel parking are still very new features offered in modern cars and they are mostly installed in the high end or limited models. More than 65% respondents out of 138 seldom or never use it. It is assumed that they do not have it equipped in their cars.

Mobile phone integration. 5-point scale where 1=Always, 2=Often, 3=Sometimes, 4=Seldom, 5=Never

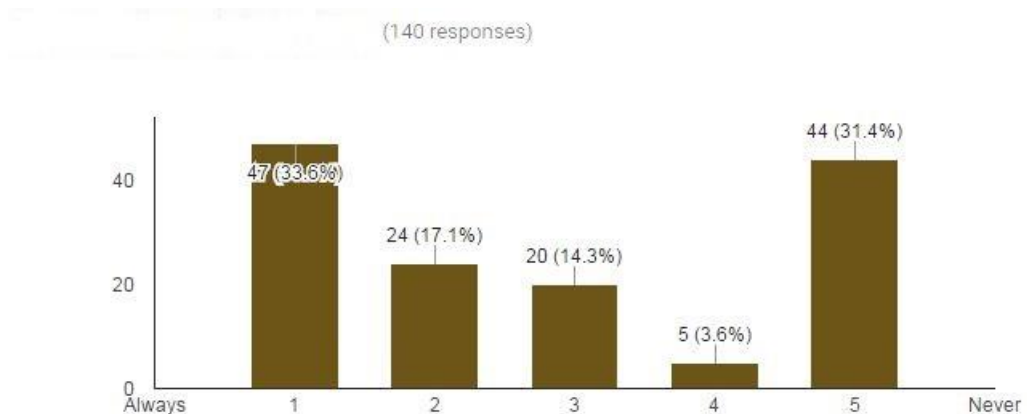


Figure 25 User responses: Question on mobile phone integration

Mobile phone integration is the process of connecting the phone via wireless technologies (Bluetooth) or wired technologies (3.5mm audio cable, USB cable) to the vehicle's infotainment system in order to use various services. The services can range from playing music from the cellphone to sync the cellphone's user interface (UI) to the vehicle UI. By syncing the cellphone to the vehicle, the user can access phonebook and call someone just by using the vehicle's touchscreen UI. Out of 140 respondents, 33.6% always use this technology and 17.1% often use it. About 31% respondents never use this technology to sync their phone to the vehicle.

What third party devices do you use in your car?

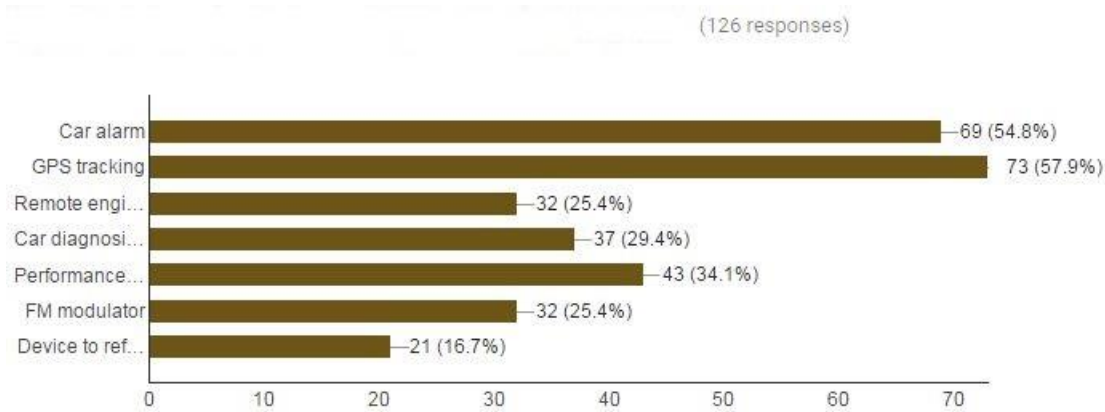


Figure 26 User responses: Question on usage of Third party devices

Of 126 respondents:

Car alarm – used by 54.8%

GPS tracking – used by 57.9%

Remote engine shut down – used by 25.4%

Car diagnosis via OBD-II – used by 29.4%

Performance monitor – used by 34.1%

FM modulator – used by 25.4%

Device to reflect driving behavior (for insurance purposes) – used by 16.7%

Observation: Most of the automotive consumers use devices or technologies which has an attack surface that can damage their vehicles. A maximum number of respondents use Bluetooth technologies alone or to integrate their cellphones to the cars. It has been studied earlier that any of these technologies are fairly hackable and consumers' privacy is at stake.

5.3 Awareness among consumers

Few questions were also asked about the awareness of the consumers about data collections, privacy and the trend of automotive hacking. They were also asked if there is a tool available to enhance automotive security, then which data will they allow to send and how much are they willing to pay for that service.

Security information and event management (SIEM) is an IT security approach to analyze logs and data to get a holistic approach of a system. Most of the SIEM systems deploy by collecting and analyzing logs from a system and look for anomalies and security breaches (Rouse 2015). Intrusion detection systems also fall under the subcategories of SIEM.

Did you know that 35% of vehicles already has technologies from manufactures that can collect driving history information? Options were Yes or No radio buttons.

(140 responses)

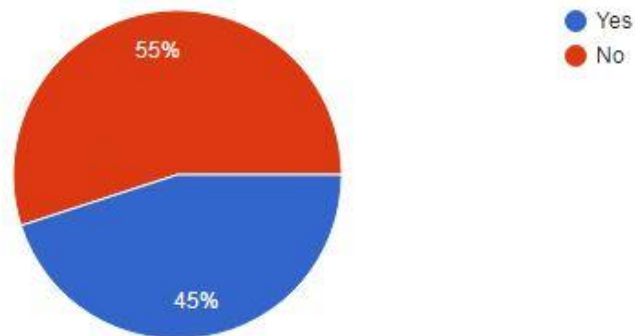


Figure 27 User responses: Question on awareness 1

Did you know that any of the above mentioned technology is fairly hackable?

(141 responses)

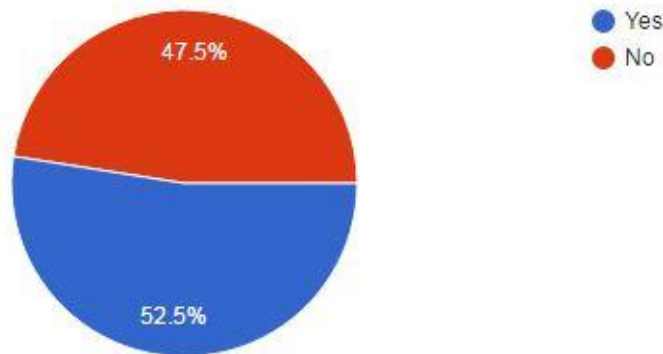


Figure 28 User responses: Question on awareness 2

If there is a SIEM tool available to enhance your automotive security, what data will you allow to pass to the provider?

(139 responses)

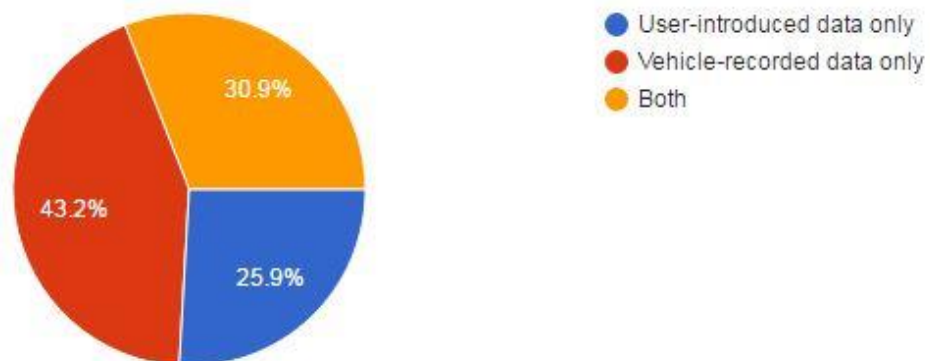


Figure 29 User responses: Question on awareness 3

A question has been asked to the consumers in the survey about possible money they are willing to spend per month to avail a service that can help to minimize automobile hacking and privacy issues. A total of 125 respondents replied in Canadian dollars, Euros, Bangladeshi taka and American Dollars. A conversion has been done to baseline all the currency to Canadian Dollar and few outliers are eliminated. The outliers that were excluded from the research are Canadian dollar \$500 and \$1000 from two respondents. The reason they were eliminated from the calculation is it is indeed a huge amount to pay per month aforementioned services and it doesn't sound practical.

How much are you willing to pay per month for that service? please enter your amount and mention the currency too (Can \$, Euro, etc.)

(125 responses)

The mean or average of this 123 responses were calculated to be Canadian dollar \$20.66 and the standard deviation is calculated to be 32.36. Although the standard deviation and the mean are independent of each other, still the standard deviation is a very large number for this data set. The probable explanations are:

1. Population is not large enough: The 123 responses might be not large enough to study this observation.
2. Privacy perception differs: Privacy perception differs from people to people, with age, education level (Madden 2014) and also countries. This was one of the limitations of this online survey of not to include the covariant such as responders age, education and country of residence. It can be included in any future work.

Observation: 55% consumers do not know that almost 35% vehicles in road has the capabilities to collect driving histories. About half of the respondents know that most of these automotive technologies are fairly hackable. That supports the fact that there are lack of awareness about information privacy. There is demand for cybersecurity services for automobiles and the consumers are willing pay a certain amount to avail it.

6 CONCLUSIONS

Cars are the primary mode of transportation in most of the developed countries. Its usage has been increased as there are variety of models available in the market in respect of prices and sizes. With the advancement of technologies and our dependencies on it, almost all of the modern cars are technologically suffice. But with great power comes great responsibilities (Know Your Meme 2015) and hence those technologies will be misused if not guarded well. This research focused on the vulnerabilities, attack surfaces and methods in modern automobiles and performed a study on it. It also look into the privacy aspect of the consumers who are using those vehicles. Online survey was the empirical data analysis methods and the data analysis was used to support the two research questions of this study.

1. What are the attack surfaces and methods in automotive systems and network? How many of them are currently used by automotive consumers? (R1)
2. In which consumer's privacy scale and/or model do automotive consumer privacy falls? (R2)

The first research question R1 asked about the attack surfaces and methods in automotive systems and network. It was well explained in chapter three. Survey analysis was conducted to answer the later part of R1. We were able to find an estimation of automotive consumers using technologies with wide open attack surfaces.

The second research question R2 was illustrated by matching the internet consumers' privacy IUIPC scale model and check if automotive consumers' privacy follows the same trend as the hypotheses of the IUIPC model. Survey results were used to support the data analysis and it is found that the hypotheses are aligned.

6.1 Discussions on hypotheses

A detail analysis on the survey results are illustrated in the previous chapter. Responses were recorded via Google Forms and statistical analyses have been performed. This study was done based on hypotheses which were stated in chapter 1. The hypotheses are:

Hypothesis 1: Automotive users' information privacy concerns will have a negative effect on trusting beliefs.

Hypothesis 2: Automotive users' information privacy concerns will have a positive effect on risk beliefs.

Hypothesis 3: Trusting beliefs will have a negative effect on risk beliefs.

According to the survey data analysis there is strong indication that the automotive users' privacy concerns will have a negative effect on trusting beliefs of the users and hence this hypothesis is accepted. Since hypothesis 1 is accepted and when the trusting beliefs of the users have a negative effect, it automatically gives a positive effect on risk beliefs, hence hypothesis 2 is also accepted. Hypothesis 1 implies on hypothesis 2 which indirectly implies that trusting beliefs will have a negative effect on risk beliefs, hence hypothesis 3 is accepted.

Hypothesis 4: Trusting beliefs will have a positive effect on intention to reveal personal information.

Hypothesis 5: Risk beliefs will have a negative effect on intention to reveal personal information.

If a user or consumer of automobile trusts their auto manufacturers or third parties, then they will reveal personal information to them and hence trusting beliefs will have a positive effect and on the other hand risk beliefs will have a negative effect. The survey results demonstrated in chapter 5 supports the hypotheses positively and hence hypothesis 4 and 5 are accepted.

Hypothesis 6: An automotive manufacturer or third party's request for more sensitive information will have a negative effect on trusting beliefs.

Hypothesis 7: An automotive manufacturer or third party's request for more sensitive information will have a positive effect on risk beliefs.

Hypothesis 8: An automotive manufacturer or third party's request for more sensitive information will have a negative effect on intention to reveal personal information.

From the data analysis of the survey it has been established that the automotive manufactures request for more information to the consumers will have a negative effect on trust beliefs and a positive effect on risk belief. That means the consumers will less trust the automotive manufacturers and hence the risk will increases among them. It also will stop them to have the intention to reveal personal information to the automotive manufactures. Hence hypothesis 6, 7 and 8 are accepted.

6.2 Future work

The future work in order to improve this thesis would be to add covariates such as age, sex, education and countries while using survey questionnaires. It should also be very helpful to have a sample size which is bigger than five hundred respondents so that the confidence level will be more and error margins in data collection will be less. Practical analysis of some intrusion detection systems or SIEM tools can also be very helpful to the research. Tools that are secure in nature and will transmit data from a vehicle in encrypted form. Automotive consumers' awareness can also be studied in greater depth as it is one of the primary factors to mitigate intrusions in automotive networks.

This research studied the attack surfaces and methods in automotive networks and matched an established privacy model that is analysed to be well aligned with automotive consumers' privacy.

7 REFERENCES

- Automotive Ethernet: An Overview (2014) Ixia Worldwide Inc. White paper Rev A, May 2014, 9.
- Bar-El, Hagai (2014) Introduction to Side Channel Attacks, Discretix Technologies Ltd. White paper, 2-3.
- Barengi, Alessandro - Breveglieri, Luca - Koren, Israel - Naccache, David (2012) Fault Injection Attacks on Cryptographic Devices: Theory, Practice, and Countermeasures. In: *Proceedings of the IEEE*, Volume 100 Issue 11, 3056-3076.
- Bhattacharjee, Anol Ph.D. (2012) Social Science Research: Principles, methods, and practices. Creative Commons Attribution-NonCommercial-ShareAlike 3.0 Unported License
- Bird, Colin (2016) Over-the-Air Updates to Become Commonplace in Vehicles. Original Equipment Suppliers Association.
<<http://www.oesa.org/Publications/OESA-News/August-2015/ver-the-Air-Updates-to-Become-Commonplace-in-Vehicles.html>>, retrieved 20.12.2015.
- Brown, David A. - Cooper, Geoffrey - Gilvarry, Ian - Rajan, Anand - Tatourian, Alan - Venugopalan, Ramnath - Wheeler, David - Zhao, meiyuan (2015) Automotive Security Best Practices Recommendations for security and privacy in the era of the next-generation car, Intel Security Inc. White paper, 6-11.
- Business Dictionary (2015) Strategy. Business Dictionary.
<<http://www.businessdictionary.com/definition/strategy.html>>, retrieved 23.04.2016.
- Carsten, Paul - Andel, Todd R. - Yampolskiy, Mark - McDonald, Jeffrey T. (2015) In-Vehicle Networks: Attacks, Vulnerabilities, and Proposed Solutions. *Proceedings of the 10th Annual Cyber and Information Security Research Conference Article No. 1*. <<http://dl.acm.org/citation.cfm?id=2746267>>, retrieved 20.9.2015.
- Carsten, Paul - Andel, Todd R. - Yampolskiy, Mark - McDonald, Jeffrey T. (2015) In-Vehicle Networks: Attacks, Vulnerabilities, and Proposed Solutions. *Proceedings of the 10th Annual Cyber and Information Security Research Conference Article No. 1*. <<http://dl.acm.org/citation.cfm?id=2746267>>, retrieved 20.9.2015.

- Carsten, Paul – Todd, Andel R. – Mark, Yampolskiy - McDonald, Jeffrey T. - Russ, Samuel (2015) A system to recognize intruders in controller area network (CAN). In: *Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research* Pages 111-114.
- Caudill, Eve M. – Murphy, Patrick E (2000) Consumer Online Privacy: Legal and Ethical Issues. *Journal of Public Policy & Marketing*, Vol. 19 (1), 7–19.
- Charette, Robert N. (2009) This Car Runs on Code. *IEEE Spectrum*.
<<http://spectrum.ieee.org/transportation/systems/this-car-runs-on-code>>, retrieved 15.11.2015.
- Checkoway, Stephan - McCoy, Damon - Kantor, Brian - Anderson, Danny - Shacham, Hovav - Savage, Stefan - Koscher, Karl - Czeskis, Alexei - Roesner, Franziska - Kohno, Tadayoshi (2011) Comprehensive Experimental Analyses of Automotive Attack Surfaces. In: *Proceedings of the National Academy of Sciences Committee on Electronic Vehicle Controls and Unintended Acceleration*, March 3–4, 2011.
- Corrigan, Steve (2008) Introduction to the Controller Area Network (CAN). *Texas Instruments Application Report*, SLOA101A, 3.
- Data privacy: what the consumer really thinks 2012. Direct Marketing Association (UK). <http://dma.org.uk/uploads/Data%20privacy%20-%20What%20the%20consumer%20really%20thinks%202012_53cfd432518f2.pdf>, retrieved 20.4.2016.
- Data privacy: what the consumer really thinks 2015. Direct Marketing Association (UK). <http://dma.org.uk/uploads/ckeditor/Data-privacy-2015-what-consumers-really-thinks_final.pdf>, retrieved 20.4.2016.
- Dowling, Grahame R. – Staelin, Richard (2001) A Model of Perceived Risk and Intended Risk-Handling Activity. *Journal of Consumer Research*, Vol. 21 (1), 119-134.
- Eck, Wim V. (1985) Electromagnetic radiation from video display units: an eavesdropping risk?. *Journal of Computers and Security*, Volume 4 Issue 4, 269-286.
- Fallstrand, Daniel – Lindström, Viktor (2015) *Applicability analysis of intrusion detection and prevention in automotive systems*. Master's thesis. Chalmers University of Technology, Gothenburg.

- Fehr, Walton (2015) Overview of Dedicated Short Range Communications (DSRC) Technology. United States Department of Transportation.
<<http://www.its.dot.gov/DSRC/>>, retrieved 20.12.2015.
- Foxman, Ellen R. – Kilcoyne, Paula (1993) Information Technology, Marketing Practice, and Consumer Privacy: Ethical Issues. *Journal of Public Policy & Marketing*, Vol. 12 (1), 106-119.
- Framework for Automotive Cybersecurity Best Practices 2014. Alliance of Automobile Manufacturers.
<<http://www.autoalliance.org/index.cfm?objectid=1E518FB0-BEC3-11E5-9500000C296BA163>>, retrieved 25.02.2016.
- Frenzel, Lou. (2013) Fundamentals of Communications Access Technologies: FDMA, TDMA, CDMA, OFDMA, AND SDMA. Electronic Design.
<<http://electronicdesign.com/communications/fundamentals-communications-access-technologies-fdma-tdma-cdma-ofdma-and-sdma>>, retrieved 02.10.2015.
- Gil, Paul (2013) What is 'pwned'?. About Tech.
<<http://netforbeginners.about.com/od/p/f/pwned.htm>>, retrieved 22.11.2015.
- Hoppe, Tobias – Kiltz, Stefan – Dittmann, Jana (2010) Security threats to automotive CAN networks—Practical examples and selected short-term countermeasures. In: *Reliability Engineering and System Safety*, 11–25.
- Hori, Yoshijiro - Sasaki, Yoshihiro - Miyamatsu, Isao - Yakura, Shinji (2000) Development of Intrusion Detection Sensor for Vehicle Anti-theft Systems. Fujitsu Ten Technology Journal, No 14.
- Howard, John D. - Longstaff, Thomas A. (1998) A Common Language for Computer Security Incidents. Sandia Report, Sandia National Laboratories SAND98-8667 Unlimited Release.
<<http://www.osti.gov/scitech/servlets/purl/751004/>>, retrieved 20.11.2015.
- Know Your Meme (2015) <<http://knowyourmeme.com/memes/with-great-power-comes-great-responsibility>>, retrieved 24.4.2016.
- Kocher, Paul C. (1996) Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In: *Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology*, 104-113.

Koscher, Karl – Czeskis, Alexei – Roesner, Franziska - Patel, Shwetak - Kohno, Tadayoshi (2010) Experimental Security Analysis of a Modern Automobile. IEEE Symposium on Security and Privacy.

Koscher, Karl (2014) Securing Embedded Systems: Analyses of Modern Automotive Systems and Enabling Near-Real Time Dynamic Analysis. Computer Science and Engineering, University of Washington, 26-29

LIN Specification Package Revision 2.1. LIN Consortium, 2006.
<http://tge.cmaisonneuve.qc.ca/barbaud/R%C3%A9f%C3%A9rences%20techniques/Bus%20LIN/LIN-Spec_Pac2_1.pdf>, retrieved 2.10.2015

Ling, Congli – Feng, Dongqin (2012) An Algorithm for Detection of Malicious Messages on CAN Buses. In: *Proceedings of 2012 National Conference on Information Technology and Computer Science*, doi:10.2991/citcs.2012.161.

Lish, Tom. (2015) 6 things OEM design engineers need to know. Setra.
<<http://www.setra.com/blog/6-things-oem-design-engineers-need-to-know/2014/11/06>>, retrieved 06.10.2015.

Madden, Mary (2014) Americans' Perceptions of Privacy are Varied. Pew Research Center. <<http://www.pewinternet.org/2014/11/12/americans-perceptions-of-privacy-are-varied/>>, retrieved 23.04.2016.

Malhotra, Naresh K. – Kim, Sung S. – Agarwal, James (2004) Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, Vol. 15 (4), 336–355.

McCarthy, Charlie – Harnett, Kevin (2014) Risk Management Framework Applied to Modern Vehicles. National Institute of Standards and Technology (NIST) Cybersecurity, DOT HS 812 073.

Microsoft Developer Network (2016) *Ensuring Data Integrity with Hash Codes*. Microsoft Developer Network. <[https://msdn.microsoft.com/en-us/library/f9ax34y5\(v=vs.110\).aspx](https://msdn.microsoft.com/en-us/library/f9ax34y5(v=vs.110).aspx)>, retrieved 20.02.2016.

Miller, Dr. Charlie. - Valasek, Chris (2015) Remote Exploitation of an Unaltered Passenger Vehicle. <<http://illmatics.com/Remote%20Car%20Hacking.pdf>>, retrieved 25.10.2015.

Murphy-Edward V. - Murphy, M. Maureen – Seitzinger, Michael V. (2015) Bitcoin: Questions, Answers, and Analysis of Legal Issues. Congressional Research Service, 7-5700.

- Murray, Sarah (2013) Ethernet in Cars Lowers Cost of Life-Saving Backup Camera Tech. Broadcom. <<http://www.broadcom.com/blog/automotive-technology-2/ethernet-in-cars-lowers-cost-of-life-saving-backup-camera-tech/>>, retrieved 20.12.2015.
- Myers, Michael D. - Avison, David (2002) *Introducing Qualitative Methods series*. SAGE Publications Ltd, Los Angeles.
- Nilsson, Dennis K. - Phung, Phu H. - Larson, Ulf E. (2014) Vehicle ECU classification based on safety-security characteristics. *Road Transport Information and Control-RTIC 2008 and ITS United Kingdom Members' Conference, IET*. <https://www.researchgate.net/publication/4348340_Vehicle_ECU_classification_based_on_safety-security_characteristics>, retrieved 23.9.2015.
- Nowak, Glen – Phelps, Joseph (1995) Direct marketing and the use of individual-level consumer information: Determining how and when “privacy” matters. *Journal of Public Policy & Marketing*, Vol. 9 (3), 46–60.
- Oguma, Hisashi – Yoshioka, Akira - Nishikawa, Makoto - Shigetomi, Rie - Otsuka, Akira - Imai, Hideki (2008) New Attestation Based Security Architecture for In-Vehicle Communication. In: *Proceedings of IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference*, 1-6.
- OWASP (2015) Attack Surface Analysis Cheat Sheet. OWASP. <https://www.owasp.org/index.php/Attack_Surface_Analysis_Cheat_Sheet>, retrieved 15.11.2015.
- Pagliery, Jose (2014) A Your car is a giant computer - and it can be hacked. CNN Money. <<http://money.cnn.com/2014/06/01/technology/security/car-hack/>>, retrieved 10.01.2016.
- Papenfuss, John J. (2015) Car hacking report refuels concerns about Michael Hastings crash. Who.What.Why. <<http://whowhatwhy.org/2015/02/20/car-hacking-report-refuels-concerns-michael-hastings-crash/>>, retrieved 20.04.2016.
- Pathan, Al-Sakib Khan (2014) *The State of the Art in Intrusion Prevention and Detection*. Auerbach Publications, Boston.
- Phelps, Joseph – Nowak, Glen - Ferrell, Elizabeth (2000) Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing*, Vol. 19 (1), 27–41.
- Pickard, Alison Jane (2013) *Research Methods in Information*. Facet Publishing, London

Prathap, Vijaiya - Rachumallu, Abhishake (2013) Penetration Testing of Vehicle ECUs. Gothenburg : Chalmers University of Technology, 2013. 39 pp.
<<http://studentarbeten.chalmers.se/publication/184988-penetration-testing-of-vehicle-ecus>>, retrieved 23.9.2015.

Rogers, Paul G. (1990) EPA History: The Clean Air Act of 1970. *United States Environmental Protection Agency EPA Journal - January/February 1990*.
<<https://www.epa.gov/aboutepa/epa-history-clean-air-act-1970>>, retrieved 20.9.2015.

Rouse, Margaret (2015) Security information and event management (SIEM). TechTarget Search Security.
<<http://searchsecurity.techtarget.com/definition/security-information-and-event-management-SIEM>>, retrieved 23.04.2016.

Saeedi, Ehsan – kong, Yinan (2014) Side-channel Vulnerabilities of Automobiles. *Transaction on IoT and Cloud Computing* Vol 2 No 2, 1-8.

Saltzman, Aaron (2015) Ajusto app that watches your driving habits leads to privacy concerns. CBC News Business. <<http://www.cbc.ca/news/business/ajusto-app-that-watches-your-driving-habits-leads-to-privacy-concerns-1.3019787>>, retrieved 10.01.2016.

Sauerwald, Mark (2014) CAN bus, Ethernet, or FPD-Link: Which is best for automotive communications?. *Analog Applications Journal*, 1Q 2014, 20–24.

Schulze, Sandro – Pukall, Mario - Saake, Gunter - Hoppe, Tobias Christian, Dittmann, Jana (2009) On the Need of Data Management in Automotive Systems. In: *Proceedings of Datenbanksysteme in Business, Technologie und Web (BTW 2009)*, 13. Fachtagung des GI-Fachbereichs "Datenbanken und Informationssysteme" (DBIS), 2–6.

Smith, Craig (2014) Car Hacker's Manual. Theia Labs, 45-49.

Smith, H. Jeff – Milberg, Sandra J. – Burke, Sandra J. (1996) Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Quarterly*, Vol. 20 (2), 167–196.

Smith, Randy Frankin. (2015) The 3 Pillars of Information Security, Confidentiality, integrity, and availability. Windows IT Pro.
<<http://windowsitpro.com/security/3-pillars-information-security>>, retrieved 08.10.2015.

Software updates. Tesla Motors Inc.

<https://www.teslamotors.com/en_GB/support/software-updates>, retrieved 15.11.2015.

Stewart, Kathy A. – Segars, Albert H. (2002) An Empirical Examination of the Concern for Information Privacy Instrument. *Inform*, Vol. 13 (1), 36-49.

Stoneff, Chris (2015) The Seven Steps of a Successful Cyber Attack. Infosec Institute. <<http://resources.infosecinstitute.com/the-seven-steps-of-a-successful-cyber-attack/>>, retrieved 20.11.2015.

Tech Terms (2016) Firmware. Sharpened Productions.

<<http://techterms.com/definition/firmware>>, retrieved 01.01.2016.

Technology. Accelerate cooperative mobility, DRIVE C2X. <<http://www.drive-c2x.eu/technology>>, retrieved 04.10.2015.

The OBD II Home Page (2011) OBD-II Background. The OBD II Home Page. <<http://www.obdii.com/background.html>>, retrieved 25.12.2015.

Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk (2015) Office of the Senator Edward J. Markey (D-Massachusetts), 3, 8.

Updating Car ECUs Over-The-Air (FOTA) (2011) Red Bend Ltd. White paper, 2, 7.

Vestlund, Christian (2014) *Intrusion Detection Systems in Networked Embedded Systems*. TDDD17 ADIT. Department of Computer and Information Science, Linköpings universitet

Vyleta, Bc. Petr (2014) Automated penetration testing in automotive industry. Archive theses, Czech Technical University in Prague. <https://dip.felk.cvut.cz/browse/pdfcache/vyletpet_2014dipl.pdf>, retrieved 20.9.2015.

Vyleta, Bc. Petr (2014) Automated penetration testing in automotive industry. Archive theses, Czech Technical University in Prague. <https://dip.felk.cvut.cz/browse/pdfcache/vyletpet_2014dipl.pdf>, retrieved 20.9.2015.

Westin, Alan F. (1967) *Privacy and Freedom*. Atheneum, New York.

Wolf, Marko - Weimerskirch, André - Paar, Christof (2004) Security in Automotive Bus Systems. Workshop on Embedded Security In Cars (ESCAR)'04.

<<http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.92.728&rep=rep1&type=pdf>>, retrieved 22.9.2015.

Wulf, Krisof De – Odekerken-Schroder, Gaby - Iacobucci, Dawn (2001) Investments in Consumer Relationships: A Cross-Country and Cross-Industry Exploration. *Marketing*, Vol. 64 (4), 33-50.

Yoshida, Junko. (2013) Ethernet Backbone in Car: Hype or Reality?. EE Times. <http://www.eetimes.com/document.asp?doc_id=1319157>, retrieved 03.10.2015.