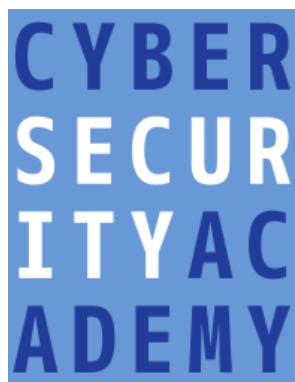


Multi actor roadmap to improve cyber security of consumer used connected cars

Cyber Security Academy
Executive Cyber Security program



Drs. Herbert Leenstra
S1727834
Telephone number: 06-12946726
E-mail: Herbert.Leenstra@kpn.com
Date of submission: 03-01-2017

Supervisor university:
Prof. dr. ir. Jan van den Berg
Prof. dr. Bert van Wee

Abstract

The automotive industry will introduce the autonomous car into the consumer market in the near future. At this moment, several forms of connected cars are introduced. These connected cars present the current state of the art on the path to the ultimate goal of the automotive industry: the consumer used autonomous car. Prior research shows that consumers have several concerns on the use of connected and autonomous cars. The system security of the connected car is one of these concerns. There are currently 7 million consumer used cars in possession of Dutch citizens. Consumer trust is key for a successful introduction of connected – and autonomous cars into the consumer market. These concerns have to be addressed by the automotive industry in order to successfully introduce the autonomous car. When we compare the consumer concerns with the actions of the automotive industry, it becomes clear that the security concern is currently not properly addressed. This threatens the successful introduction of autonomous cars in the future.

This research presents a multi actor roadmap which indicates what actions each actor in the automotive industry can take to address and improve the security of connected cars.

In order to do this we show that there are technical security threats on the current implementation of connected cars. A separate paragraph describes the malicious actors that take advantage of these security flaws in the connected car design. The last part of our argument consists of the description of the actors and an analysis on their actions and interests. These elements, plus the consumer security concerns, deliver the design requirements that are needed to construct a multi actor roadmap that shows what each actor can contribute to improve the security of the connected car.

Five important elements must be solved in order to generate a more cyber secure car. The first element is that the government must answer the question of car data ownership and the question on how long cars must be patched by the car manufacturers. The second element is the implementation by the branch organisations of an auto ISAC in Europe. The fundamental redesign of the ICT architecture of the connected car by the car manufacturers is the third element. The fourth element is the logging of cyber security incidents by the insurance companies. Network providers must implement a secure 5G standard the automotive industry can use to communicate to and from the connected car. The last element is that car users must start asking questions about the cyber security of their car.

Key words: Cyber security, connected car, autonomous car, system security, cyber threats, threat landscape, car hacking, roadmap.

Acknowledgement

This research was an interesting journey that took almost a year to complete. In that timeframe I explored an interesting new subject: “looking into all cyber security related aspects of the automotive industry.” I visited several companies and talked to a lot of interesting people. During the process of writing this thesis, I received great support from a lot of experts. Interesting new insights were gained from these talks. I would like to thank all the experts and survey respondents for their cooperation and ideas. It is clear that the subject is new to a lot of people and that it triggers a lot of emotion in people’s hearts and minds. I would like to thank the experts in the automotive industry who delivered a lot of interesting knowledge and insights. Thanks to those of you who sent me emails and documents. By doing so you contributed to this end result that is now in front of you.

The Cyber Security Academy is a cooperation between Leiden University and Delft University. Special thanks to Andre Beijen and Edwin Jongejans of KPN who made it possible to work with the Cyber Security Academy of Leiden University and Delft University. Jan van den Berg, first supervisor, for his patience and his good advice. Bert van Wee, second supervisor, for his insights into the automotive industry. I also want to thank my family for their endless support and patience.

Table of Contents

Abstract	2
Acknowledgement.....	3
1. Introduction.....	6
1.1 Problem relevance.....	7
1.2 Assumptions and definitions	11
1.3 Scope	11
1.4 The objectives of the study	13
1.5 Research question	14
1.6 Sub questions	14
1.7 Methodology	15
1.7.1 Research design.....	16
1.7.2 Data sources.....	16
1.7.3 Data collection techniques.....	17
1.7.4 Sampling techniques	18
1.7.5 Ethical considerations	18
1.7.5.1 Confidentiality	18
1.7.6 Informed consent	18
2 Technical attack vectors and threat actors	19
2.1 Technical attack vectors	19
2.2 Threat actors	26
3 Actor analysis.....	31
3.1 Actor overview	31
3.2.1 Car manufacturers.....	31
3.2.1.1 Economic factors from car manufacturer perspective.....	33
3.2.2 Government	36
3.2.3 Insurance companies.....	40
3.2.4 Branch organisations.....	42
3.2.5 Network provider	43
3.2.6 Car user.....	46
3.2.6.1 Car users concerns.....	47
4 Multi actor roadmap to improve connected car security	51
4.1 Car manufacturers.....	52
4.2 Government	53

4.3 Insurance companies.....	54
4.4 Branch organisations.....	54
4.5 Network provider	55
4.6 Car users	55
5 Reflection.....	56
5.1 Looking back.....	56
5.2 Looking forward	58
5.2.1 Car manufacturers.....	58
5.2.2 Government	59
5.2.3 Insurance companies.....	60
5.2.4 Branch organisations.....	60
5.2.5 Network provider	61
5.2.6 Car users	61
6 Conclusion	62
6.1 Conclusion	62
6.2 Future Research.....	63
Bibliography.....	65
Appendices	70
Appendix 1: Survey.....	70
Survey part 1	70
Survey part 2	71
Survey part 3	73
Appendix 2: Survey structure, process and results.....	76
Appendix 3: Requirements overview	107
Appendix 4: Interview overview.....	111
Appendix 5: Bug hunting program rewards	112

1. Introduction

The automotive industry will introduce the autonomous car into the consumer market in the near future. At this moment, several forms of connected cars are introduced. These connected cars present the current state of the art on the path to the ultimate goal of the automotive industry: the consumer used autonomous car. Prior research¹ shows that consumers have several concerns on the use of connected cars. The system security of the connected car is one of these concerns. Consumer trust and social acceptance is key for a successful introduction of connected – and autonomous cars into the consumer market.² These concerns have to be addressed by the automotive industry in order to successfully introduce the autonomous car. When we compare the consumer concerns with the actions of the automotive industry, it becomes clear that the security concern is currently not properly addressed. Hackers can compromise the system security of the connected car. By hacking the connected car, hackers can influence the physical safety of the car user. This threatens the successful introduction of autonomous cars in the future.

The available literature on the cyber security of connected cars is limited. The literature that is available deals with either the technical aspects of hacking into connected car systems³ or deals with hacker profiling in general.⁴ The specific profiling of hackers of connected cars was not yet available. There is also no overall study available that deals with both aspects simultaneously. This research fills that gap. We analyse the technical attack vectors of the connected car and also profile the attackers. We look into the concerns of the car user and use that input as a guideline to construct a roadmap to improve the cyber security of the connected car. These three elements deliver requirements we use to construct a multi actor roadmap which indicates what actions each actor in the automotive industry can contribute to address and improve the security of connected cars.

The report by Dokic et al⁵ mentions the issues on autonomous cars. The issues mentioned concern data security, legal & liability, safety, economy and ethics. We cluster these elements in Safety, Security and Liability. These issues are directly related to the consumer trust in the connected car. The following picture shows an overview of the relations between the automotive actors that are capable of addressing the consumer concerns in order to improve the security of the connected – and autonomous car.

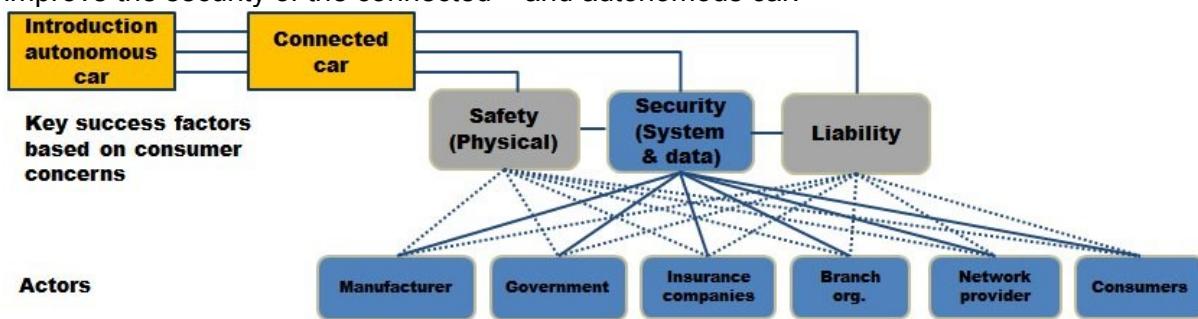


Fig 1. Multi actor diagram indicating the actors in relation to the consumer concerns of the connected– and autonomous car

We show that there are technical security threats in the current implementation of connected cars. A separate paragraph describes the malicious actors that take advantage of the security flaws in the connected car design. The next part of our argument consists of the description and analysis of the other actors, their behaviour and interests. These elements, plus the consumer security concerns, deliver the design requirements that are needed to

¹ ANWB, 2015

² Dokic, j., et al, 2015, p5

³ Checkoway, S et al., 2011; Valasek, C; Miller, C., 2013; Anderson, M., 2014; Smith, C. 2016

⁴ Gutierrez, M., 2014; Oosterbaan, W., Lei van der G., 2014; Verizon, 2016

⁵ Dokic, j., et al, 2015

construct a multi actor roadmap that shows what each actor can contribute to improve the security of the connected car.

1.1 Problem relevance

We can see the importance of the security of connected cars in daily lives. The Dutch CBS indicated that there are about 7 million consumer used cars in possession of Dutch consumers.⁶ The figures also show that about 71,5% of the Dutch households possesses at least one consumer used car.⁷ Connected cars are all around us in our society. We live in a connected world in which all kinds of devices get connected to the internet. Cars are no exception and also follow this trend. The possibility of connecting the car to the internet makes the car even more valuable to people. As the research by Steg⁸ shows, car users value their car, and dislike public transport, for three reasons. The first reason is that car users perceive their car as a better functional instrument to fulfil their personal requirements. The other reasons are that the car represents important cultural and psychological values. For many car users, the car is a symbol of freedom and independence. The car is often seen as a symbol of status. Driving a car is perceived as pleasurable and to be preferred above public transportation. By adding more functions to the car, like connecting the car to the internet, the car becomes even more valuable to the car user.

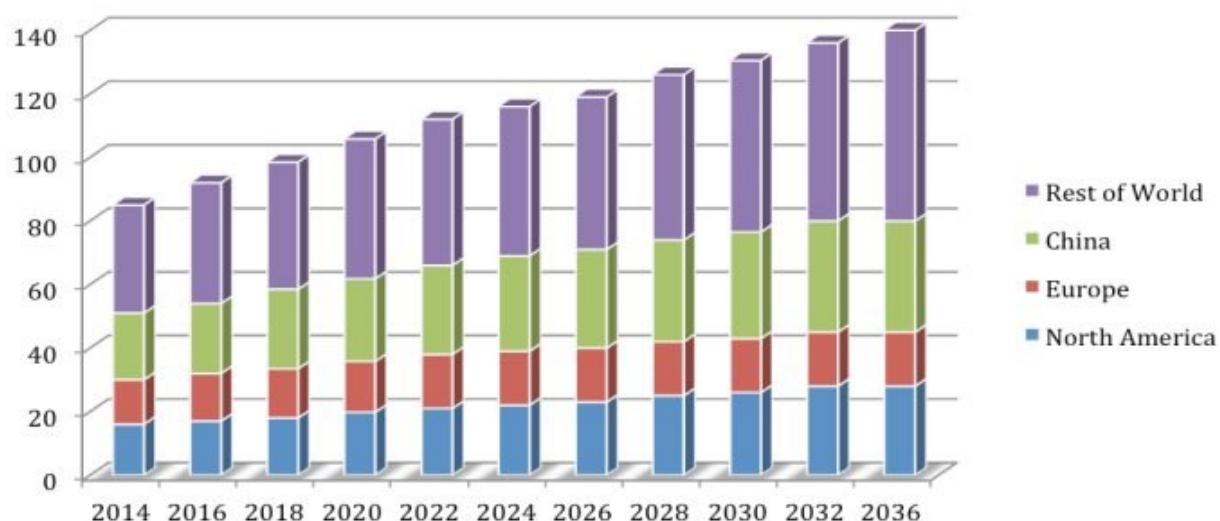


Fig. 2. Global market for cars, in millions, by region⁹

All car brands have recently introduced “main stream” connected cars. Examples of these are Volvo, Tesla, Nissan, Toyota, Volkswagen, Jeep, Chrysler and BMW. The consumer can interact with his connected car using mobile applications. The follow up in this trend is the careful introduction by car manufacturers of the autonomous car. In the autonomous car, the car user is no longer required to drive. The car drives and navigate by itself to the required destination. The main argument of introducing connected cars is about increasing the safety of the car. The claim is that the driver needs assistance in order to avoid accidents. The NHTSA published a report¹⁰ that shows that 94% of all accidents were driver related. Smith

⁶ CBS, Centraal Bureau voor de Statistiek, 2016.

⁷ CBS, 2015

⁸ Steg, L., 2003

⁹ Jiang, T., et al, 2015 p6

¹⁰ Singh, S., 2015

¹¹ refers in his article to several studies from 1979 till 2013 which all show that the driver is a major contributor to car accidents.

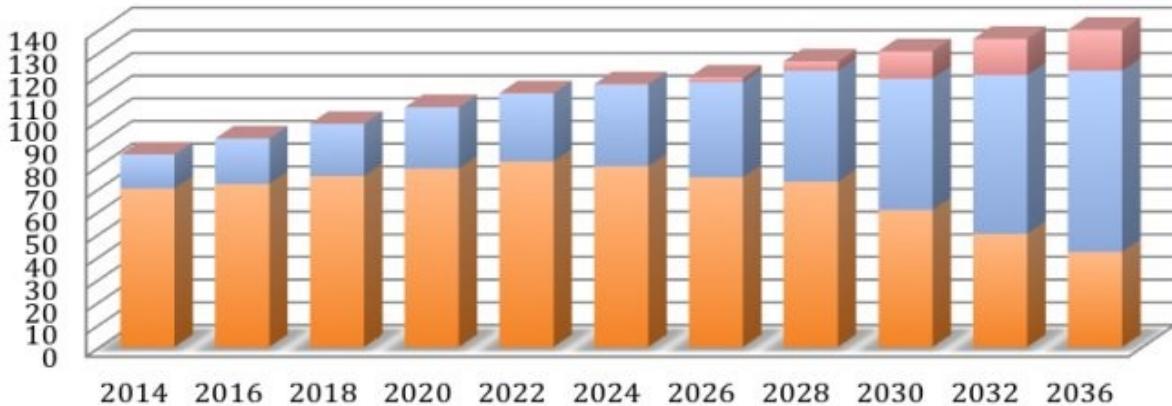


Fig. 3. Global Market for cars in mln, ■ Traditional driven car, ■ Semi-autonomous car, ■ Autonomous car¹²

IHS researchers predict 54 million autonomous cars in 2035. About 2.4 million of these cars will drive in Europe.¹³ Car manufacturers traditionally focus on car safety and user features like car navigation. The security element is, as is the current state of almost all cars, left out of the equation. This is remarkable because a recent international study by Kyriakidis¹⁴ in which 5000 people participated, shows that the three biggest consumer concerns are the possibility of misuse / hacking of the car software, legal issues and safety issues. Car manufacturers only address the car safety issue. The study also shows that 69 percent thinks that the autonomous car will have a market share of fifty percent before 2050. The results of this study are confirmed in a recent study by the ANWB in the Netherlands in 2015.

¹⁵ The Dutch respondents indicated to be concerned about the commercial use of collected car data (88%). The second concern was about hacking the car software (84%) and 94% wanted protective legislation.

The study by Heide¹⁶ predicts the introduction of the main stream autonomous car around 2021. The first argument used by the automotive industry for the rapid introduction of the connected car is that the car driver is unable to detect and respond quick enough to all the relevant traffic issues the driver encounters. The introduction of connected cars results in a more efficient use of the road and therefore result in less traffic jams. The third argument is that the car user has less stress in a connected car and more time to do other activities. These are exactly the claims Volvo makes in their autonomous car trials in 2017 in the UK and China. Volvo predicts less accidents, a reduction of traffic jams, less pollution and saving the valuable time of the car user. In case of the autonomous car, Volvo commits itself to make sure that in 2020 "no one will be seriously injured or killed in a new Volvo".¹⁷ The other thing that makes the Volvo experiment interesting is that Volvo will use production cars

¹¹ Smith, B., 2013

¹² Jiang, T., et al, 2015 p6

¹³ IHS Markit, 2014

¹⁴ Kyriakidis, M. et al., 2015

¹⁵ ANWB, 2015

¹⁶ Heide, A. et al., 2006

¹⁷ Volvo, 2016b

instead of special prototypes. The drivers in this experiment are regular people and not engineers. In order to keep the car users safe several systems are made redundant.¹⁸

Research by Kyriakidis in 2015¹⁹ shows that the respondents of the developed countries were also worried about the transmission of data from their car. The term “developed” in this study means that those countries have lower national accident statistics and the respondents have a higher income and higher education level. The study by Gonder²⁰ shows that the collection of car data and the possibility to profile the car users is possible and might indeed cause a serious privacy concern. Enev concluded in his research²¹ that a person could be identified with an accuracy of 87% by analysing the car data of a single sensor (brake) and a 99% accuracy when the data of five sensors are combined.

Our study aims to address the concern about car security by introducing a multi actor roadmap to improve the security of connected cars. The benefit for society is that the improvement of the security of the connected car will also improve the personal safety of the car user.

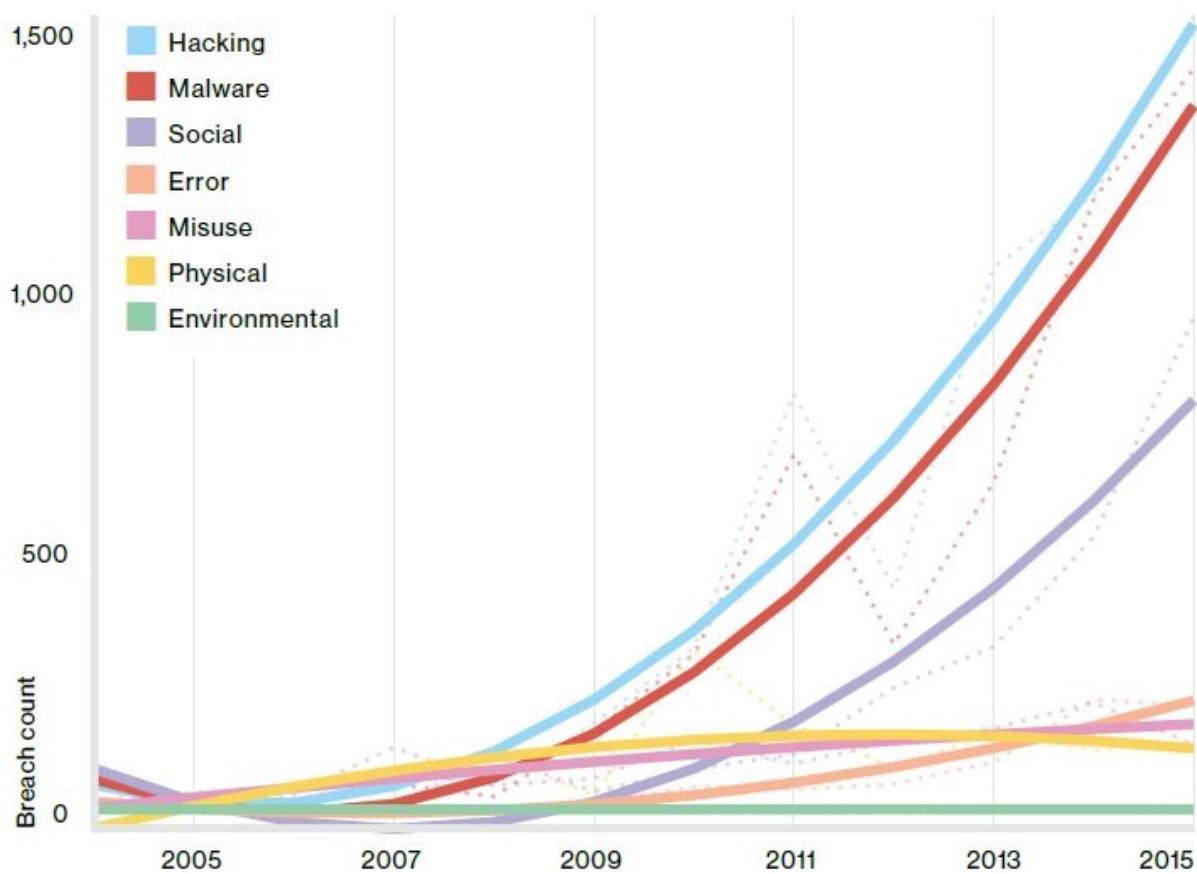


Fig. 4. Number of security breaches per threat action category over time, (n=9,009)²²

¹⁸ Ross, P., 2016

¹⁹ Kyriakidis, M. et al., 2015

²⁰ Gonder, J. et al. 2015

²¹ Enev, M. et al, 2016

²² Verizon, 2016, p8

The figure above shows the number of security breaches per threat category. The main source of security breaches can be found in hacking, malware and social engineering. Social engineering is out of scope of our research. In chapter 2 and 3 of our study we address the hacking and malware threats.

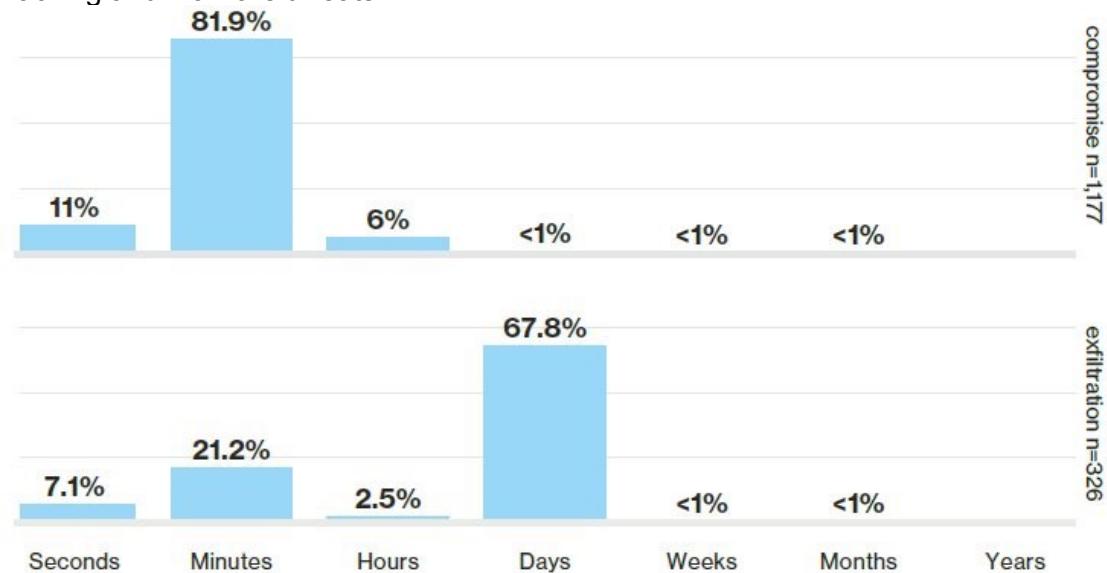


Fig. 5 Time to compromise a system and data exfiltration time.²³

The figure above shows how quickly ICT systems are compromised. It takes the attacker minutes to days to exfiltrate the data he is after. The figure below shows that the time to compromise the security of a system, related to the time it takes to discover a security breach. The same applies to the security of the connected car. The security of a connected car can be breached, and it takes longer to detect such a security breach.

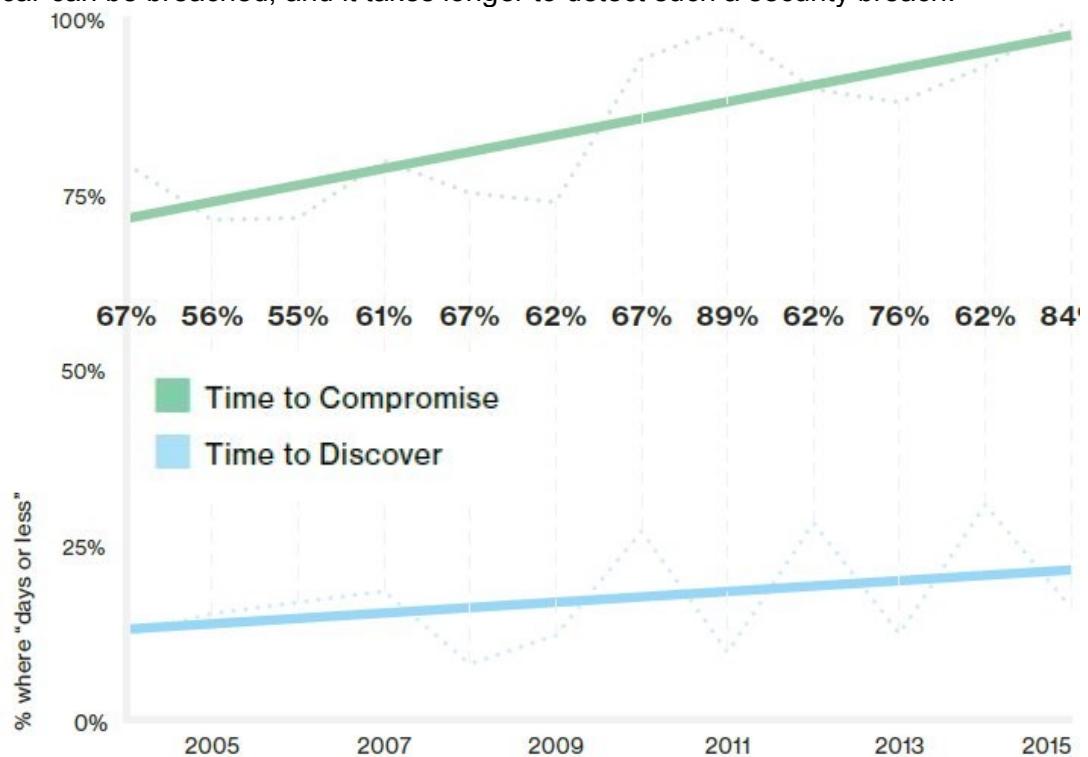


Fig. 6 Percent of breaches where time to compromise (green)/time to discovery (blue) was days or less²⁴

²³ Verizon, 2016, p 10

1.2 Assumptions and definitions

Our assumption is that all forms of connected – and autonomous cars are based on the same principles. We assume that all connected cars consist of the following elements. The first element is a car. This makes sense because without a car, you can't have a connected car. The second element is that there must be some form of communication possibility to and from the car. In addition to that, we see that a lot of cars are connected via the internet. This is the actual “connection” in the term “connected car”. The third element is that the connected car contains computer chips. The automotive industry calls these chips ECU's²⁵. An average car has about 50-70 ECU's which are connected by the controller area network (CAN).^{26 27} The fourth element is that a connected car contains software. This software is controlling all kinds of functions in a connected car. This includes the motor management, navigation and the entertainment systems. The fifth element of a connected car is some form of data storage. Otherwise the software and the data that runs through the applications could not function correctly. The last element is a volatile computer memory. Some of the calculations must be executed “in memory” because of the necessary processing speed to act “real time” on the car movement. When you look at it, a connected car is in fact a computer on wheels that can also transport people and goods.

Based on these assumptions we can better understand what a connected car is and investigate the possible attack vectors. In fact, we can now better understand how it is possible that connected cars get hacked. A connected car is just a computer on wheels connected to the internet. Computers connected to the internet can and will be hacked. The more “interesting” the connected target is, the more people will try to hack that computer. Connected cars are no different and will be attacked by hackers.

Although the terminology and definitions in literature differ²⁸, a connected car always consists of the elements that are specified and described above. In short, a connected car is any car that has remote communication possibilities. The next definitions that needs explaining is the difference between safety and security. We follow Burns in his analysis on safety and security.²⁹ We define safety as the condition of being protected from direct (physical) harm. The term safety always involves a human being. The definition of security we use is, that it is the state of being free from danger or threat. The term security involves a system. We define hacking as gaining unauthorised access to (computer) systems.

Foundations, associations, special interest groups and generally accepted organisations that are seen as “organisations involved in- or active for the automotive sector” are hereinafter referred to as “branch organisations”.

1.3 Scope

The scope of this research is bound by several elements. The first element is limiting this research to cars. The term “vehicles” would be too broad because that includes cars, drones, vessels and a wide variety of other devices. An example of this is the recently introduced autonomous vessel by the US navy that can operate by itself on the ocean for

²⁴ Verizon, 2016, p 10

²⁵ ECU, Electronic Control Unit

²⁶ Wijk van, M., 2016.

²⁷ Geraets, M., 2016

²⁸ SAE standard J3016 and NHTSA

²⁹ Burns, A., et al., 1992

several months.³⁰ The second element is that we use the term “connected” cars.

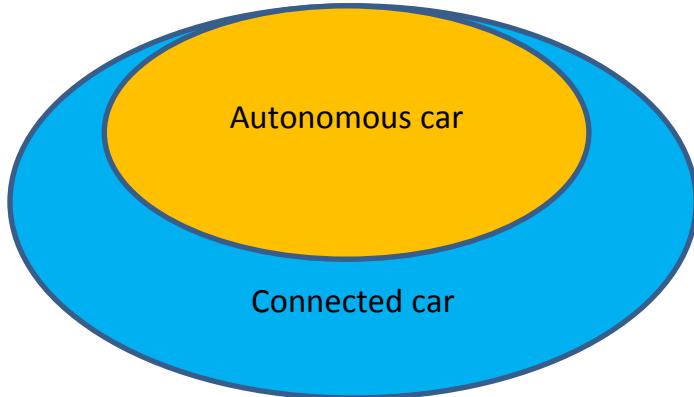


Fig 7. Relation diagram between connected cars and autonomous cars

The figure above shows the relation between connected cars and autonomous cars. All autonomous cars are connected cars. Our study uses the term “connected cars” which includes the autonomous car. The automotive industry defines several stages of connected cars in which the last stage is a fully autonomous car. The automotive industry generally agrees that there are six stages of connected cars, as depicted below.

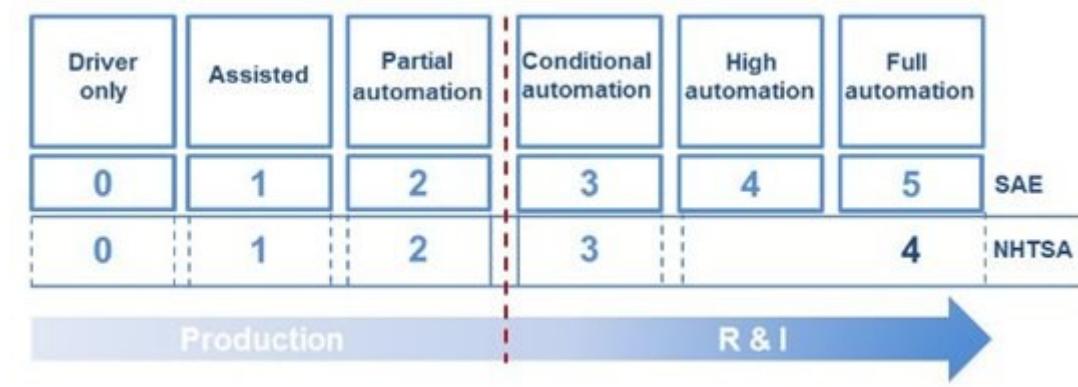


Fig. 8. Overview of stages of connected cars based on SAE standard J3016 and NHTSA.³¹

Only the last stage contains a fully autonomous car. The problem with the six stages model is that the definitions for each stage are not clear within the automotive industry. In practice, the boundaries between these stages are not clearly defined. When one car manufacturer claims a car in stage 3, another car manufacturer claims that that is not the case and it is just a car in stage 2. The most commonly used models are of the SAE³² and NHTSA.³³ The SAE model consists of six stages of a connected car. The NHTSA model consists of five stages. We look into the cyber security of the connected car and for our research it does not matter in which stage a connected car is. We research the cyber security of connected cars in general. This includes all forms of connected cars including the autonomous car. We see the autonomous car as just another form of a connected car.

³⁰ Anonymous, 2016

³¹ SAE, 2014

³² SAE, Society of Automotive Engineers <http://www.sae.org/automotive/>

³³ NHTSA, National Highway Traffic Safety Administration <http://www.nhtsa.gov>

The third element to limit our scope is, that we focus on the consumer used connected car. Out of scope are connected cars that are used in harbours, by the military and other non-consumer use. We want to improve the cyber security of the consumer used connected car.

Our research includes the relevant actors within the automotive industry that can influence and improve car security. We look at the car ecosystem and the actors that are involved. The fourth scoping element in our study is the limitation of actors to: car manufacturers, government, insurance companies, branch organisations, network providers and car users. We determine the actions and motivation for each cluster of actors. When these elements are identified, a multi actor roadmap is constructed in order to improve the current security situation of connected cars. We show that the actor that has to start this change are the car manufacturers.³⁴ In order to help the car manufacturers to implement the lessons learned from previous security breaches, a security roadmap is presented in a way the car manufacturers can use it to take this next step.

The last scoping boundary is geographical. The security aspects of the connected car is not a single nation problem, but a worldwide problem. By setting the geographical roadmap boundary to the Netherlands we are able to deliver a concrete example roadmap for the parties involved. The roadmap indicates which actions each actor can take to improve car security. We show that it is possible to construct a national cyber security roadmap to improve the security of connected cars.

1.4 The objectives of the study

An objective of this study is to deliver a multi actor roadmap to improve the cyber security of consumer used connected cars. We take the current situation of the cyber security of connected cars in the Netherlands as a starting point.

Literature shows that there are several possible attack vectors and a limited type of attackers that want to deliberately harm a connected car. The current actor landscape of the connected car is focused on safety and not on security. Because it is now possible to harm the safety aspect by breaching car security, it is time to act and address the cyber security aspects of the connected car. The constructed roadmap is based on the requirements we gather in the sub questions we defined.

For the qualitative part of this research we have defined several objectives. The first is to explore the possible attack vectors of a connected car. We answer questions like: Is it possible to hack the cyber security of connected cars? How can we cluster the technical vulnerabilities in connected cars in order to find and define solutions to prevent misuse of the connected car systems.

People often speak of “an evil hacker exploited vulnerability x”. What are the triggers of a person in order to become a hacker? What are the inhibitors, accelerators, and other factors for a person to become a hacker? Can we categorise these attackers? The second action is to categorise the possible attackers that are capable and motivated to breach the security of a connected car. This analysis gives us the hacker incentives that we can block in order to prevent people from hacking connected cars. These requirements are input for the multi actor roadmap.

³⁴ See survey question 1.3 and 1.4

From our literature research the picture emerged of a standard pattern of behaviour of the automotive actors when confronted with a security breach. Of course it is not possible to examine all the automotive security breaches in the world. This research is limited to the security breaches that made it to the media. Describing several of these cases we show that a repetitive pattern of behaviour that is typical of the actors in the automotive industry when they are confronted with a security issue.

The introduction of the connected car also results in many new functionalities consumers can use. It delivers a new set of (legal) questions. There are liability questions, platooning issues of cars, privacy aspects and data storage questions. We will discuss the legal issues in short when we discuss the role of the Dutch government to improve the security of connected cars in the Netherlands.

These objectives come together in one overall goal. To create a multi actor roadmap to improve the cyber security for connected cars.

1.5 Research question

Based on that the question becomes how the automotive industry can improve the cyber security of civilian used connected cars. When we look at the current landscape on the connected car the main research question becomes:

What multi actor roadmaps can be defined to improve the cyber security of consumer used connected cars?

This research question is broad and includes all consumer used connected cars. Car manufacturers build and sell connected cars on a global scale. In order to show that a multi actor roadmap to improve the security of the connected car can be created, we construct this roadmap for the Netherlands.

1.6 Sub questions

In order to answer the main research question we have to break the issue apart in several sub questions. There seems to be little awareness within the automotive industry on cyber security. This is also the picture that emerges from the interviews and the survey. We have to show that there are plausible technical attack vectors to breach the connected car security. This is the first sub question we have to answer.

- 1) What are the possible technical attack vectors to attack a connected car? We need this element in our argument in order to demonstrate that there are technical vulnerabilities in connected cars that can be exploited. This analysis delivers the first requirements for the multi actor roadmap.

In the preliminary investigation in the automotive branch revealed that many actors find it hard to imagine that someone would deliberately hack the security of a connected car. We present an overview of the possible attackers of a connected car and describe their motivation and capabilities. This element delivers the second sub question.

- 2) How can the possible attackers of connected cars be defined and categorised? With this element we show what the most likely attackers are and what drives them. This analysis delivers the inhibitors, catalysts and amplifiers of attackers. These elements are input for the multi actor roadmap.

Another element that was revealed during this research was the predictable repetitive patterns of behaviour of the actors in the automotive industry when confronted with a cyber security breach of a connected car. That fact delivers the next research sub question and the answer to this delivers the requirements needed to construct the multi actor roadmap.

- 3) Identify and describe the factors and incentives of the actors in the connected car ecosystem when they are confronted with security issues of connected cars. With this element we show that there are fixed patterns of behaviour by the actors of the connected car when confronted with a cyber security incident.

Based on the answers on these sub questions we define the requirements we need to construct a multi actor roadmap.

- 4) What are the possible roadmap items for the Dutch automotive industry to improve the cyber security of consumer used connected cars in the Netherlands?

1.7 Methodology

We start with describing the scope and the domain of this research. We describe the trend within the automotive industry which leads to common ground, the autonomous car. We define the issues which lead to the problem statement. In chapter 2 we look at the technical attack vectors and the actors that exploit these vulnerabilities. In chapter 3, we analyse the actors in the automotive industry that are involved in the security of the connected car. We look into the actions and responsibilities of these actors, their interests and show how they act when they are confronted with the security challenge of the connected car. This actor analysis leads to the design requirements to construct the multi actor roadmap. The roadmap is presented in chapter 4. Reflection is the topic of chapter 5. In this chapter we look at the problem from a meta point of view. In final chapter, chapter 6, the conclusions are presented.

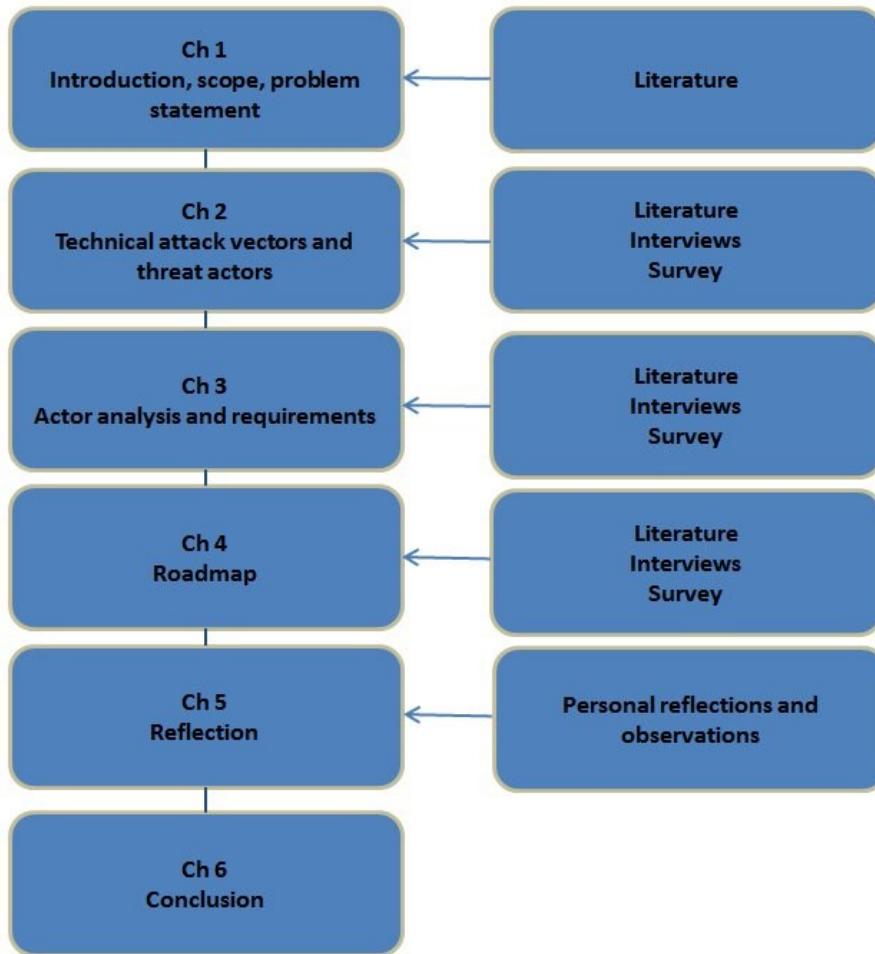


Fig. 9 Methodology

1.7.1 Research design

This paragraph addresses the question how this research was constructed and executed. In this part of the research we show the initial research design including the used data sources, data collection techniques, reliability issues and ethical considerations. This qualitative research consists of several elements in order to get a clear picture of the different cyber security aspects of the connected car in its ecosystem. Interviews are part of this qualitative research. Other elements of this research are exploratory and descriptive. These parts are the attack vector analysis, the attacker analysis and the behaviour analysis of the actors in the automotive industry when confronted with security incidents. These elements deliver the requirements we need to construct a multi actor roadmap to improve the cyber security of the connected car. Because of that this thesis is part of design science.³⁵

1.7.2 Data sources

The first data source element is a desk research on the available scientific literature. The complicating factor is that there is not much scientific research available on the cyber security of connected cars. To broaden the search for relevant information, non-scientific documents, conferences and videos are also be taken into account.

³⁵ Hevner A., et al, 2004

The second data source element consists of interviews with experts and stakeholders within the automotive industry. The interviews are conducted to verify the information found in literature. By introducing the expert interviews we try to solve the void that is created with the scarce scientific research available. A survey is the third data source element in this research. The fourth and last data source consists of personal observations and insights during the interviews. See Appendix 4 for an overview of conducted interviews.

1.7.3 Data collection techniques

The desk research is conducted in a structured way. This research includes a literature search. The first step is to gather literature based on key word search. The used key words, and combination of key words, to search relevant literature are: connected car, autonomous car, automotive, security, hack, breach, black hat, testing, non-disclosure, network, CAN bus, architecture, security by design, security standard, legislation. The second step is to screen the gathered literature and make a selection based on subject relevance. In this process all non-car related literature is removed. The literature that remains is studied in full and forms the basis for our research. The third step is to look at the relevant literature and check the used references. Some of these references are also relevant for our own research. The fourth step is to look at the authors of the literature and look for more articles of these authors regarding the same subject. This snowball method delivered some additional literature. Some papers are excluded in this phase, based on their specific details that does not fit our research scope.

A preliminary screening on the available scientific research indicates that there is little scientific literature available in the research area of cyber security of connected cars. To cope with this lack of available literature, also non-scientific literature, newspaper articles, hacking video's and hacking events are taken into account. The selection of these non-scientific documentation follows the same pattern as the scientific literature selection.

The literature review results are tested and compared in the expert / stakeholder interviews. In order to obtain the maximum "connection" possible with the interviewed person, we always interviewed "in person" at their own office. This was occasionally followed with an follow up interview by phone. An interview in person at their own office, makes the interviewed person feel at ease and the chance of obtaining relevant information increases. The downside of "interviews in person" is that it takes significantly more time to execute all these interviews. Getting into people's busy agenda is also an extra barrier for these interviews. An Excel file is kept containing the logging of the all communication contacts with the experts in the automotive industry. The persons and organisations that refused to cooperate in this research are also logged in this file. Notes are taken from each interview including personal observations and gained insights during the interview. We chose to take notes and not to record the interviews. Previous experiences show that people tend to be careful in their choosing of words when confronted with a recording device.

Each interview started with an unstructured part which allows the person that is interviewed to present information that is important to them or their organisation. This maximizes the information output, but the gathered information is unstructured and a lot of that was unusable. The positive side of it is that it delivered unexpected new insights of information we did not think of before. The advantage of starting the interview with unstructured questions is that the person that is interviewed is less biased and "steered" by the structured questions of the interview based on the survey.

The survey questions are available in appendix 1. For a detailed overview of the survey structure, the survey process and survey results see appendix 2. The second part of each interview is structured and strictly follows the survey questions. The person that was interviewed, and other persons that are present in the meeting, obtained the survey questions on paper. Sometimes the person that was interviewed took an expert with him/her during the interview to assist them in answering the questions. The input of the interviewed person was logged. Only one interview + survey, including their remarks, is put into the dataset. The input of the other persons present is not in the dataset. This prevents cross contamination of the gathered interview / survey data. The researcher took notes of additional remarks that the interviewed person, or other persons present, adds during the interview. Each interview ended with the question who to contact in the automotive industry to obtain a full and fair overview of this research area. The last interview question was always a "catch all" question: "Do you have any other remarks on this subject that we missed in this interview?" This gave the interviewed persons the possibility to add items that are important to them.

1.7.4 Sampling techniques

This qualitative research started initially without a network or connections in the Dutch automotive industry. We started in March / April 2016 with a preliminary research in the field of the automotive industry to discover if there were enough people and organisations that could / would want to participate in this research to get a significant outcome. We started the initial search with TNO and used the snowball technique to discover the relevant stakeholders within the automotive industry. Each interviewed stakeholder was asked who we should consult next in order to generate an adequate overview of the automotive industry. We stopped gathering data at 11-11-2016.

1.7.5 Ethical considerations

We did not hack connected cars ourselves in this research, but we did speak to people that have hacked connected cars. We use this input of (hacking) experts to generate requirements for the multi actor roadmap.

1.7.5.1 Confidentiality

During the interviews the respondents sometimes indicated that certain information was confidential. Such a remark was noted and that specific piece of information is not in this report. All conducted surveys are anonymous. Some people replied to the researcher that they filled out the survey and added extra comments in the mail. Of course these people realise that they are no longer anonymous participants because timestamp of mail including specific remarks makes a correlation possible.

1.7.6 Informed consent

Each interviewed participant is aware that the results of this research is published. All interviewed persons and organisations are aware that the research outcome is presented in an university thesis repository system. Several participants asked that specific information was not linked to their company in a possible publication in the media. The facts can be presented, but not linked to their specific name or company. Of course we comply to these confidentiality requests.

2 Technical attack vectors and threat actors

The first step in our analysis is to determine the technical attack vectors and cluster them. This gives us the answer on the first sub question what the possible technical attack vectors are to attack a connected car.

We start at looking at the kill chain.³⁶ The kill chain consists of seven stages. The attacker must pass all seven stages in order to execute a successful attack on the connected car. The attacker can be stopped at each of these stages and the attack will fail. In this chapter we look at the possible attack vectors and motivation for the different types of attackers. By analysing these elements we gain insight in the criminal business case and the kill chain. The attacker has to complete every step in the kill chain to be successful. The defenders of a system have to stop the attacker at one of these steps. The elements that deliver the possibility to stop an attacker, are the requirements we need to incorporate into the multi actor roadmap.

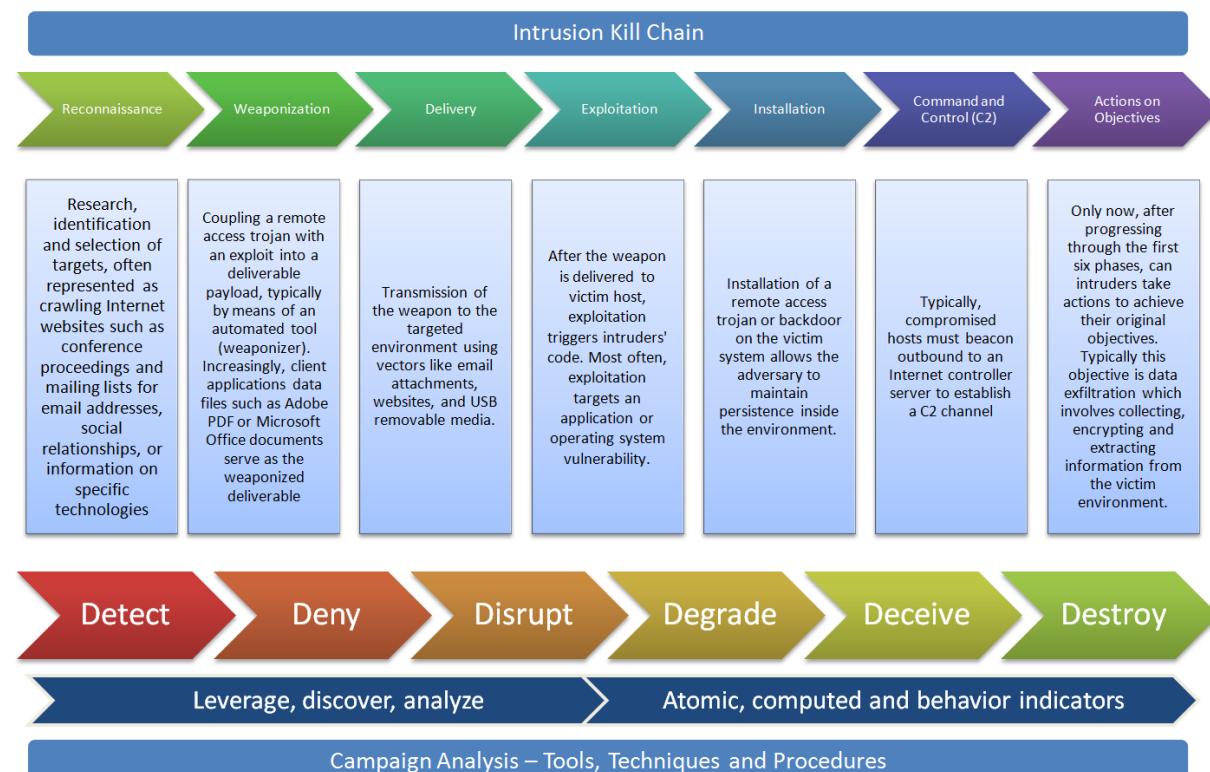


Fig 10 Kill chain³⁷

Looking at the kill chain it becomes clear that the effort to protect the connected car by only implementing prevention measures will fail. The average lifespan of a car is more than 10 years. State of the art cyber security will be obsolete after 10 years. Cyber security can and will be compromised over time. A sufficient technical security solution to protect the connected car should also try to detect the security breach and generate an appropriate response.

2.1 Technical attack vectors

In this paragraph we look into the possible technical attack vectors to attack a connected car. Anderson³⁸ investigated the security aspects of 21 different cars. His research shows that there are three main components necessary to succeed in a successful hack attack on a car.

³⁶ Hutchins, E. et al, 2011 Based on the Lockheed Martin Kill chain

³⁷ Rocha, L., 2016

³⁸ Anderson, M., 2014

The first element is finding a way into the car. The second element is compromising an ECU³⁹ and the third element is finding a control feature that could be compromised. The report by FireEye⁴⁰ also indicates a number of technical vulnerabilities. These overlap with the results found by Anderson, Checkoway and Valasek. We use a slightly different approach that is based on prior research by Checkoway and Valasek.⁴¹ These researchers present a broader view how car security can be compromised. The “Car Hackers Handbook” by Smith⁴² presents an extensive overview of the possibilities to hack into connected cars. Before we look into the details we present a high level picture, indicating the attack clusters. In the next step we zoom in into the detailed hackable elements of the connected car. These requirements are attributed to an actor and put into a multi actor roadmap to improve the security of the connected car. The figure below shows the identified high level attack clusters. You can also recognise the elements defined by Andersen. There are four main clusters. The first cluster is the direct physical attack possibility. In that case the attacker has direct access to all parts of the car. Car manufacturers should realise that their product is functioning in a hostile environment. Expert interviews⁴³ as well as hacker presentations shown in public⁴⁴ indicate that an object that can be directly accessed can and will be breached. There is no good defence against a direct physical attack. In the end the attacker wins. That means that your car is vulnerable when people have direct access to the car. This is the case when your car is in for maintenance, repairs or when you lend your car to other people.



Fig 11. Overview of the clustered attack vectors of a connected car based on research by Checkoway, et al., 2011 and the TU Automotive report 2016.

The second cluster concerns the indirect physical attacks. That means that a carrier of some sort is necessary to carry out the attack. This carrier can be an USB stick or CD with a special WMA song that compromises the car firmware.⁴⁵ Also the existence of SD cards in

³⁹ Electronic Control Unit

⁴⁰ FireEye, 2016

⁴¹ Checkoway, S et al., 2011; Valasek, C; Miller, C., 2013

⁴² Smith, C. 2016

⁴³ Smulders, A. 2016; Hoop, de A. 2016

⁴⁴ Mahaffey, M.R.K. et al. 2015

⁴⁵ Cornell, D., 2016

cars like Tesla opens all kinds of new attack possibilities.⁴⁶ Some car manufacturers, like Fiat Chrysler Automobiles (FCA), teach their customers to download software patches on USB devices in order to patch vulnerabilities in connected cars.⁴⁷ In our opinion this is not a smart thing to do because you teach the end user that “it is ok to put an uncontrolled USB device in your car to update the firmware / software of the car”. This increases the possible attack surface of the connected car. Malware, like ransomware, spreads for example via e-mail and USB sticks. An attacker can send a letter containing an infected USB stick with malware / ransomware to the car user with the request to patch the software of the car.

The third cluster is about the wireless attacks on a connected car. Bluetooth as well as attack on or via the mobile network are possible. The current application development for iOS and Android in which the car user can interact with his car gives, according to Kim et al.,⁴⁸ an abundant variety on attack possibilities. Weinmann describes fundamental mobile baseband attacks based on flaws in the protocol stack.⁴⁹ These facts in combination with the fact that a lot of mobile devices and smart phones are not and cannot be properly and timely patched,⁵⁰ gives the attacker of the connected car an additional attack surface.

The fourth cluster is about sensor fooling. There are no known hacks documented in literature that indicate that you can compromise and take over a car by fooling the sensors. That's why the line in the figure above is a red dotted line. Sensor fooling however is a real threat that can seriously harm the car user. Connected and autonomous cars often use Lidar⁵¹. Research shows that camera based autonomous car systems and Lidar systems can be fooled in an cheap and easy way.⁵² These systems can be blinded or fooled with false information that might cause accidents. GPS has also vulnerabilities that can be exploited.⁵³

When we look into the communication architecture of the connected car, we see that there are several communication channels that are interconnected and also connected to the outside world. Looking at the ICT architecture of the connected car we see that any breach will lead to multiple access and tampering possibilities.⁵⁴ The research by Zhang⁵⁵ describes how connected cars could be infected and protected from malware attacks. This research indicates four general entry points. The first cluster of vulnerabilities are related to the architecture and design of the hardware and software of the connected car. Communication protocols and applications may also contain vulnerabilities and the last element of this cluster are the implementation failures. The second cluster of vulnerabilities are related to the operating system of the connected car. This operating system is often some form of Linux.

⁴⁶ Mahaffey, M.R.K. et al. 2015

⁴⁷ Fiat Chrysler Automobiles (FCA) <https://www.fcagroup.com/en-US/Pages/home.aspx> is the seventh largest manufacturer of automobiles in the world. Car brands that are part of the FCA group are: Abarth, Alfa Romeo, Chrysler, Dodge, Fiat, Jeep, Lancia, Ram, SRT and Maserati. The update site for the FCA Uconnect service is <http://www.driveuconnect.com/software-update/>. The end user can download new software on an USB device and update the firmware of the car. The access to the software download is based on the VIN number of the car. The VIN number of each car is visible from the outside of the car. FCA indicates that it takes about 30 to 45 minutes to update the car software.

⁴⁸ Kim, P. 2014

⁴⁹ Weinmann, R., 2012

⁵⁰ Husted, N. et al., 2011

⁵¹ Lidar is “Light Detection And Ranging” also known as “Laser Imaging Detection And Ranging”

⁵² Petit, J., 2015

⁵³ Nighswander, T., et al., 2012

⁵⁴ Kleberger, P., 2011

⁵⁵ Zhang, T. et al., 2014

The next cluster consists of vulnerabilities that enter the car via software patches and updates. When these software patches are infected the entire system gets infected. The last cluster contain the car users themselves. When the car user visits a malicious website or downloads an infected file the connected car can be infected.

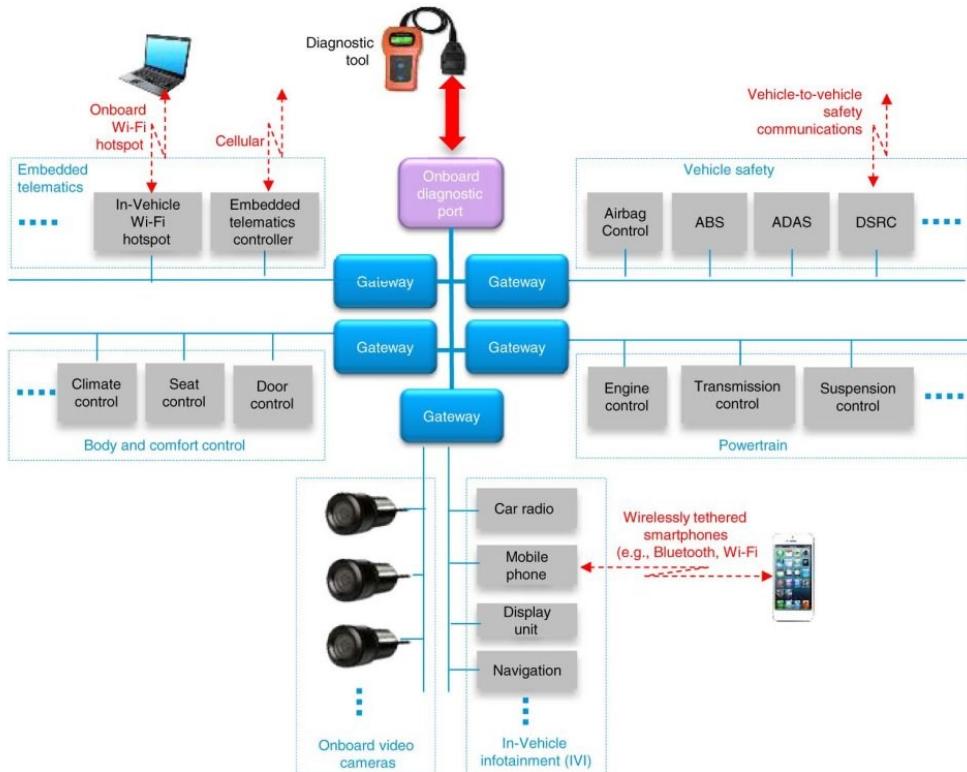
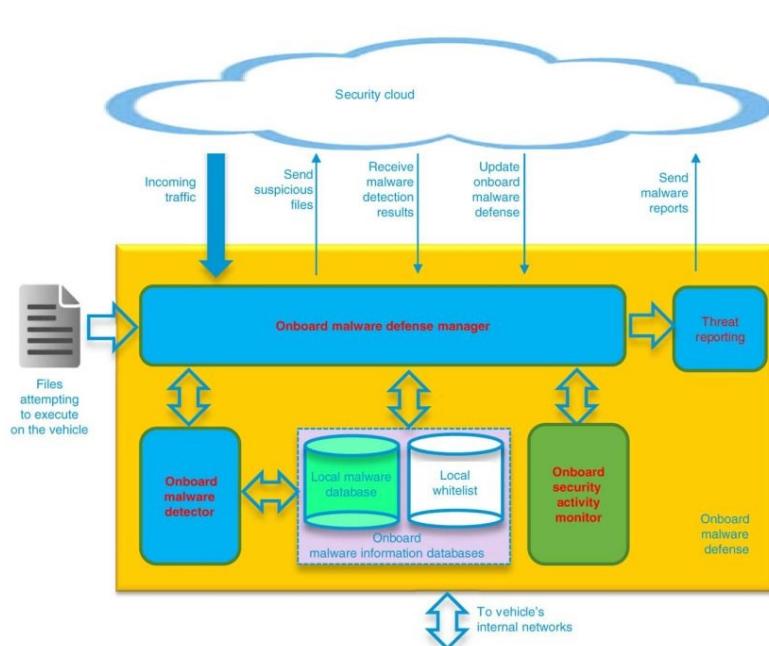


Fig 12 Connected car overview - existing in-vehicle network architectures⁵⁶



The research of Jun Li⁵⁷ proposes an IDS, CAN See, that detects anomalies. Zhang suggests to protect the data of the connected car by checking each file to the gathered data in the security cloud.⁵⁸ Zhang's research has also a flaw. His research focus lies entirely on the protection of the car. The connected car ecosystem should be looked at as well.

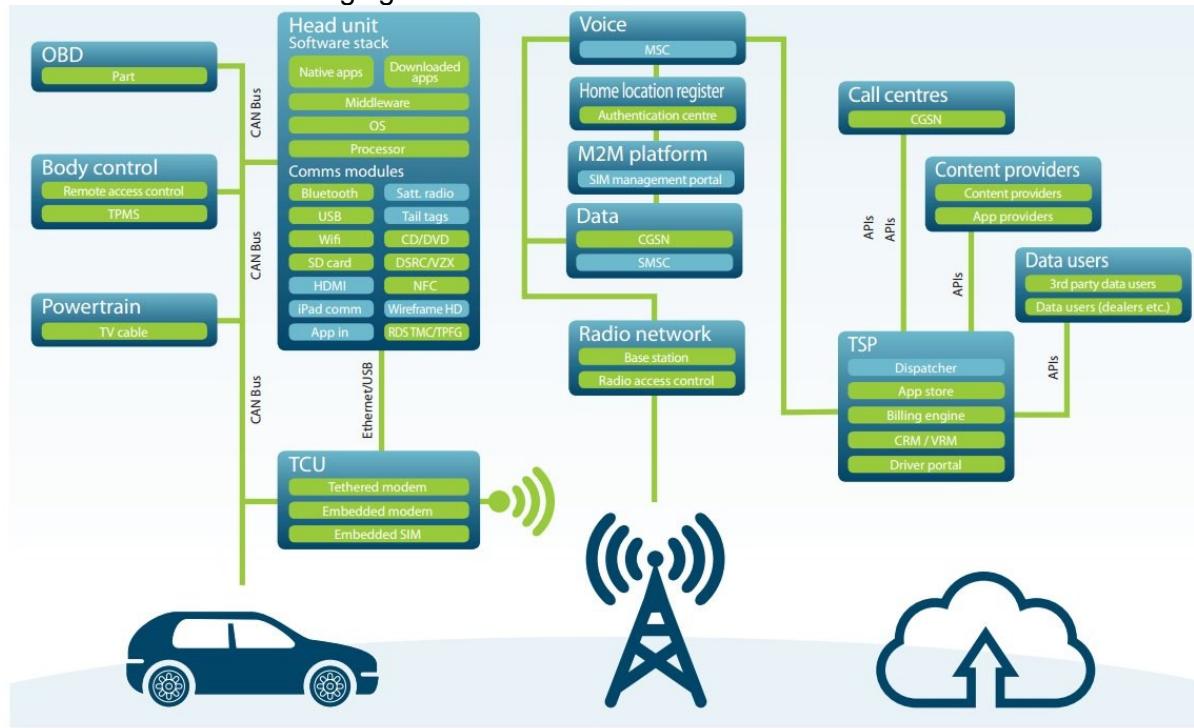
Fig 13 Zhang, Architecture of the connected car malware defence

⁵⁶ Zhang, T. et al., 2014 p12

⁵⁷ Li, J., 2016

⁵⁸ Zhang, T. et al., 2014 p19

Applying the knowledge of the attack vectors in combination with known vulnerabilities on cars results in the following figure below.



© Mike Parris, SBD.
Fig. 14. Detailed overview of possible attack vectors of a connected car 2016 ⁵⁹

The figure above shows an overview of the possible attack vectors of the connected car. The figure shows that not only the connected car itself contains vulnerabilities, but car security can also be breached by other elements in the connected car communication chain. The car manufacturers, the network provider and the car dealer all play a role in improving the security of the connected car.

Research by Oosterbaan et al. in 2014 ⁶⁰ indicates that the current connected car implementation contains an average car of 30 to 100 separate but interconnected systems. The security model of these implementations seem to follow the coconut model, a hardened shell and no extra security measures within or between the systems in the connected car. That seems a logical step in a non-connected car. The researchers state that car manufacturers did not update their traditional security approach to the new connected car.

Miller and Valasek showed in 2014 a brand and type specific overview per car brand how easy it was to breach car security. This is depicted in the figure below.

⁵⁹ TU Automotive, 2016

⁶⁰ Oosterbaan, W., Lei van der G., 2014

Car	Attack Surface	Network Architecture	Cyber Physical
2014 Audi A8	++	--	+
2014 Honda Accord LX	-	+	+
2014 Infiniti Q50	++	+	+
2010 Infiniti G37	-	++	+
2014 Jeep Cherokee	++	++	++
2014 Dodge Ram 3500	++	++	--
2014 Chrysler 300	++	-	++
2014 Dodge Viper	++	-	--
2015 Cadillac Escalade	++	+	+
2006 Ford Fusion	--	--	--
2014 Ford Fusion	++	-	++
2014 BMW 3 series	++	--	+
2014 BMW X3	++	--	++
2014 BMW i12	++	--	+
2014 Range Rover Evoque	++	-	++
2010 Range Rover Sport	-	--	-
2006 Range Rover Sport	-	--	-
2014 Toyota Prius	+	+	++
2010 Toyota Prius	+	+	++
2006 Toyota Prius	-	--	--

Figure 15 shows three columns.

1) The column “Attack surface”, which includes all wireless attack vectors like Bluetooth, cellular, keyless entry systems. This is the first step to access the car.

2) The “network architecture” column indicates if the attacker can reach important systems (eg. steering, brakes etc) after the initial entry.

3) The column “Cyber Physical” means automated car systems (eg. Lane control) that are vulnerable for spoofing which results in loss of control over the car.

Legend: + is hackable,
- is less hackable

Fig 15. Car vulnerability overview by Miller and Valasek 2104 ⁶¹

The first column “attack surface” refers to the first stages in the kill chain. That is the “reconnaissance, weaponisation and delivery” phase. The second column “Network architecture” is represented in the “exploitation, installation and command & control” phase of the kill chain. The last column “Cyber physical” is represented by “command & control and actions on objectives” in the kill chain. The kill chain is overlaps several columns and there are no hard lines between the columns.

Many connected car brands have been hacked. Some examples to show our point:

Mitsubishi Outlander plug in hybrid (PHEV) was hacked in June 2016. Point of entry was the Wi-Fi connection ⁶². Initial reaction from Mitsubishi was “disinterest”. After the hackers involved the BBC, the car manufacturer responded and fixed the security issue. BMW, Mercedes and Chrysler were hacked in July 2015. ⁶³ The hackers used the hacking toolkit called “Ownstar” to hack into the “OnStar” car management system of the connected

⁶¹ Miller, C., & Valasek, C., 2014

⁶² Lodge, D., 2016

car.⁶⁴ Although SSL⁶⁵ was used in the encrypted communication, the hackers could still intercept and read the communication between the car and the OnStar servers. The hackers used a MitM attack⁶⁶. The car user tries to connect to the server and finds a fake Wi-Fi access point nearby. When the connection is made via the fake access point, the attacker can intercept the communication and compromise the security. The following car brands were vulnerable for this kind of attacks: BMW Remote, Mercedes-Benz mbrace, Chrysler's Uconnect, and Dodge Viper's Smartstart.

In February 2016 BMW was confronted with several vulnerabilities in the BMW's ConnectedDrive Web portal. Hackers could exploit vulnerabilities like XSS⁶⁷ and VIN session hijacking to attack and change the car configuration.⁶⁸ Security researcher B. Kunz Mejri concluded that five months later, the issues still existed. XSS is a well-known issue in web portals. XSS is in the top 10 list by OWASP⁶⁹ for several years. XSS vulnerabilities are well known common vulnerabilities and are easy to solve by developers of web portals.

Researcher T. Hunt showed in February 2016 that the Nissan Leaf app⁷⁰ was vulnerable and could be exploited. The Nissan user application uses the VIN number⁷¹ to identify and authenticate the car and the car user in the Nissan app. When a hacker enters another VIN number in the app, he can access another car. The Nissan app lacks any authentication. The Nissan Leaf is therefore easy to hack. Hackers can even write a script to disrupt the Nissan Leaf without any human intervention. The researcher contacted Nissan to report the issue. Nissan did not visibly react for about four weeks and then took the service offline.⁷²

In 2014 Miller & Valasek hacked a Jeep Cherokee over the internet exploiting the Uconnect wireless connection.⁷³ The car manufacturer, Fiat Chrysler Automobiles (FCA), responded with a recall action of 1.4 million cars.⁷⁴ The FCA dealt with this and other hacks of the FCA OwnStar system⁷⁵ by sending a letter to the car users containing an USB stick and the question to update the software of the car to patch the vulnerability found. Car users could also download the updated car software from a website and patch the car themselves.

When we look at the technical attack vectors supported by the cases we discussed in this paragraph, we can conclude that connected cars contain vulnerabilities. Connected cars are computers on wheels and do have the same vulnerabilities as regular computer systems. Connected cars should be treated in the same way in order to protect these computers on wheels.

The requirements we derive from this technical attack vector analysis are: the connected car should have a layered defence. The car should have security zones, anomaly detection

⁶³ Cimpanu, C., 2015

⁶⁴ In December 2015 at the DEFCON 23 conference, researcher S. Kamkar presented his findings in a presentation called "Drive it like you hacked it: New Attacks and Tools to wireless"

<https://www.youtube.com/watch?v=UNgvShN4USU>

⁶⁵ SSL – Secure Socket Layer

⁶⁶ MitM, Man in the Middle attack

⁶⁷ OWASP, 2016 XSS, Cross site scripting

⁶⁸ Cimpanu, C., 2016

⁶⁹ OWASP, Open Web Application Security Project <https://www.owasp.org>

⁷⁰ Hunt, T., 2016

⁷¹ VIN number, Vehicle Identification Number. The VIN number can be read from outside the vehicle and is mostly placed at the bottom of the windshield.

⁷² Weise, E, 2016

⁷³ Greenberg, A., 2015b, p1

⁷⁴ Greenberg, A., 2015a, p1

⁷⁵ Cimpanu, C., 2015

systems and redundancy in system with critical functions. The CAN bus⁷⁶ should only connect those systems that must share data or communicate with each other. Non-essential systems, like entertainment systems, should not be on the same CAN bus as the motor management systems. This change in the architecture of the connected car must take place in order to improve the cyber security of the connected car. But we have to remember that the required adjustment of the connected car architecture is a trade-off based on the underlying law and commercial business case. Lessig⁷⁷ stated in his publication that the implemented technology is a weighted balance between privacy, security of the individual on the one hand and the commercial business case of the organisation on the other hand. The identified requirements from this paragraph are summarised in the chapter on car manufacturers and network providers.

2.2 Threat actors

In this paragraph we analyse the threat actors that take advantage of the existing technical vulnerabilities of the connected car. The figure below presents an actor overview based on the connected car ecosystem. In this paragraph we look at the people that deliberately harm the connected car. These actors are indicated in red. The other actors are discussed in the next chapter.

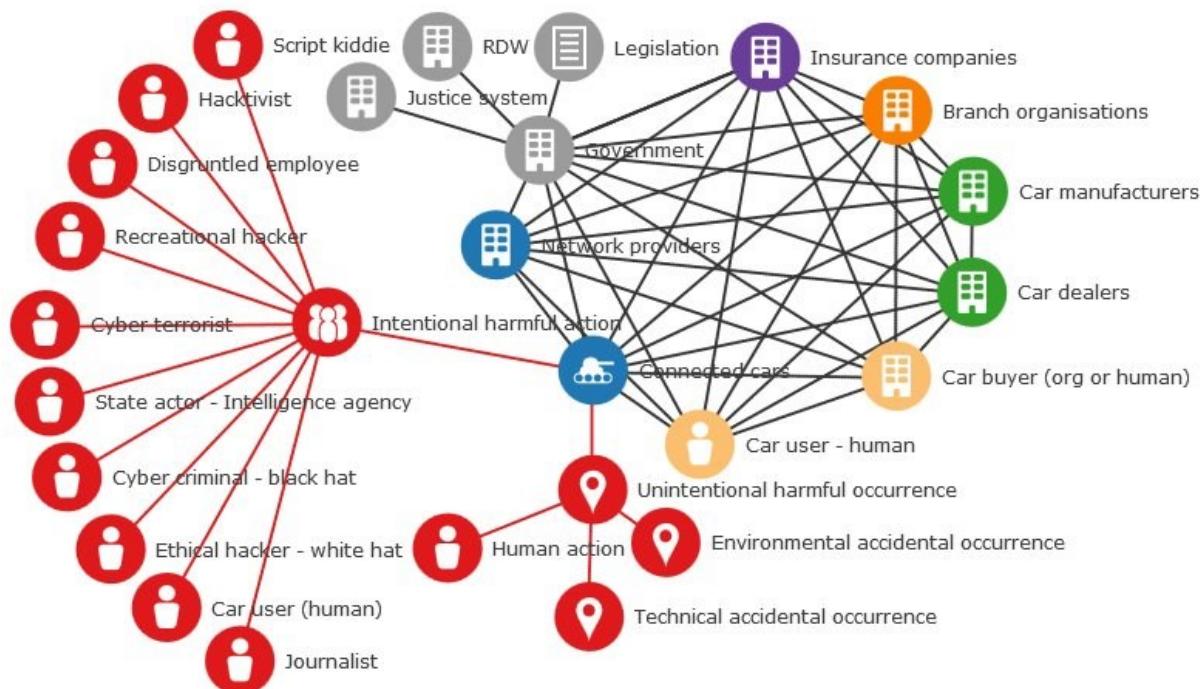


Fig 16 Actor overview in the connected car ecosystem⁷⁸

We use the SABSA framework by Sherwood⁷⁹ to categorise and define the attacker of the connected car. This framework was chosen because it shows the necessary elements that an actor has to possess to attack a connected car. When we understand these elements we can try to define requirements to block or limit these elements in order to stop an attacker.

⁷⁶ Wijk van, M., 2016. CAN bus, The Controller Area Network bus forms the communication data backbone in the car and connects all car systems.

⁷⁷ Lessig, L. 2006 p53

⁷⁸ The actor threat actor overview is based on literature: Gutierrez, M., 2014; Oosterbaan, W., Lei van der G., 2014; Verizon, 2016

⁷⁹ Sherwood, J., 2004

before they compromise the security of a connected car. The essence of the SABSA actor analysis framework is shown in the picture below.

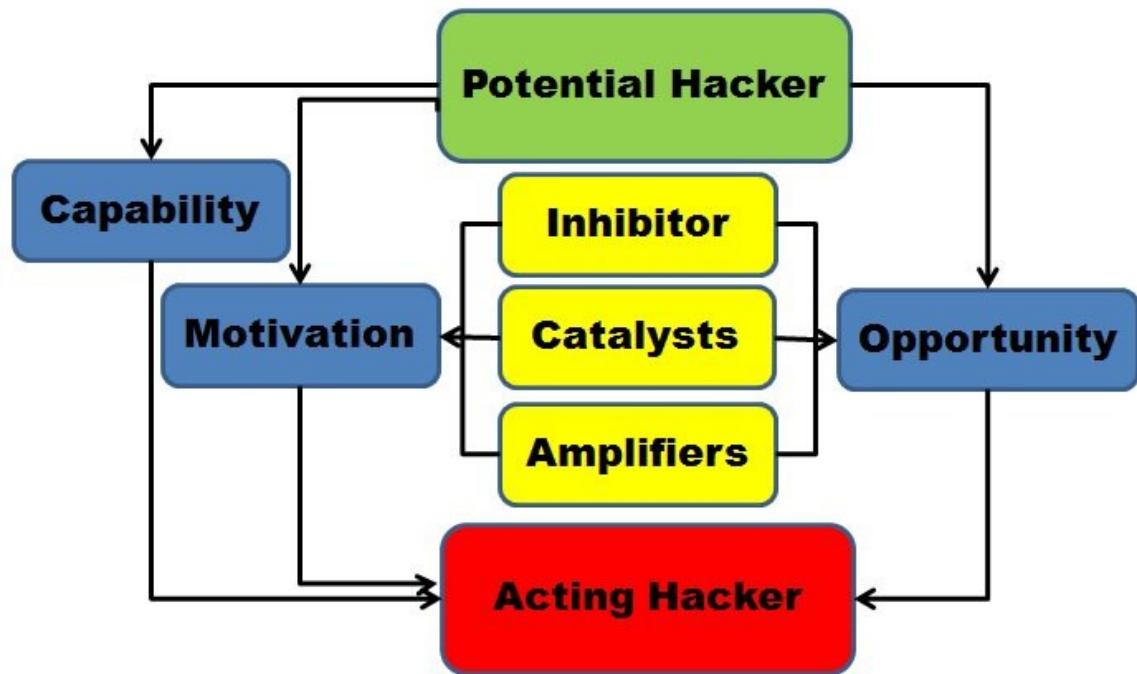


Fig 17 Overview of the relevant SABSA framework elements by Sherwood, 2004.

We analyse the following elements a hacker needs to execute a successful attack: Capability, Motivation and Opportunity. These are indicated in blue in the figure above. The opportunity factor is described in the previous paragraph and includes the technical attack vectors. The next element is the motivation of the attacker.⁸⁰ The research by Gutierrez shows that the following elements can explain why people hack cars. They hack first of all for fun. Another motivation is that an attacker hacks cars for criminal purposes, and to make money. The third motivation mentioned is for criminal purposes to kill someone and make it look like an accident.⁸¹ The last motivation defined by Gutierrez is that someone wants to make a statement. The research by Oosterbaan et al,⁸² and Verizon⁸³ indicate the same elements. The organised online criminals are after money, power and knowledge. They have the technical capabilities and are willing to invest financially. An additional advantage is that the criminal can execute the attack on the connected car without a physical presence.

The capability of the attacker is the last element in the SABSA framework we look at. An attacker must have hacking skills like knowledge and must be able to use the proper tools. Perseverance is another element that the attacker must possess. It might take some time to solve the security puzzle. An attacker must also be willing to invest financially in the attack. These three elements together, form the capability factor. We categorise the attackers based on the identified capabilities: skill and knowledge, perseverance, willingness to invest financially.

⁸⁰ Gutierrez, M., 2014

⁸¹ Luh, R., 2013

⁸² Oosterbaan, W., Lei van der G., 2014, p8

⁸³ Verizon, 2016, p 36

The yellow blocks in the figure indicate the Inhibitors, Catalysts and Amplifiers. Sherwood describes these factors as depicted in the table below.

Inhibitors	Catalysts	Amplifiers
Fear of capture	External events that trigger a response	Peer pressure
Fear of failure	Changes in personal circumstances creating a "need"	Fame
Insufficient access limiting the opportunity	Changes in level of access increasing the opportunity	Easy access providing high level of opportunity
High level of technical difficulty	Changes in level of difficulty through new technologies and tools	Ease of execution because of low level of technical difficulty
High cost of participation	Changes in level of cost	Low cost of participation
Sensitivity to adverse public opinion	Dramatic changes in public opinion and cultural beliefs	Belief in sympathetic public opinion

Table 1 Sherwood, 2015, Catalysts, Inhibitors and Amplifiers ⁸⁴

The problem with the SABSA model is that when we apply this model on our threat actors, we get a distorted picture of the threat landscape because some things are possible but the action that is theoretical possible lacks relevance. We add the factor "Relevance / interest in car hacking" to the model. When we apply the model the following picture emerges.

Type of attacker	Relevance / interest in car hacking	Knowledge	Financial investment	perseverance	Score
Script kiddie / Disgruntled employee / car user	1	1	0	1	2
Cyber terrorist	0,5	2	2	2	3
Intelligence agency	0,5	2	2	2	3
Recreational hacker	1	1	1	1	3
Hacktivist	1	1	1	2	4
Journalist	2	1	1	1	6
Ethical hacker	2	2	2	2	12
Cyber criminal / Black hat	2	2	2	2	12
High = 2, Medium = 1, Low = 0. Used formula => relevance * (knowledge + fin invest+ perseverance) = score					

Table 2 Threat actor analysis on car hacking using the SABSA model.

When we plot these figures into a graph it becomes clear that not all hackers pose the same threat to the connected car. The outcome of this analysis, black hat hackers and ethical hackers are the persons most likely to hack a connected car, matches the results found in literature and the expert interviews.⁸⁵ The two most likely threat actors are the ethical hacker and the black hat hacker. The third most likely actors are journalists looking for a story.

⁸⁴ Sherwood, N., 2015, Table 9-7

⁸⁵ Smulders, A. 2016; Hoop, de A. 2016; Visser, T., 2016

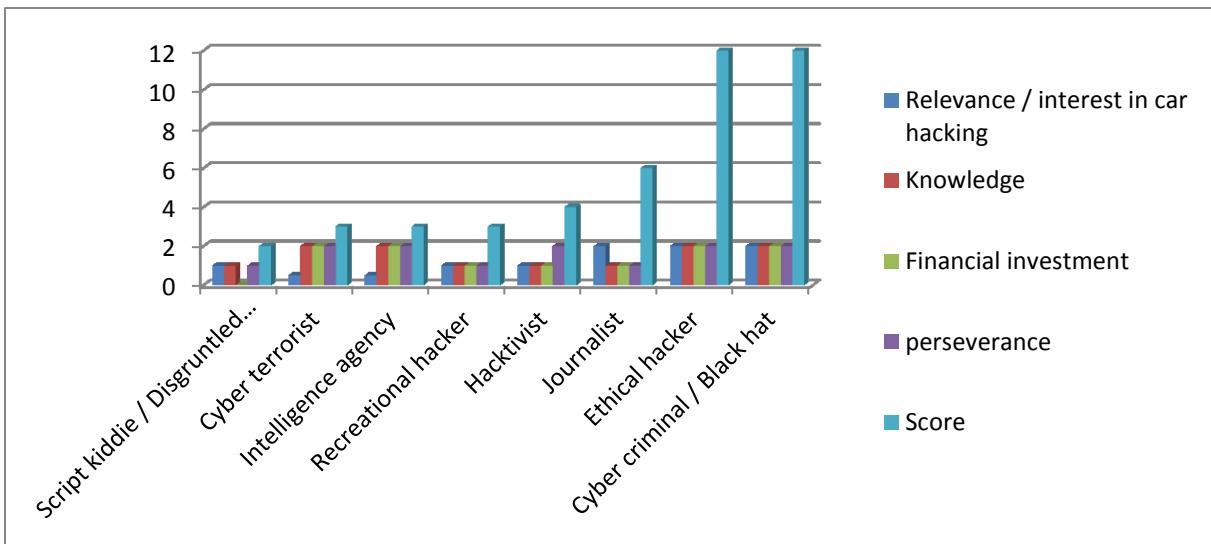


Fig 18. Threat actor graph on car hacking using the SABSA model.

The black hat hackers want to earn money by extortion, malware and ransomware attacks.⁸⁶ In order to stop a black hat hacker, we must break the kill chain that results in a negative criminal business case. When car manufacturers have a “responsible disclosure” policy the ethical hacker, also known as “white hat hacker”, has a procedure to follow. Some companies like Tesla⁸⁷ and GM⁸⁸ have these kind of “responsible disclosure” policies. The ethical hacker does not want money, but recognition. In the Netherlands, the NCTV published in 2015 a guideline for responsible disclosure policies.⁸⁹ We see this on the responsible disclosure page of Tesla on hacker fora.⁹⁰ When we look at the Tesla page it states that “yes, offers bounties” and “yes, offers thanks” notification. The ethical hacker is happy with his name on a website “hall of fame”. These two elements are easy to realise and will potentially generate new security insights that the automotive industry can use to improve the current implementation of the connected car.

We must not overestimate the power of the attackers, but the general public must also understand that there is a risk. In order to inform and make the general public aware of the risks, the government must initiate an annual cyber security threat awareness campaign.

The roadmap requirements we derive from this analysis of the Threat actors are:

T1	The Dutch government must ensure that there is enough chance for the threat actor, or non-compliant to legislation automotive business, of being caught and brought to justice when a threat actors compromises the security of a connected car. This triggers the inhibitor factor “fear of capture”.
T2	As the previous chapter shows it is fairly easy to gain access to a connected car and compromise its security. The ease of access is also an amplifier for threat actors to hack a connected car. Improving the technical access barriers by encrypting the communication to and from the connected car is one element that will block this amplifier. The action for this lies with the network provider and the car manufacturer.

⁸⁶ Oosterbaan, W., Lei van der G., 2014

⁸⁷ Anonymous, 2015, Also see Appendix 5

⁸⁸ Gallagher, S., 2016. GM means General Motors.

⁸⁹ NCTV, Nationaal Coördinator Terrorismebestrijding en Veiligheid “Leidraad Responsible Disclosure” <https://www.nctv.nl/actueel/nieuws/2015/Responsibledisclosurekansvoordigitale samenleving.aspx>

⁹⁰ <https://hackerone.com/teslamotors>

T3	Making it harder to break the security measures of the connected car will increase the cost of the attacker. An example of this is the implementation of segmentation in the connected car system design. This works as an inhibitor that blocks the amplifier "low cost of participation". The action for this lies with the car manufacturer.
T4	In the communication and information campaign must send the message that tampering with a connected car endangers the lives of the people in that car. This will influence the public opinion that it is not ok to breach the security of connected cars. This will work as an inhibitor that blocks the amplifier "belief in sympathetic public opinion". This communication and information action lies with all actors involved, car manufacturers, government, insurance companies, branch organisations, network providers.
T5	Splitting the CAN bus of the car into two separate systems (one for motor management and one for other systems like entertainment and navigation) makes it harder for an attacker to gain access to the motor management of the car. This triggers the inhibitor "high level of technical difficulty".
T6	Annual cyber security threat awareness campaign by the government to educate the general Dutch public on cyber security issues.
T7	Each car manufacturers must implement and publish a responsible disclosure policy
T8	Car manufacturers must start a, preferably European, "hall of fame" for those ethical hackers that exposed cyber security vulnerabilities in connected cars and complied to the responsible disclosure policy.

Table 3 Requirements Threat actors

3 Actor analysis

In this chapter we examine the actors in the automotive industry that play a role in the construction and security of the connected car. We look in the actions and responsibilities of these actors, their interests and how they act on the security challenge of the connected car. The actor analysis leads to the design requirements that we need for the construction of the multi actor roadmap to improve the security of the connected car.

3.1 Actor overview

As presented in the previous chapter the figure below shows the actor overview based on the connected car ecosystem.⁹¹ In the previous chapter we discussed the threat actors. In this chapter we look at the other actors and indicate their interests in order to understand why they act as they do in the case of security of the connected car. We present several actual cases to illustrate the normal behaviour including the actions of our actors in the connected car case. The indicated actors we discuss in this chapter are: car manufacturers, the government, insurance companies, branch organisations, network provider and car users.

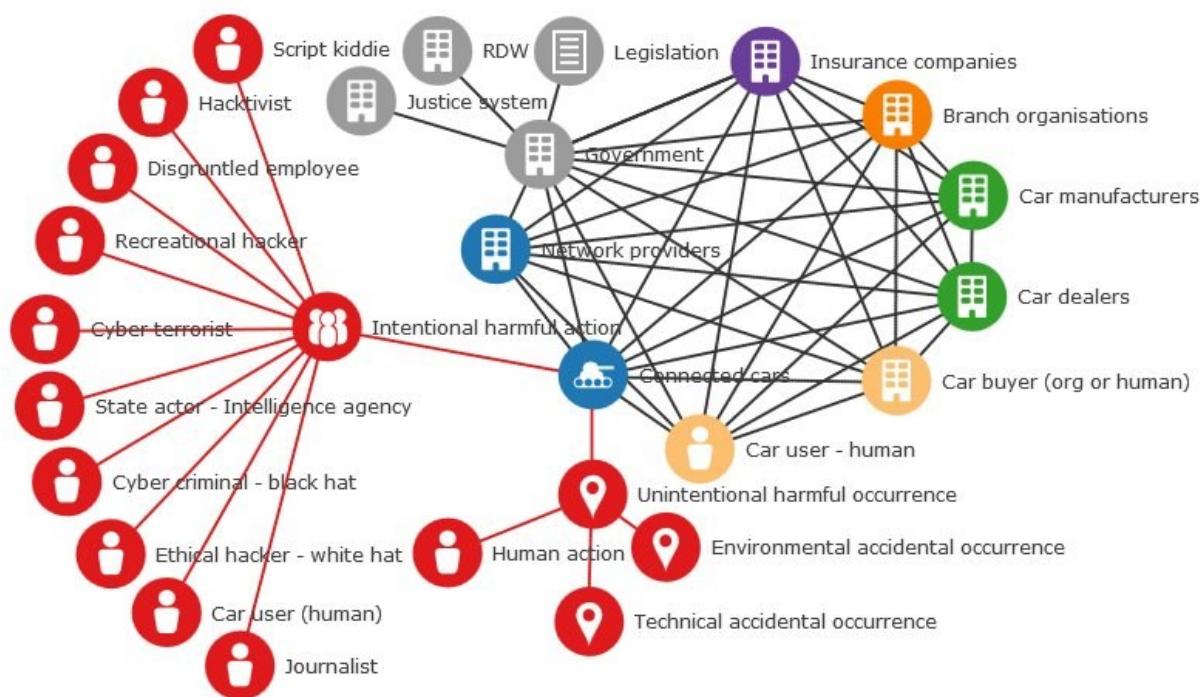


Fig 19 Actor overview in the connected car ecosystem⁸⁹

3.2.1 Car manufacturers

We start with an analysis on the risk appetite of the car manufacturers. The most important thing for the car manufacturer is profit and business continuity. Security issues are only be addressed when it directly threatens the business of the car manufacturers. Important factors are car brand reputation, market share and financial figures. Car manufacturers weigh the impact of these three business factors in each separate security case. They weigh the security investments to prevent breaches and damage on the one hand, and the possible effects on car brand, market share and financial on the other hand. Car manufacturers have a moderate risk appetite. They do accept some damage and financial loss, but when this

⁹¹ The actor overview is based on literature: Gutierrez, M., 2014; Oosterbaan, W., Lei van der G., 2014; Verizon, 2016 and our interviews.

exceeds the expected financial impact, they act to safeguard their business. The risk appetite of the car manufacturers is an important factor to take into account when you want to trigger a change in behaviour of the car manufacturers. The expert interviews confirms our findings.⁹²

The car manufacturers seem to follow the 3D model before they act. The 3D model consists of three layers before the actor takes appropriate action: Deny, Delay, Detail. The first layer is "Denial". The actor will deny that there is a case in which he has to act. Arguments that are used in this phase are: this is just a single case incident, we have never heard this before, the issue at hand is theoretical etc. The second stage of this model is "Delay". In this phase the actor stretches the timelines as far as possible. They do this for several reasons like: raising the cost of a possible lawsuit and hoping the issue at hand solves itself in time. The actor may also start a lawsuit against the person who pointed out the issue. The third phase of the 3D models consists of looking into the "Details" of the case. Can we find a way around the issue at hand. This can be done by changing the definitions, the timeframe of the incident, the geographical location and the applicable rules & regulations. The actor takes appropriate steps after dealing with these three steps in the 3D model. After implementing the required measures the actor states that mistakes are made. The incident happened "long ago" and it will never happen again.

In the LandRover case, four of our actors interact in a recognisable pattern. These actors are: the car user who unintentionally acts in an understandable but not so smart way. The car manufacturer that is reluctant to act. The insurance company that wants to reduce their loss. The criminal that takes advantage of the flaw in the system and steals the car. This case is about the high end LandRover Evoque that was presented in the media in 2015.⁹³ The facts of this case are confirmed by an expert in 2016.⁹⁴ In the LandRover case the car user must click twice on his key to lock the car and activate the car alarm. In case the user only clicks once, the doors shut without activating the car alarm. Most car users were unaware of the fact they had to click twice to activate the alarm of the car. Criminals discovered this security flaw and started to steal LandRovers on a large scale. In fact, the chance a LandRover gets stolen in the Netherlands is 1 in 30, as the normal chance with other brands is 1 in 800.⁹⁵ In reaction the insurance companies started to demand extra security measures to reduce their loss and started to put some pressure on LandRover. LandRover reacted and created a patch to overcome this security issue, but did not actively push the solution to the car users. The effect is that still today a significant number of LandRovers is not patched and the vulnerability still exists.

In another illustrative case the car user and the car manufacturer interact in another recognisable pattern. The justice system and the government are also actors in this case. The car user experiences a malfunction in the product and the car manufacturer tries to ignore this because the costs to fix this seem too high. In the end the case gets out in the media or in court, all kinds of experts look into the case and the car manufacturer still has to solve the product malfunction. On top of that the car manufacturer has to pay a fine to the authorities and promises it will never happen again. We already discussed the Chrysler⁹⁶

⁹² Kerkhof, van M., 2016; Hoop, de A. 2016

⁹³ Weijer, B., 2015

⁹⁴ Visser, T., 2016

⁹⁵ Weijer, B., 2015; Visser, T., 2016

⁹⁶ Chrysler, Illinois, 2015

case. The Chrysler case is worth mentioning because of two reasons. The first reason is that hackers showed that the Chrysler could be hacked and that the vulnerability existed in many other cars as well.⁹⁷ The second reason is the way Chrysler patched the security vulnerability and informed the car user. When Chrysler was confronted with the security breach, the company reacted with a denial of the facts. Confronted with the evidence they released a patch on a website and sent a letter to their car users with the request to download the software and patch the vulnerability by using a USB stick. Although this might be a financially efficient way to inform and patch security vulnerabilities, it seems not a logical way to implement security patches. The way the Chrysler patch was communicated, introduces a new attack vector for criminals. They can persuade the end user to install the malware / ransomware themselves by sending them a letter and an USB stick to "update" the car software.

Another case is the Toyota⁹⁸ class action lawsuit. The Toyota case started with a car user who was confronted with a malfunction. This case started in 2005 with a Toyota Camry that crashed due to a defect in the electronic throttle control system of the car. The class action lawsuit against Toyota started in 2008. In 2010 Toyota recalled approximately 2,3 million cars with a gas pedal malfunctioning. Toyota had to pay 16.4 million US dollar to the NHTSA in April 2010, because they failed to report the problems with the malfunctioning of the gas pedals. The verdict of the class action in the Toyota case came in 2013. The verdict was that Toyota was liable for the product malfunction and that the company was reckless and therefore had to pay 1.5 million dollar to each of the plaintiffs. Toyota CEO North America, Jim Lentz, said that the company learned to be more transparent, act more quick when confronted with product issues and not to mislead customers by concealing and making deceptive statements.⁹⁹ This pattern of behaviour is not unique to Toyota. Looking at recent court cases, other car manufacturers seem to react in the same way when confronted with product liability issues. Future court cases involving connected cars, will be complicated because the safety and security aspects of a malfunction must be taken into account. What was the root cause for the malfunction? Was the security of the system enough? Was the car properly patched with the latest security patches? Is there a security standard the car manufacturer should have implemented? Is it reasonable to hold the car manufacturer liable for the damage? It is reasonable to expect new business deriving from this trend. Experts and businesses will offer new proposals into the connected car market to fill this void.

3.2.1.1 Economic factors from car manufacturer perspective

This paragraph identifies the economic factors from the car manufacturing actor perspective that influences the cyber security of connected cars. The economic factors are determined in combination with the actors the car manufacturers interact with. These actors are the government, insurance companies, branch organisations and car users.¹⁰⁰

The first and most important element is the positive business case of the car manufacturers by introducing car security of the car software. The business case in combination with the business continuity of the car manufacturer is weighed in order to determine if the investment is important enough. Security issues are only be addressed when it directly threatens the

⁹⁷ Greenberg, A., 2015b, p1

⁹⁸ Toyota class action lawsuit, Oklahoma, 2008; Toyota class action lawsuit, Oklahoma, 2013

⁹⁹ Rechtin, M., 2014

¹⁰⁰ See figure 19 for the full actor overview.

business of the car manufacturers. Important factors are car brand reputation, market share and financial figures. Car manufacturers weigh the impact of these three business factors in each separate security case. They weigh the security investments to prevent breaches and damage on the one hand, and the possible effects on car brand, market share and financial on the other hand. The Gordon-Loeb model¹⁰¹ states that the security investments should not exceed 37% of the expected loss without security investments. We keep this in mind when we define the required actions of the automotive industry to improve the cyber security of connected cars. The answers to the defined sub questions form the input for the multi actor roadmap. The attention and actions we need to improve the cyber security of the connected car will be countered by resistance from the automotive industry. We see this as the first phase regarding the “sense of urgency” in the change model by Kotter.¹⁰² Car manufacturers have a moderate risk appetite. They do accept some damage and financial loss, but when this exceeds the expected financial impact, they act to safeguard their business. Security cost money that cannot be spent on new features for customers. Expert interviews confirm this finding.¹⁰³ The automotive market is a competitive market. For example: a regular car has 50 to 70 ECU's.¹⁰⁴ Each of these ECU nodes can contain vulnerabilities that can influence the cyber security of the car systems. Car manufacturers are willing to spent one US dollar per critical node on security, with a maximum of 20 US dollar per car.¹⁰⁵ That leaves little room for a positive business case on car security.

The next factor that plays a part, is that car manufacturers tend to look at each other to take the first step. The argument is that other car brands also don't have a high level of car security. So why bother and spent money on that? Sometimes one company takes the lead to address certain issues. When that is to be profitable, other manufacturers will follow. An example of this is Volvo stating that they are liable for all damage with connected cars. The CEO of Volvo states “...that Volvo will accept full liability whenever one of its cars is in autonomous mode”¹⁰⁶

The next element is lack of knowledge and awareness. Not all car manufacturers believe that car hacking is a real risk. Their risk appetite on car security is moderate because there is no record of a successful executed connected car hack in a “live” situation. The assumption is that our modern day society connected cars are safe and secure. The only known hacks of connected cars were executed by ethical hackers and researchers who wanted to show that the system was not secure. The interesting question is now: is the risk of connected car security underestimated or are the security researchers exaggerating these risks?

Media attention based on security incidents are also a factor that can triggers changes in car security. An example of this, is the first death¹⁰⁷ due to a failing system in a connected car. The first death due to a “self-driving” car occurred in 2016. Joshua Brown died using the “Autopilot” in his Tesla model S.¹⁰⁸ There are four lines of text that express grief in the official Tesla statement and 34 lines of text that should make clear that the accident is not the fault

¹⁰¹ Gordon, L., Loeb, M., 2002

¹⁰² Kotter, J. 1996

¹⁰³ Kerkhof, van M., 2016; Zijden, van der, B.; Mason, A., 2016; Hoop, de A., 2016

¹⁰⁴ Electronic Control Unit, Geraets, M., 2016

¹⁰⁵ Geraets, M., 2016

¹⁰⁶ Volvo, 2016a

¹⁰⁷ The first reported death, due to a crash of a “self-driving car”, is Joshua Brown in 2016 in the USA.

¹⁰⁸ Tesla, 2016

of Tesla. Even if that is the case, the wording “autopilot” in the Tesla Model S is giving the end user the wrong idea. The Cambridge English dictionary states that an autopilot is “a device that keeps aircraft, spacecraft, and ships moving in a particular direction without human involvement”.¹⁰⁹ The essence of an “autopilot” is that it functions “without human involvement”. A quote from the official Tesla statement regarding the accidental death in relation to the autopilot feature: “When drivers activate Autopilot, the acknowledgment box explains, among other things, that Autopilot “is an assist feature that requires you to keep your hands on the steering wheel at all times,” and that “you need to maintain control and responsibility for your vehicle” while using it.” It proves that the communication from the car manufacturers to the end user can benefit from communication improvements on security and safety issues. This communication improvement starts with clear communication in a language the end user understands. This is a requirement that we can use in our roadmap.

Who pays the cost when security fails, is the next factor that plays a role. Security issues occur when the actor who should protect the system is not the one paying for the cost if the security fails. This is also the case in the cyber security of connected cars. The car manufacturer is responsible for the delivery of a cyber secure connected car, but the car user is the one who pays when the car security is breached. So why would car manufacturers invest heavily on the cyber security of connected cars? This issue can be solved by government legislation and penalties from the judges in our justice system.

Worth mentioning is the first “digital recall” in the world in 2015. The ADAC^{110 111} found a security vulnerability in all BMW Connected Drive models. All it took was a simple “one time preparation” and a few minutes to open these BMW cars without a trace. 2.2 Million cars, including BMW, Mini and Rolls Royce are effected of this hack by phone. The ADAC made the security breach public after the agreed embargo period with BMW. BMW solved the security issue by encrypting the communication of the car.

The roadmap requirements for the Car manufacturers we derive from this analysis are:

C1	Design a connected car architecture where the motor management systems are fully separated from the other car systems.
C2	Design at least four security zones into the system design. Example of these security zones: Red (the outer shell of the car facing the outside communication), Orange and Green (the data of the car user that should be protected). The Blue zone is the management interface for firmware updates etc.
C3	Use system redundancy into the car architecture design. Examples of this can be found in the aircraft industry.
C4	The car manufacturers cooperate with branch organisations, insurance companies and government in developing (international) standards on security requirements, communication and storage standards.
C5	Use detection systems to detect anomalies in the internal network of the connected car.
C6	In an autonomous car, the “intelligence” must decide on at least two out of three systems that agree that the chosen action is safe for the car user.
C7	Each connected car should be tested on security issues by the car manufacturer before market launch.
C8	Code review and proper “punishment” of developers that built in “Easter eggs”.
C9	Change of culture within the development department that Easter eggs in software

¹⁰⁹ Cambridge University, 2016

¹¹⁰ ADAC, 2015

¹¹¹ ADAC means Allgemeiner Deutscher Automobil-Club

	code are not ok.
C10	Development and publishing of responsible disclosure agreement to ensure that external white hat hackers contribute to the connected car security and are not punished. (see Tesla example, appendix 5)
C11	The Car manufacturer limit the number of employees and third parties that have access to the stored data as much as possible. RBAC ¹¹²
C12	Clear and understandable communication to the end user on terminology, processes, security and use of the features the connected car contains. Example: the Tesla Autopilot case.

Table 4 Requirements Car manufacturers

3.2.2 Government

Legislation is often the first factor people think of when it comes to the role of the government. In the case of automated driving and connected cars the current legislation must be updated. The Vienna Convention on Road Traffic ¹¹³ states in article 8 that “Every moving vehicle ...shall have a driver”. Article 13 states that “every driver of a vehicle shall in all circumstances have his vehicle under control....” This convention from 1968 ¹¹⁴ on which the EU road traffic rules are based should be updated to allow autonomous cars. Some proposals are submitted to adjust this convention, but these proposals are not yet agreed upon. Legislation can be an economic factor as well. Legislation can impose all kinds of requirements on manufacturers that cost money to implement in the product. There is no legislation in the Netherlands that deals specific with the issue of cyber security of connected cars. The legislation that deals with traffic and cars is already in place and deals with the rules and regulation of traffic. ¹¹⁵ Other legislation that is relevant to the automotive industry is regulated in civil law. ¹¹⁶ The RDW ¹¹⁷ has been given a mandate by the Dutch government to assess connected cars before these are allowed on Dutch territory. The RDW has been given a mandate to set requirements for connected cars in the Netherlands. ¹¹⁸ The introduction of the EU GDPR ¹¹⁹ in the near future will have an impact on the current use of car data by the car manufacturers. Due to the heavy fines that can be imposed on the car manufacturers when they do not comply with the GDPR, we expect that the introduction of the GDPR will have a positive effect on the data protection of car data and its security.

Not only the Netherlands are struggling with the introduction of proper legislation to address the issues of connected – and autonomous driving. The CAVCOE ¹²⁰ presented a report to the Canadian government in which 30 recommendations were given. ¹²¹ Two of those recommendations are about security. The first recommendation is to develop a national cyber security strategy and standard for autonomous cars. ¹²² The report states that without this the first major hack might neutralise a lot of progress for a long time. The second recommendation is to proactive analyse and mitigate the potential threat of autonomous cars

¹¹² RBAC – Role based access control

¹¹³ United Nations, 1968

¹¹⁴ The Vienna Convention on Road Traffic 1968 is ratified by 74 countries.

¹¹⁵ Wegenverkeerswet and related legislation

¹¹⁶ Burgerlijk Wetboek, Onrechtmatige daad and product aansprakelijkheid.

¹¹⁷ Doll, G., Rijksdienst voor het Wegverkeer, 2016

¹¹⁸ Doll, G., 2016

¹¹⁹ EU General Data Protection Regulation

¹²⁰ CAVCOE, Canadian Automated Vehicles Centre of Excellence

¹²¹ CAVCOE, 2015

¹²² CAVCOE, 2015 rec. 21.

in the hands of criminals and terrorists.¹²³ These two pieces of advice also seem relevant for the Dutch situation. As the picture below shows, several states within the USA tried to introduce legislation that deals with autonomous driving as well. The picture indicates that not all legislation proposals on autonomous driving are immediately accepted. Because of the fact that one of the major concerns of the consumers and the automotive industry is the wish for proper legislation, the proper legislation will eventually emerge and be implemented. The Dutch government consulted the automotive branch on autonomous driving in 2014.¹²⁴

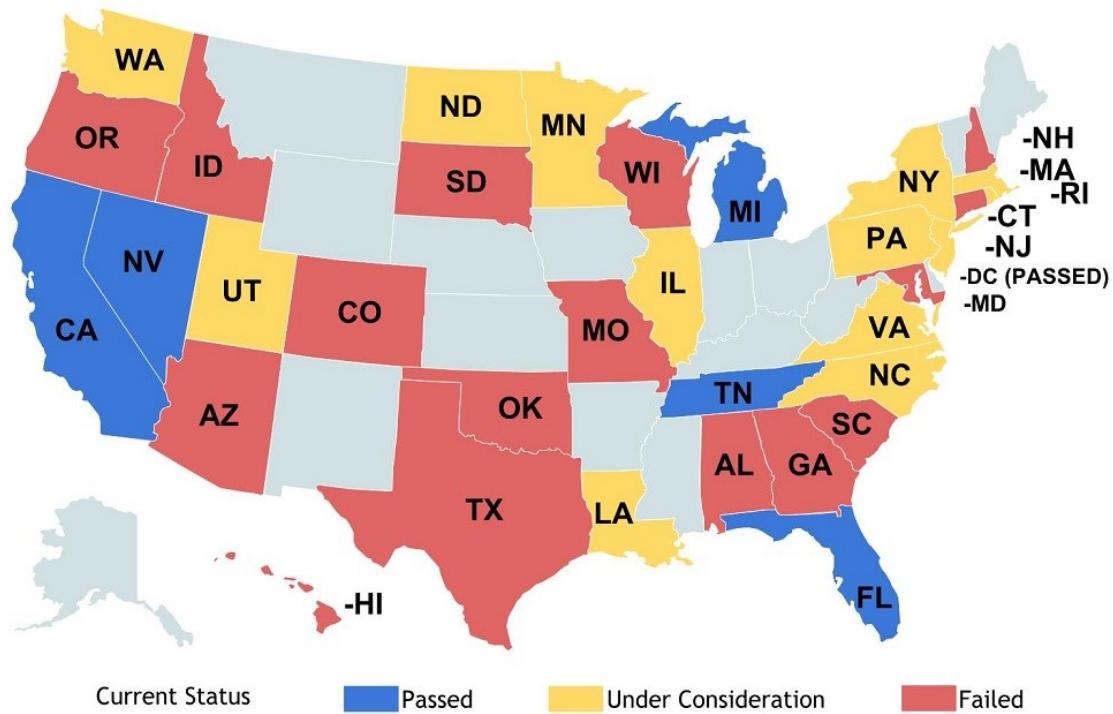


Fig 20 USA state legislatures that have considered a bill on autonomous driving as of June 2016¹²⁵

The AMvB¹²⁶ concerning “autonomous cars” gives the RDW the authority to test and authorise new innovative cars on the Dutch public roads. Legislation is necessary to address consumer concern, insurance issues, car and road safety. Legislation is also needed to protect the car manufacturers. In the current situation the RDW is allowed to waive certain requirements and set new requirements for the manufacturers.¹²⁷ This is confirmed in the RWD expert interview.¹²⁸ Part of this new situation, is that the car manufacturers may also get a waiver for certain traffic regulations. The text indicates this is about car lights and reflectors, but it leaves room for interpretation. The concern about liability is not yet addressed by the Dutch government.

¹²³ CAVCOE, 2015 rec. 25

¹²⁴ Overheid, AMvB, 2014

¹²⁵ Stanford university, 2016

¹²⁶ AMvB, Algemene Maatregel van Bestuur concerning “zelfrijdende auto”, 2014

¹²⁷ Overheid, Regeling voertuigen, 2016

¹²⁸ Doll, G., 2016

The Dutch government is also active in public private partnerships like DAVI.¹²⁹ The goal of DAVI is “to research and demonstrate automated vehicles on the Dutch roads.”

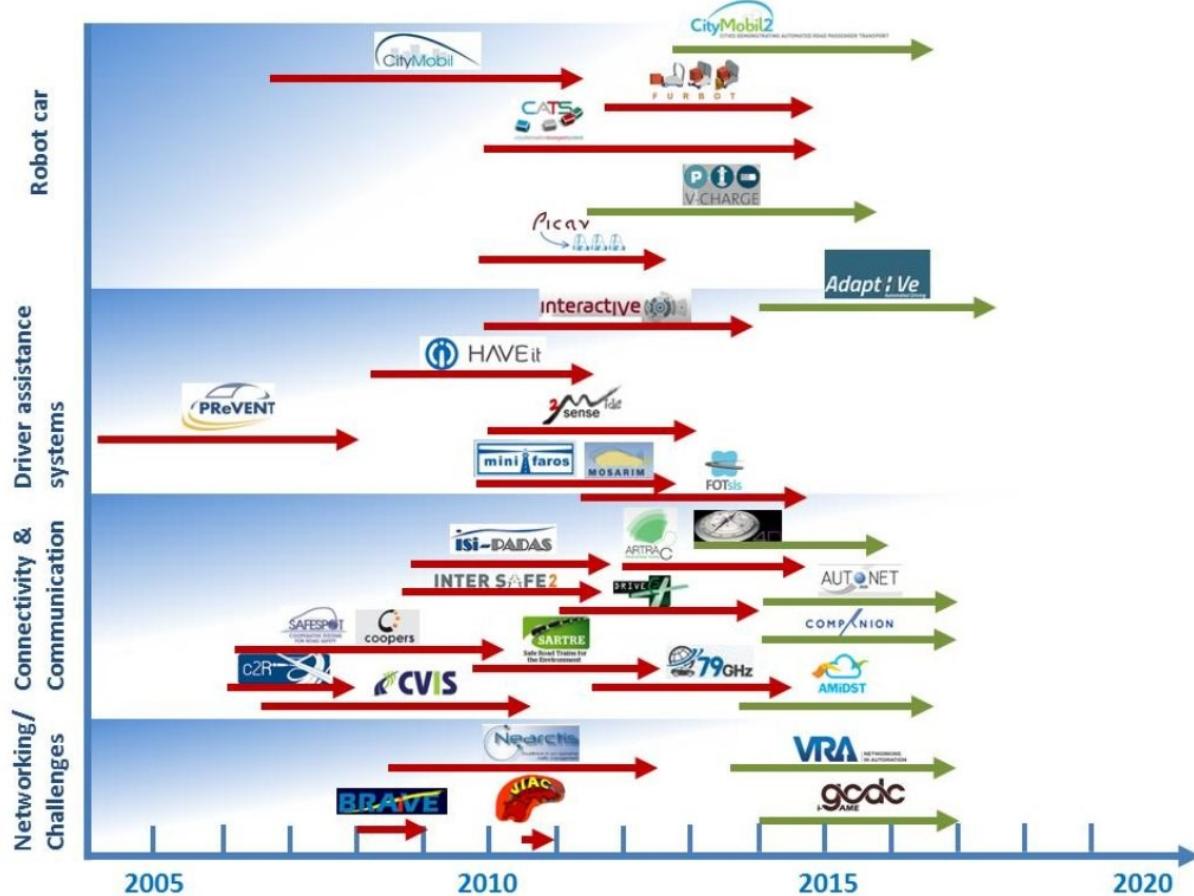


Fig 21 EU projects on automated driving.¹³⁰ The red arrows projects are finished. The green arrows are current projects.

There are international standards as described above. Those standards include elements that address some elements of the cybersecurity of connected cars. The lack of international agreed standards on the security of connected cars, makes it difficult for car manufacturers to introduce car security. What if you put too much security in the product that makes it too expensive compared to the competition? There are several initiatives in the Netherlands that try to deal with this issue by creating standards to self-regulate the automotive branch.¹³¹ Examples are SIMS^{132 133} and Connekt.^{134 135} The SIMS initiative was stopped in 2016. Mr. De Waal of Bovag and Mr. Boutens of RAI stated that, after seven years of cooperation, their goal of creating awareness was achieved and that their strategic goals were now different. The driving forces of SIMS, Bovag¹³⁶ and RAI, both choose their separate ways and now continue with their own initiative. This shows again how hard it is to get a broad agreement on the standards in the automotive sector. Initiatives like SIMS make progress in defining the

¹²⁹ DAVI, Dutch Automated Vehicle Initiative <http://davi.connekt.nl>

¹³⁰ Dokic, j., et al, 2015, p10

¹³¹ SIMS, 2015, p8

¹³² Sombekke, J., 2016

¹³³ SIMS means “Standaardisatie- en Informatiebeleid MobiliteitsSector”, <http://www.sims4u.org/>

¹³⁴ Juffermans, N., 2016

¹³⁵ Connekt, <http://www.connekt.nl/home/>

¹³⁶ Bresser, H.; Kamps, E., 2016

agreed standards when all parties agree upon the required outcome. When parties do not agree upon the underlying principles and the outcome affects the business case of the parties involved, this kind of self-regulation does not work. In those situations the government has to step in. Questions that the government has to answer to give guidance to the automotive industry are: Is the collected car data owned by the car owner (consumer) or by the car manufacturer? Another question is “how long must the car manufacturer support security patches for the connected car?”¹³⁷ The answer to these two questions have a huge business impact on the automotive industry. New initiatives, like the VW and LG cooperation on a new connected car platform, try to gain momentum in order to set new standards.¹³⁸

The Australian government published a report by Brown¹³⁹ that describes which steps the government can take to encourage manufacturers to implement security measures into consumer products. The steps in this report are defined based on lessons learned. The steps seem to fit also in our case to improve the security of connected cars. The figure below indicates that the pressure of the chose government intervention may vary.

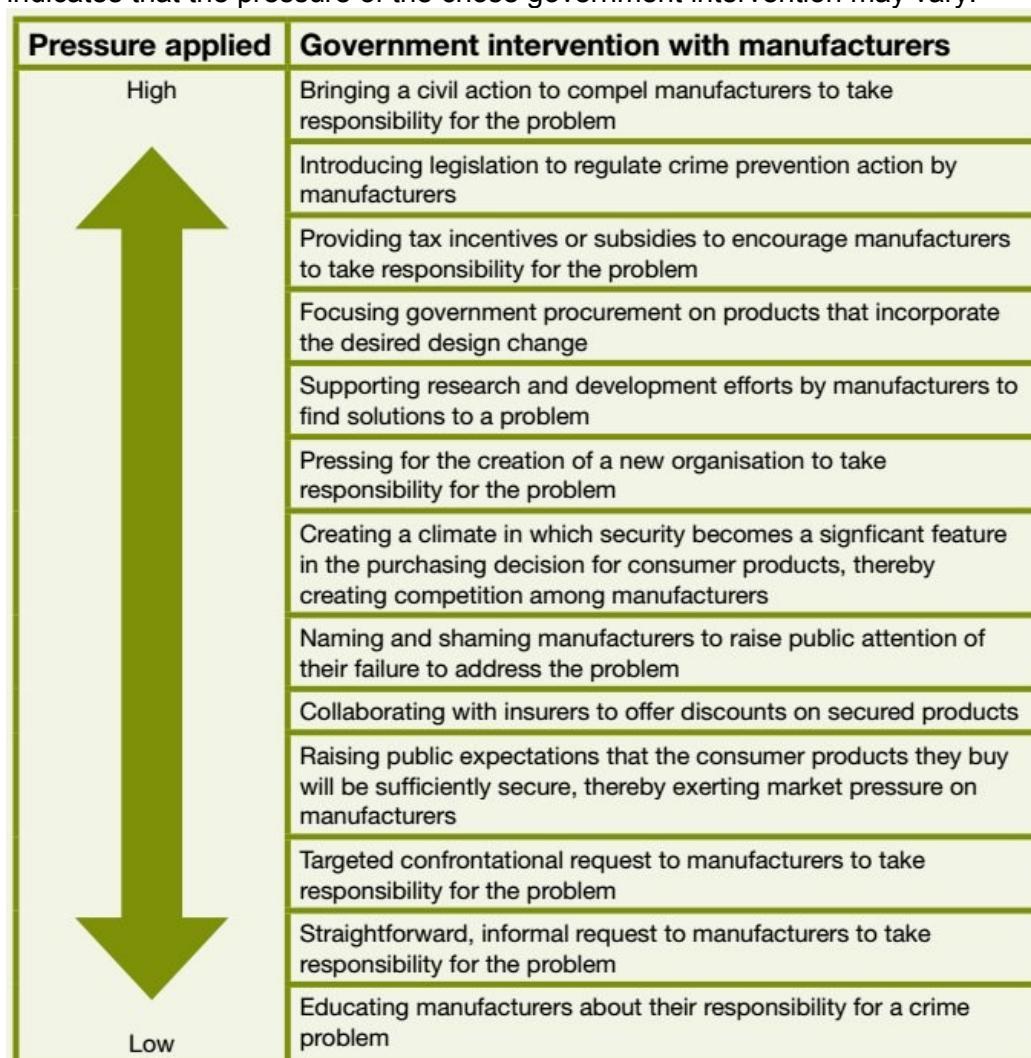


Fig 22. “Hierarchy of government interventions to encourage manufacturers to incorporate crime prevention measures into consumer products” as described by Brown.¹⁴⁰

¹³⁷ See survey question 3.4

¹³⁸ LG, Volkswagen, 2016

¹³⁹ Brown, R., 2013

¹⁴⁰ Brown, R., 2013 p5

The roadmap requirements for the Government we derive from this analysis are:

G1	Appropriate legislation on liability of connected cars & autonomous vehicles, platooning, privacy issues, insurance, driving licence, standards and security requirements.
G2	The government cooperates with branch organisations, insurance companies and car manufacturers in developing (international) standards on security requirements, communication and storage standards.
G3	See T6. Annual cyber security threat awareness campaign by the government to educate the general Dutch public and businesses on cyber security issues.
G4	The government limit the number of employees and third parties that have access to the stored data as much as possible. RBAC
G5	The government must answer fundamental questions with a huge business impact to guide the automotive industry. Examples are: Is the collected car data owned by the car owner (consumer) or by the car manufacturer? How long must the car manufacturer support security patches for the connected car. ¹⁴¹

Table 5 Requirements Government

3.2.3 Insurance companies

Insurance companies can play a big role in the improvement of the security of the connected car. At this moment, insurance companies do not demand any form of cyber security of connected cars. What complicates the matter is that car insurance companies do not record or log cyber security related incidents of connected cars. The insurance companies cannot indicate how much cyber security related incidents, linked to connected cars, take place.¹⁴² Insurance companies act when there are a lot of claims that cost them money. In such cases the insurance companies demand additional security measures from the car manufacturers. An example of this is the LandRover Evoque case in 2015. A lack of security resulted in a 1 in 30 chance the LandRover gets stolen. The normal figures for these type of cars is a 1 in 800 chance.¹⁴³ This resulted in additional demands for security from the insurance companies.

Branch organisations and insurance companies are sometimes interwoven. An example of this is the ANWB.¹⁴⁴ The ANWB offers special insurance policies to customers with an additional discount when they drive safely. The car user must agree to have a monitoring device linked to the OBD port of the car. That unit monitors car movements and collects car data. Elements that are collected are for example: speed, timestamp, the way the car accelerates and brakes. This data is sent to the ANWB for analysis. If the driver drives within the ANWB required specifications a discount is given on the costs of the insurance policy. At this moment the ANWB sold 1800 of these "monitored driving" insurance policies of which 77 people were contacted by the ANWB on their driving behaviour. About 50% of these drivers changed their way of driving. Those drivers who did not change their behaviour, were warned. If they continue their way of driving, they are given the choice to terminate the insurance policy within five days. After that the ANWB terminates the policy. Insurance companies register users with a terminated policy in the CIS database.¹⁴⁵ Insurance companies have access to this database. A registration in the CIS database means that it will

¹⁴¹ See survey question 3.4

¹⁴² Geurts, P.; Beveren, van J., 2016

¹⁴³ Weijer, B., 2015; Visser T., 2016

¹⁴⁴ ANWB. Algemene Nederlandse Wielrijders Bond. The correct terminology is "Koninklijke Nederlandse Toeristenbond ANWB".

¹⁴⁵ CIS, Stichting Centraal Informatie Systeem. <https://www.stichtingcis.nl/> F. Smith of the ANWB indicated on 09-01-2017 that a policy termination by the ANWB does not lead to a registration within the CIS database.

become very hard to obtain a new car insurance policy. Research by the Consumentenbond in November 2016 showed that the ANWB terminated a few insurance policies due to continuous “unsafe” driving.¹⁴⁶ The ANWB is just one vendor of this kind of car insurance policies.¹⁴⁷ The Consumentenbond has several concerns on these kind of policies. The first concern is the fact that the data that are logged and shared among the insurance companies. The boundaries the driver is required to limit himself to, are not explicit and clear. Another concern is that the collected data should not be used to add extra fees to certain kind of consumer categories. The insurance companies should not use this data to exclude consumers from future insurance policies. The car user should have the right to look into the collected data and have data corrected or removed upon request.¹⁴⁸ The insurance companies should not gather more data than they strictly need for the car insurance service. The Consumentenbond notices that many insurance companies gather more data than they should. The last concern is who has access to this kind of data. The terms of use are not clear on this.

This kind of behaviour poses a security threat because it gives the attacker an attack vector to this kind of data and possibly to enter software of the connected car as well. This can be done via the management port. It is possible to breach the security of the management update channel that is used to update the firmware of the monitoring device. Another attack vector is the communication device, encryption standard and network communication from the car to the insurance company. The last attack vector is a breach of the database of the insurance company where all the collected data is stored and processed.

The roadmap requirements for the Insurance companies we derive from this analysis are:

I1	The insurance companies log all cyber security incidents related to connected cars.
I2	The insurance companies do a trend analysis on the gathered data and share this with government policy makers.
I3	Insurance companies define and communicate a set of minimum security requirements a connected car must have.
I4	In case insurance companies collect data from connected cars: The insurance companies use encryption in communication and storage.
I5	In case insurance companies collect data from connected cars: The entire chain of collected data by the insurance companies are audit proof.
I6	The insurance companies provide information to its customers on what data is stored, how long it is stored and who has access to that data.
I7	The insurance companies limit the number of employees and third parties that have access to the stored data as much as possible. RBAC ¹⁴⁹ .
I8	The insurance companies cooperate with government, branch organisations and car manufacturers in developing (international) standards on security requirements, communication and storage standards.
I9	The insurance companies store the collected data as long as needed and as short as possible.

Table 6 Requirements Insurance companies

¹⁴⁶ Consumentenbond, 2016, p 6 jo 20 – 23

¹⁴⁷ Other vendors of these kind of insurance products are: ASR, Reaal and Delta Lloyd, ChipWise car insurance policy; Aegon, CarKroodle car insurance policy; Allsecur, MyJINI car insurance policy.

¹⁴⁸ This is already an existing obligation from the Dutch “Wet Persoonsgegevens.”

¹⁴⁹ RBAC – Role based access control

3.2.4 Branch organisations

The branch organisations in this paragraph are active in the Netherlands. Each country has its own branch organisations and some branch organisations work in Europe or worldwide. Some of these international branch organisations might have the same goals as these Dutch branch organisations.

The ANWB is an organisation with commercial interests that delivers road assistance when your car breaks down and also sells additional services and products. The ANWB offers a discount on car insurance policies when drivers use the ANWB plugin driving logger that monitors the driver behaviour.¹⁵⁰ The ANWB is collecting car data and is also using this data for its own policy and profit. We described the details in the paragraph on the insurance companies. The use of an insurance dongle in the OBD port generates new security vulnerabilities. Security researcher Thuen showed in 2015 that these kind of dongles generate a new attack vector for attackers.¹⁵¹

Another branch organisation is SIMS.¹⁵² SIMS is a cooperation between the branch organisations BOVAG and RAI. A lot of companies and experts joined forces in order to generate an agreed standard on mobility data. The goal of SIMS is to define an agreed information standard for mobility data. This standard can be used in the automotive industry. The SIMS cooperation ended in July 2016. SIMS stated in a press release, via the RAI, that the goal of SIMS to address the importance of mobility data is achieved.¹⁵³ BOVAG stated in a notification to its own members that “the data marriage between BOVAG and RAI is over”. BOVAG states that the interests of BOVAG and RAI are too far apart to continue the SIMS initiative. The opinion of BOVAG is that it is not possible to unite the interests of retail organisations and manufacturers.¹⁵⁴ The same notification states that the opinion of BOVAG is that the end user customer should have control over the collected car data. The RAI organisation thinks otherwise and is now working with its own Intelligent Transport Systems (ITS) platform. SIMS stated in their annual 2015 report that they tried to come up with standards in order to self-regulate the automotive branch regarding to this matter.¹⁵⁵ Looking at the standards and documentation SIMS has delivered, it strikes that there is little written down on the data integrity and security of the gathered car data.

Another branch initiative is the Amsterdam Group.¹⁵⁶ This strategic alliance has the objective to develop Intelligent Transport Systems (ITS) in Europe. Large organisations like CEDR¹⁵⁷, ASECAP¹⁵⁸, POLIS¹⁵⁹ and C2C CC¹⁶⁰ participate in the Amsterdam Group initiative. The Amsterdam Group addresses the cyber security aspects of the connected car in the “open issues” that have to be addressed. They state: “Agree on Security & Privacy framework” is

¹⁵⁰ ANWB, 2016

¹⁵¹ Fox-Brewster, T., 2015

¹⁵² SIMS means Standaardisatie- en Informatiebeleid MobiliteitsSector. SIMS was initiated in 2009.

¹⁵³ RAI, 2016

¹⁵⁴ BOVAG, 2016

¹⁵⁵ SIMS, 2015, p8

¹⁵⁶ Amsterdam Group, <https://amsterdamgroup.mett.nl/default.aspx>

¹⁵⁷ CEDR, Conférence Européenne des Directeurs des Routes, <http://www.cedr.fr/home/>

¹⁵⁸ ASECAP, European Association of Operators of Toll Road Infrastructures,

<http://www.asecap.com/index.php?lang=en>

¹⁵⁹ POLIS, Network of European cities and regions to develop innovative technologies and policies for local transport, <http://www.polisnetwork.eu/>

¹⁶⁰ C2C CC, Car2Car Communication Consortium, <https://www.car-2-car.org/index.php?id=5>

an open issue in which the C2C CC is leading.¹⁶¹ Indications for the lack of security was also concluded in an analysis by Connekt of 2014, which stated that “not every car manufacturer takes its responsibility regarding the security aspects.”¹⁶²

An European analysis on the Cooperative Intelligent Transport Systems (C-ITS) shows several legislation, security and privacy issues but does not come up with an answer to the posed issues.¹⁶³ Other initiatives to improve the security of the connected car are “E-safety Vehicle Intrusion Protected Applications” (EVITA), the Trusted Platform Module (TPM) and the Secure Hardware Extensions (SHE). There are other initiatives to define the new cyber security standards that can be used in the automotive industry. We mention ISO 26262, NIST, SAE J2980, SAE J3061 and the published documentation of the NHTSA. The problem with these initiatives is that neither of them is accepted worldwide and neither of them describes an adequate cyber security framework that can be used in the connected and autonomous car.

The US Auto ISAC¹⁶⁴ initiative started in 2015. This ISAC addresses the cyber security aspects of connected – and autonomous cars. Another American initiative is the Auto Alliance. This Auto alliance claims to address the industry wide emerging threat regarding to cyber security issues.¹⁶⁵ Both are American initiatives with an American view on security and privacy. There are no such initiatives in Europe or Asia. Both American initiatives look closely to the hacking events that present new vulnerabilities found. Examples of these hacking events are: DEF CON¹⁶⁶, Black hat¹⁶⁷ and SAE Battelle Cyber Auto¹⁶⁸.

The roadmap requirements for the Branch organisations we derive from this analysis are:

B1	The branch organisation provides information and advice to its members
B2	The branch organisation uses encryption in communication and storage.
B3	The branch organisations cooperate with government, insurance companies and car manufacturers in developing (international) standards on security requirements, communication and storage standards.
B4	The branch organisations limit the number of employees and third parties that have access to the stored data as much as possible. RBAC
B5	Start an European Auto ISAC to share cyber security knowledge within the (European) automotive industry
B6	Organise an annual hacking challenge for connected and autonomous cars. This information can be used to improve the connected car designs.

Table 7 Requirements Branch organisations

3.2.5 Network provider

The network provider is another actor that is part of the connected car eco system. The connected car sends its data via a network to the data collector. This network must be secure as well in order to obtain security throughout the entire chain. Other aspects that play

¹⁶¹ The addressed security aspect concerns the PKI (Public Key Infrastructure) and is linked to the ETSI TC ITS standard. <https://amsterdamgroup.mett.nl/Road+Map/Road+Map+Open+Issues/default.aspx> retrieved 12-11-2016.

¹⁶² Connekt, 2014, p1

¹⁶³ Connecting Mobility, 2016

¹⁶⁴ Auto ISAC, Automotive Information Sharing and Analysis Center <https://www.automotiveisac.com/>

¹⁶⁵ Auto Alliance, <http://www.autoalliance.org/auto-issues/cybersecurity>

¹⁶⁶ DEF CON <https://www.defcon.org/>

¹⁶⁷ Black Hat <https://www.blackhat.com/>

¹⁶⁸ SAE <http://www.sae.org/events/cyberauto/2016/>

a role are the constant growth of the data stream to and from the connected car. Networks have a limited capacity and the network provider has to ensure that there is enough bandwidth to cope with this data growth (capacity & availability).

Internet access is becoming a commodity. People expect that there is free, or low cost, access to the internet everywhere. Initiatives from Google¹⁶⁹, RailTel¹⁷⁰ and IPass¹⁷¹ fit the trend that they aim to connect as much people to the internet as possible. These initiatives provide Wi-Fi access at train stations and other public places. Google aims with the Google station project to help a “the next billion” internet users with free Wi-Fi to get online. This trend to connect more and more users to the internet, has a direct effect on the development of the connected car. In a few years people expect that their car is connected to the internet and that a variety of services is available in the car. Network providers will have to expand their network capacity in order to provide access and content to the end user. The capacity and availability problem lies in the radio access domain and not in the fixed network domain. The radio domain has a limited capacity and new innovations and international agreed standards are needed to optimise the use of this radio domain. A short overview of the wireless access network options delivers the following picture: 2G, 3G, 4G and soon 5G will become available. Other wireless options are: Bluetooth¹⁷² and Wi-Fi¹⁷³. These forms of access have different quality aspects considering range, functionality, security and cost. The respondents in the survey indicated that they expect that the wireless connection is the most vulnerable and can be used to hack into a connected car.¹⁷⁴ The facts presented in the media seems to prove them right. The Mitsubishi Outlander plug in hybrid (PHEV) was hacked in June 2016. The point of entry was Wi-Fi¹⁷⁵.

To summarise the differences between these options: Bluetooth has a short range and limited bandwidth. Wi-Fi has a medium range of about 30 meters and a bigger bandwidth. Downside is that Wi-Fi uses more energy. 4G¹⁷⁶ and 5G has a large range and a big bandwidth.

	Range	Bandwidth	Energy consumption	Possible Security
Bluetooth	Short	Small	Small	Low
Wi-Fi	Medium	Medium	Medium	Medium
4G / 5G	Large	Large	Medium	High

Table 8. Overview of the different communication options based on the current standards.

Network providers and vendors of network equipment are planning the new 5G standards to deal with the expected communication demands to and from connected cars. The picture below indicates the possible traffic flows the new standard has support. The new standards

¹⁶⁹ Hall, G., 2016 Google station <https://station.google.com/> Google project Loom is another project that aims to connect people to the internet.

¹⁷⁰ <http://www.railtelindia.com/> RailTel claims to connect 3.5 million people each month to the internet.

¹⁷¹ <https://www.ipass.com/> IPass claims to provide access to 57 million Wi-Fi hotspots in more than 120 countries.

¹⁷² <https://www.bluetooth.com/> and <https://nl.wikipedia.org/wiki/Bluetooth> Bluetooth uses 2,4 GHz radio frequency and has a range of max 10 m, power consumption is approx.. 30 microampere, max 24 Mbit per sec.

¹⁷³ Wi-Fi is a collection of wireless network standards as described in IEEE 802.11. Uses 2,4 GHz and/or 5 GHz radio frequency, range of approx. 30 m, max 600 Mbps. <https://standards.ieee.org/about/get/802/802.11.html>

¹⁷⁴ See survey question 2.4

¹⁷⁵ Lodge, D. 2016

¹⁷⁶ 4G, LTE, European Long Term Evolution uses 800, 900, 1800 and 2600 MHz, up 1,5 Gbit down 3Gbit per sec.

are necessary to cope with the expected increase in data traffic due to an increase of vehicle density, demanded quality of service and the increased data traffic to and from the connected car. The picture shows that new data flows between connected cars (V2V) and from the car to the infrastructure (V2I) emerge.

Network providers are cooperating with vendors of network equipment to define these new standards to ensure the continuous availability of the network. The new communication standards that are currently under revision are 3GPP 36.885¹⁷⁷ and Wi-Fi, IEEE 802.11X.

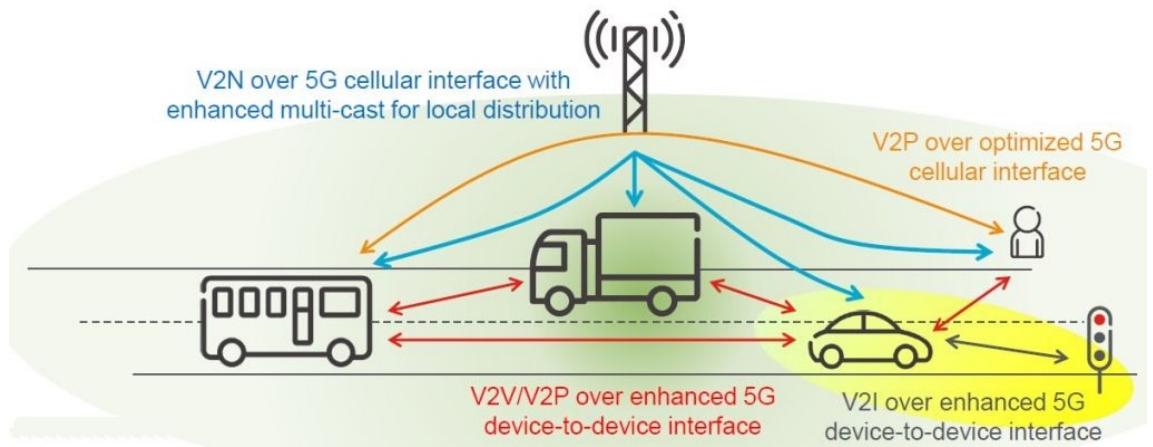


Fig 23. 5G based V2X communication flows ¹⁷⁸

Car manufacturers like Audi and Toyota are testing LTE V2X¹⁷⁹ with companies like Huawei and Deutsche Telekom on the A9 highway in Germany.¹⁸⁰ These tests focus on user friendly features and performance issues and not on the security aspects of this new technology. The roadmap requirements for the Dutch Network providers we derive from this analysis are:

N1	The network provider provides access to the network (access) and ensures that the latest security patches for vulnerabilities are implemented.
N2	The network provider delivers enough bandwidth on the access network for the required data stream (capacity & availability)
N3	The network provider uses encryption in communication and storage. (confidentiality)
N4	The network provider uses agreed communication standards in order to ensure that the message is received by the data collector as required (ensure integrity of the message)
N5	The network provider provides a handover to another network of another country when the connected car leaves Dutch territory and drives into another country.
N6	The network provider informs its customers on the terms and conditions of the provided service within the boundaries of the law.
N7	Create, test and innovate new standards to standardise the network data traffic like on LTE V2X and ITS-G5 (802.11p)
N8	The network provider limit the number of employees and third parties that have access to the stored data as much as possible. RBAC

Table 9 Requirements Network providers

¹⁷⁷ 3GPP is “Third Generation Partnership Project” and is an agreement on telecom standards. 3GPP was erected in 1998. 3GPP standards that are currently used are 3G and 4G for mobile telecom communication. 3GPP 36.885 is LTE (Long Term Evolution) based V2X

<https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2934>

¹⁷⁸ Dimitrovski, T., Sambeek, van M.; 2016, p 26

¹⁷⁹ V2X includes V2N – vehicle to network, V2P – vehicle to person, V2V – vehicle to vehicle, V2I – vehicle to infrastructure.

¹⁸⁰ Deutsche Telekom, 2016

3.2.6 Car user

The Dutch CBS indicated in May 2016, that there are about 8 million consumer used cars in the Netherlands. 7 Million of these cars are in possession of consumers. That is 477 cars per 1000 inhabitants.¹⁸¹ The CBS figures of December 2015 indicate that about 71,5% of the Dutch households possess at least one consumer used car.¹⁸² From that perspective it makes sense to look into the cyber security awareness of the general public. In the first part of this paragraph we discuss the threat awareness of the general public in the Netherlands. In the second part of the paragraph we look at the consumer concerns in relation to the connected car. TNS research of September 2016 shows that the general public are not concerned about cyber security.¹⁸³ This fact is consistent over the past few years. The research commissioned by the Dutch ministry of General Affairs and NCTV in 2012 depicted the same outcome.¹⁸⁴ The figure below shows that the threat awareness on cyber security of the general public in the Netherlands is low. The Dutch government organises an annual "Alert Online" campaign in order to raise the cyber security awareness of the general public.¹⁸⁵

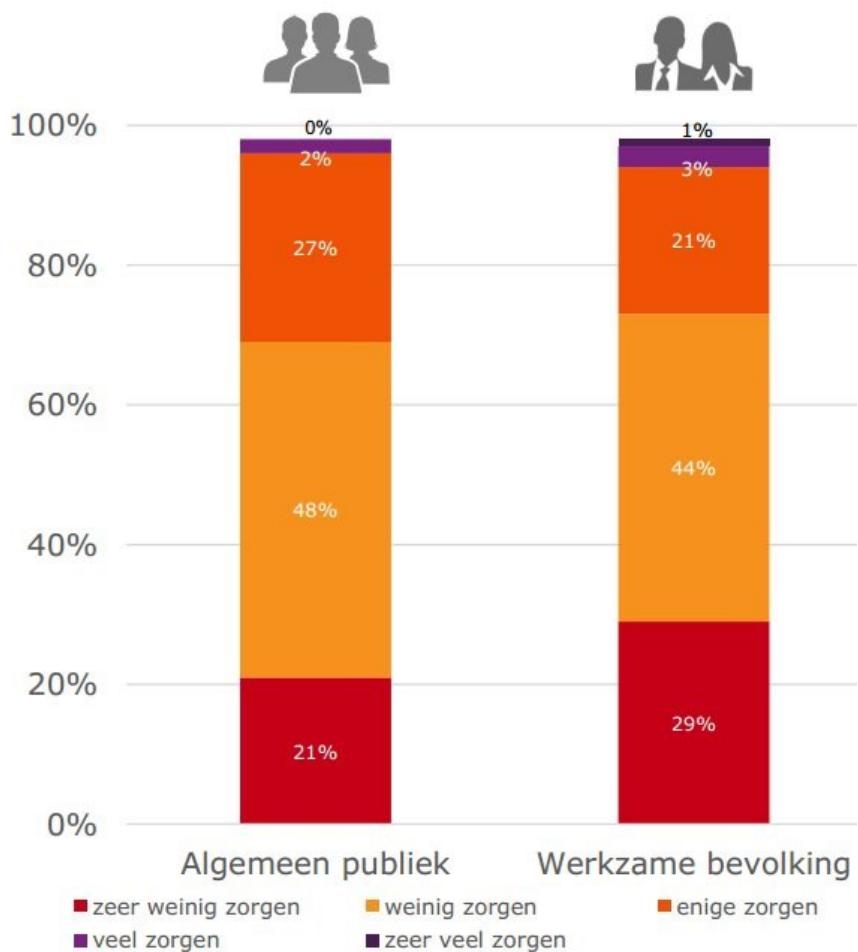


Fig 24 TNS 2016, p21. General concern about cyber security¹⁸⁶

As the figure below shows, the general Dutch public estimates the chance of being a victim of cyber security attacks, like malware or ransomware, as "very low". The figure also shows

¹⁸¹ CBS, 2016

¹⁸² CBS, 2015

¹⁸³ TNS, 2016, p21

¹⁸⁴ Randsdorp, Y; Zondervan, I., 2012 p 14

¹⁸⁵ Alert Online <https://www.alertonline.nl/>

¹⁸⁶ TNS, 2016, p21

that the actual victimisation on malware is significant. About 40% of the respondents has experienced some form of malware victimisation.

When we look at the chapter about the technical attack vectors and take the attitude of the car manufacturers into consideration, we see that they teach the car user that it is "ok" to update the car software / firmware via an USB stick.¹⁸⁷ This introduces an easy way for attackers to spread malware and ransomware into the connected car. It is also the opposite advice of the government in the Alert Online campaign.¹⁸⁸ Looking at the malware & ransomware threat we see the following picture.

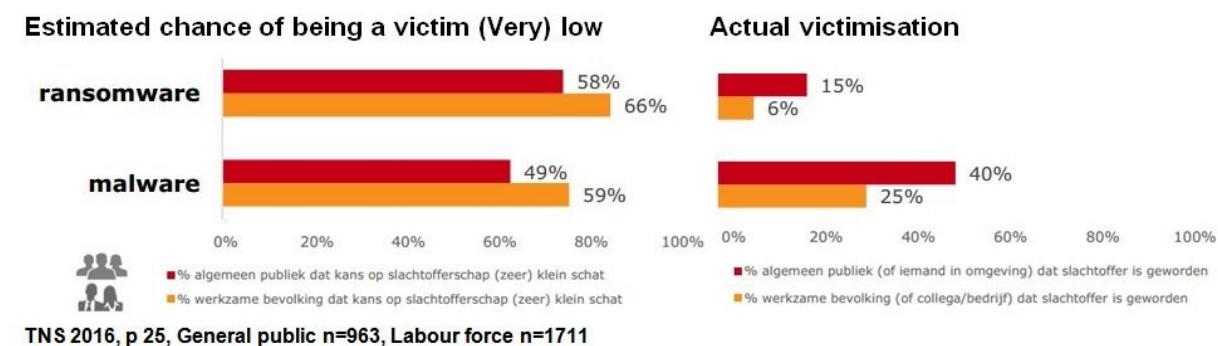


Fig 25 Overview of "Estimated chance of being a victim – (very) low" and actual victimisation.¹⁸⁹

Looking at these facts, we can conclude that people estimate the chance of being a victim is very low and that in reality this chance is higher. When we combine this with the fact that car manufacturers "teach" customers that it is ok to put an USB stick in the car to update or patch the software, it seems a matter of time before we will see "live" connected car malware. Car manufacturers should make an uniform policy to patch the connected car software in a quick and secure way. The car users should be aware and informed not patch his own car via an uncontrolled USB device. These two requirements are input for the roadmap.

3.2.6.1 Car users concerns

Prior research by the ANWB in the Netherlands in 2015¹⁹⁰ shows that consumers have several concerns on the use of connected cars. This research indicated that there were privacy concerns related to the commercial use of the collected car data (88%). A second indicated concern was related to the possibility that the car software could be hacked (84%). The absence of protective legislation was the third concern people indicated (94%). The respondents in this research had a low security awareness related to the connected car. About 44% of the respondents did know that a connected car is able to send and receive data, but only 24% were aware that there might be security risks involved.

In essence consumers want to be physical safe in a connected car. Consumer trust is at stake when system security can be compromised and threaten the physical safety of the car user. Consumer trust is the key element in the development and introduction of connected

¹⁸⁷ Fiat Chrysler Automobiles (FCA). The update site for the FCA Uconnect service is <http://www.driveconnect.com/software-update/>. The end user can download new software on an USB device and update the firmware of the car. The access to the software download is based on the VIN number of the car. The VIN number of each car is visible from the outside of the car. FCA indicates that it takes about 30 to 45 minutes to update the car software.

¹⁸⁸ Randsdorp, Y; Zondervan, I., 2012 p 32

¹⁸⁹ TNS, 2016, p25

¹⁹⁰ ANWB, 2015

cars. A quote from Blobel & Spath fits nicely “Trust begins where certainty ends”¹⁹¹ Consumers don’t have any certainty on the security of connected cars. Consumers cannot check the security of a connected car. They have to rely on what the car manufacturers tell them. Consumers have to trust that the security of the connected car is fine and works as designed. Trust seems to be the key word.

Customers do not ask for cyber security of connected cars. This is seen as an argument that explains why there is little attention on car security by the car manufacturers. Car security is not a unique selling point of cars and the customer cannot check the level of security of the connected car. The available information is asymmetric. That means that some actors have more knowledge and insight than other actors. That leads to market disturbance. The customer lock-in plays also an important role. Manufacturers want a certain customer lock-in. This lock-in can be based on the technical aspects of a solution, service based or be based on loyalty programs. When the customer wants to stay with you, or the cost of leaving you is too high, the manufacturer can maximise its profit. This is also the case with connected cars. Each car brand has its own system that is not compatible with other car brands.

The survey outcome indicates that security awareness and informing the customer in an understandable way are important factors.¹⁹² As Downs showed with his “issue attention cycle”, it seems hard to get and maintain the attention of the consumer regarding a topic.¹⁹³ Just like the fact that “the hacker” does not exist, “the customer” or “the car user” does also not exist. In order to be able to inform the car user (customer) we must understand in what way we can reach the car user. The Mentality model of Motivaction can be of assistance here. This model consists of eight clusters of people in the Dutch society grouped according to their life situation. The clustering is based on the shared values of these people on factors like work, politics, ambition, leisure and consumption patterns. Each group will act different based on these values. Motivaction states that their research shows that these eight clusters form a stable, consistent social environment. In order to reach each cluster, the communication and information must be addressed in a specific way. The way the communication is shaped determines if the information will reach the targeted people.

¹⁹¹ Blobel, F., Spath, P., 2005 p 538

¹⁹² See survey question 1.1 jo 1.7 jo 1.10 and 3.3 jo 3.9

¹⁹³ Downs, A., 1972

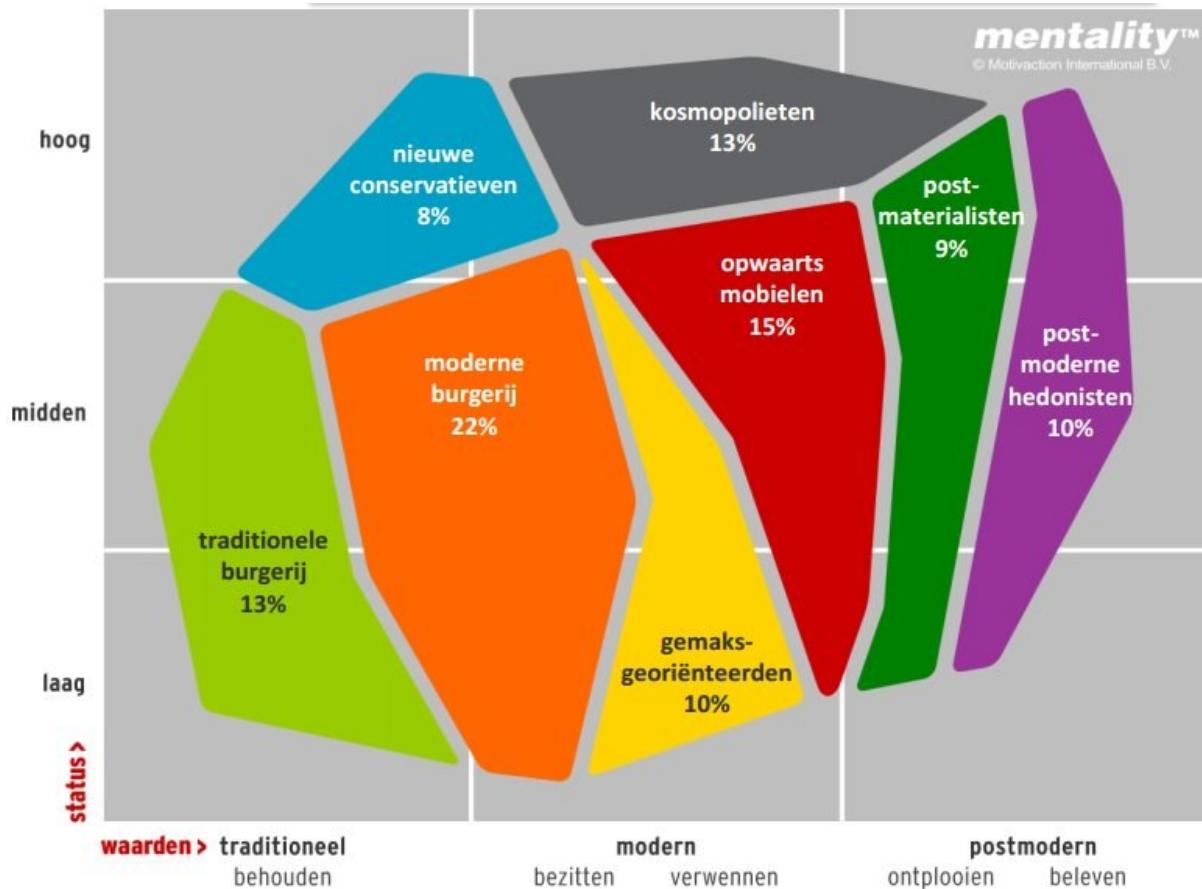


Fig 26 Mentality model shows the 8 social environment milieus in the Netherlands 2016 ¹⁹⁴

The model above shows eight clusters. The first cluster shows the “Traditionals” (13% of the Dutch population). The second cluster is the “Modern mainstream” (22%). The “Convenience oriented” people are the third cluster (10%). The “Social climbers” (15%) are indicated in red in the figure above. The “Post materialists” (9%) are the fifth cluster of people. The cluster on the right side of the picture show the “Post-modern hedonists” (10%). In the left hand corner the seventh cluster is depicted with the “New conservatives” (8%). The last category are the “Cosmopolitans” (13%). There is a role for the government, car manufacturers and branch organisations in initiating an annual event, like the current Alert Online event,¹⁹⁵ in which the security aspects of our new connected society is be discussed. The current Alert Online campaign is too narrow focussed and does not reach all people in society. As the Mentality model above shows, each group must be addressed separately in their own language within their own communication channels. The current uniform communication does not reach each specific group as depicted by the Mentality model.¹⁹⁶ The automotive industry can and should play a role in informing the car users in our society how to behave regarding the security aspects of the connected car. This is a requirement for the roadmap.

Because the users are not an structured entity that can participate and deliver content into the security discussion, we address these requirements to other identified actors.

¹⁹⁴ Motivaction, 2016 The Mentality model is published with permission of Motivaction, K. Slootman, 2016-09-28. Model is based on the annual representative research by Motivaction on 13 mln Dutch citizens between 15 and 80 Year. Motivaction indicated that this model can be used for purposes within the automotive industry.

¹⁹⁵ Alert Online, <https://www.alertonline.nl/>

¹⁹⁶ Spangenberg, F., 2016

The roadmap requirements for the car Users / consumers we derive from this analysis are:

U1	Ask questions about car security to your connected car dealer. Example: Can you show to me how cyber secure this car is compared to other connected car brands? How do I obtain security patches for my connected car? How long do I get security patches and firmware updates for my connected car? Action by branch org, government, car manufacturer
U2	Ask branch organisations to investigate, compare and publish the results of cyber security penetration tests on different types of connected cars.
U3	Ask questions about car security to your representative in parliament. Example: What kind of protective legislation (e.g. liability and security) is there in place that protects me in my connected car? What does the government do to ensure that my connected car is and stays secure? What security requirements did the government impose on the car manufacturers to ensure that the connected car is cyber secure? Action of government to provide adequate answers and actions.
U4	Ask questions about car security to your insurance company Example: how many times is this type of car stolen or had security breaches? Can you publish the annual statistics on connected car brands on how many security hacks / breaches there were? Action of insurance companies to provide adequate answers and actions.
U5	Ask your insurance company to deliver what information / collected data is logged and stored about the user behaviour when using the car.
U6	Car manufacturers should make an uniform policy to patch the connected car software in a quick and secure way.
U7	The car users should be aware and informed not patch his own car via an uncontrolled USB device. Action by car manufacturers, government and branch organisations.
U8	Inform each of the 8 Mentality groups in an annual event about their expected behaviour regarding cyber security aspects of the connected car. Each group must be addressed separately in their own language within their own communication channels. Action by government, car manufacturers and branch organisations.

Table 10 Requirements Users

Summary and short conclusions

Based on literature and interviews, several factors are identified that influence the automotive actors on the topic of the cyber security of consumer used connected cars. The combination and the weight of these factors might vary for each actor.

The most important factor is the business case. Other identified factors include the fact that insurance companies and customers don't ask for security, they assume security is there.

The fact that other car manufacturers don't have an improved level of security as well, seems a reason for some actors not to act because it affects their business case. The fact that there is no legislation and are no agreed standards, does not help to improve the car security. Lack of knowledge, awareness and media attention are the last factors that play a role in the economic considerations of the automotive actors that impact car security.

4 Multi actor roadmap to improve connected car security

In order to improve the security of connected cars we have to find common ground. The common ground on which the actors agree,¹⁹⁷ is the introduction of the autonomous car to be used by regular consumers in our society. In order to introduce the autonomous car consumers must have faith that the autonomous car is safe and cyber secure. In order to maintain consumer trust, consumer concerns must be addressed by the automotive industry.

Based on the gathered requirements we constructed a roadmap which shows which actor can initiate which actions in order to make connected cars more cyber secure. The car manufacturers should take the first step in this,¹⁹⁸ because they control the entire production chain of a connected car. Not all identified requirements lead up to defined projects in our roadmap. We can demand for example, that each sensor must have its own wiring to the main computer, but that is just not feasible. The weight of the cables would add about 100 kilo to the overall weight of the car.¹⁹⁹ The CAN bus was invented to solve this problem. That extra weight has a negative effect on the fuel consumption of the car, tax and environmental effects. Some requirements are known to be too expensive and have too much negative side effects to implement. The roadmaps in this chapter are based on our ICT experience and the detailed planning might vary from organisation to organisation. The timelines might vary due to the ICT complexity, business case, law & regulations, prioritisation by management, organisation culture, knowledge of the people that have to execute the project and the willingness to cooperate within the organisation.

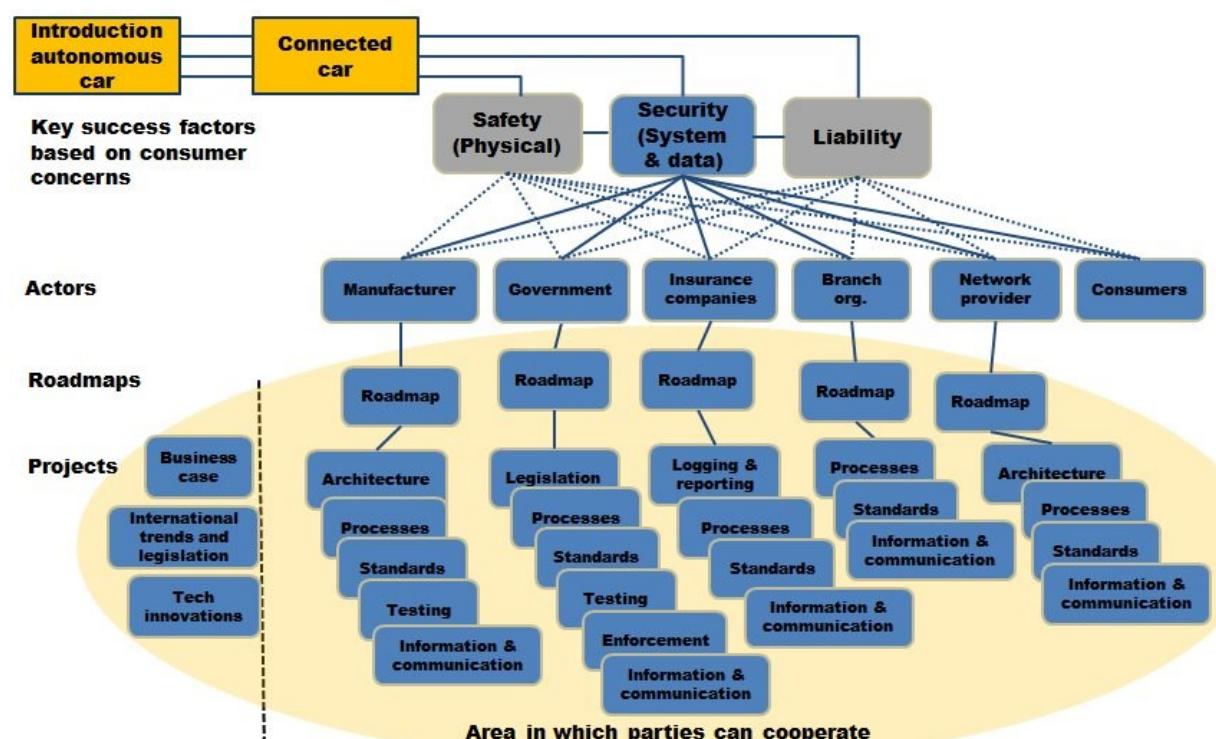


Fig 27. Multi actor diagram indicating the actors, their roadmaps in relation to the improved security of the consumer used connected cars

The diagram above shows the actors in the automotive industry. Each actor has its own roadmap. As depicted, each actor has interdependencies with other actors. It is possible that

¹⁹⁷ As indicated in the interviews

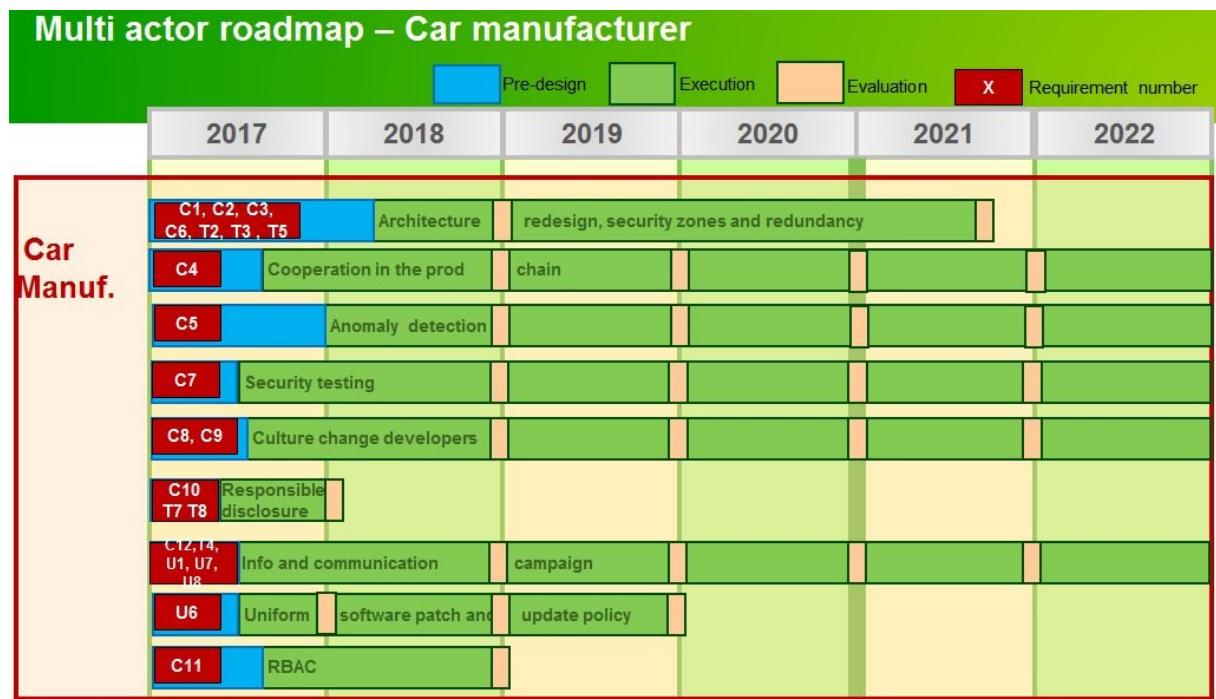
¹⁹⁸ See survey question 1.4

¹⁹⁹ Wijk van, M., 2016.

actors cooperate in their effort to execute the roadmaps in order to improve the security of the connected car.

4.1 Car manufacturers

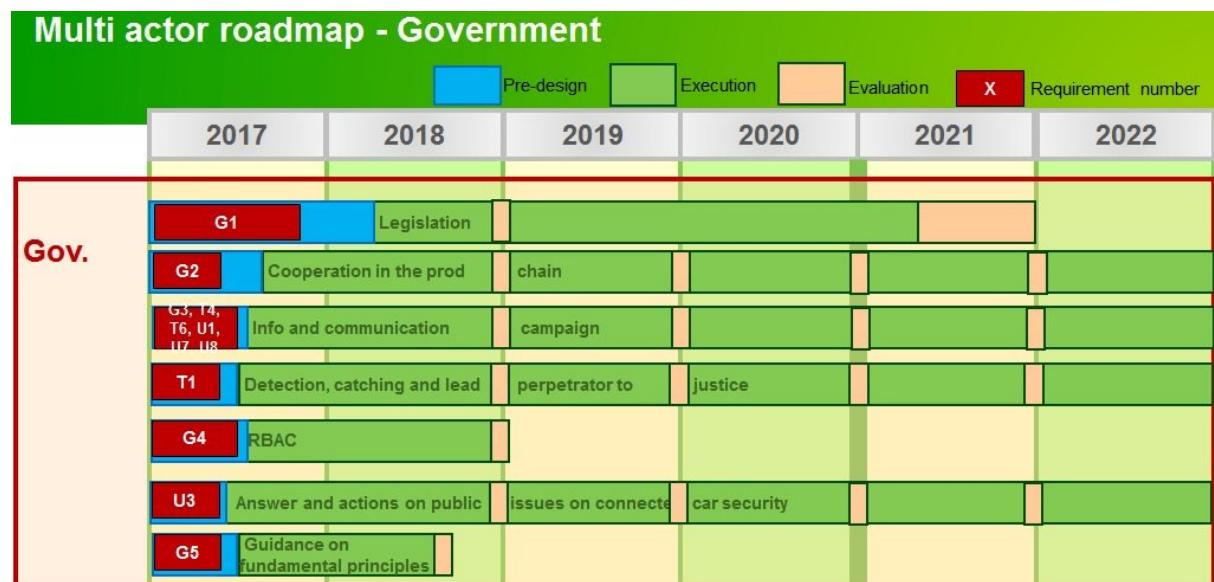
The roadmap for the car manufacturers contains “quick wins” that are easy to implement. The fundamental security adjustments are also indicated. It will take longer to solve these.



A quick win is the implementation of a responsible disclosure policy and the necessary follow up on the ethical hacker issues that are called in. The roll out of a uniform software patching and update policy might take longer due to the complexity in the production chain and the organisational implications. The architectural changes within the connected car will take time due to the changes in production chain and the agreements and contracts that have to be negotiated with the suppliers. Cyber security testing of connected cars is new to the car manufacturers. Implementing a good testing procedure with the right people takes time. All activities have to be evaluated. The product or process has to be adjusted based on the evaluation outcome. This is a continuous process.

4.2 Government

The government roadmap shows several actions the government take to improve the security of the connected car. Besides the obvious legislation, the government should answer fundamental questions to set clear boundaries for the automotive branch. The model by Brown²⁰⁰ can be used to “motivate” the automotive industry in an effective way.



Country specific legislation is needed to protect the car user as well as the car manufacturer. For the Dutch situation, legislation is needed that fits within the EU legal framework. This is a necessary, but slow and time consuming process. It is important that the government answers the fundamental questions (eg. car data ownership & how long should the connected car software be patched and updated) to give the automotive industry the boundaries needed to proceed to improve the security of the connected car. A continuous process that can be initiated by the government, in cooperation with the automotive industry, insurance companies and branch organisations, is informing the general public on cyber security issues of the connected car. Another roadmap item is to catch and prosecute hackers and those actors within the automotive industry that do not comply to the implemented legislation.

²⁰⁰ Brown, R., 2013

4.3 Insurance companies

The roadmap for the insurance companies shows the actions the insurance companies can take to improve the cyber security of the connected car.

		Pre-design	Execution	Evaluation	X	Requirement number	
		2017	2018	2019	2020	2021	2022
Ins.	I1, I9	Logging	all security	related incidents			
	I2	Trend analysis & reporting					
	I3, I8	Define security and comm	requirements for	automotive	industry		
	I4, I5	Communication and storage	encryption				
	I6, T4	Info and communication	campaign				
	I7	RBAC					
	U4, U5	Answer and actions on public	issues on connect	car security			

The car insurance companies should start to log and document in a structured way, all cyber related security issues of connected cars. This generates the needed historical data that can be used for trend analysis. This data can also be used to weigh the cyber security risks of the connected car. Based on this data the insurance companies can demand additional security requirements for certain brands of connected cars.

4.4 Branch organisations

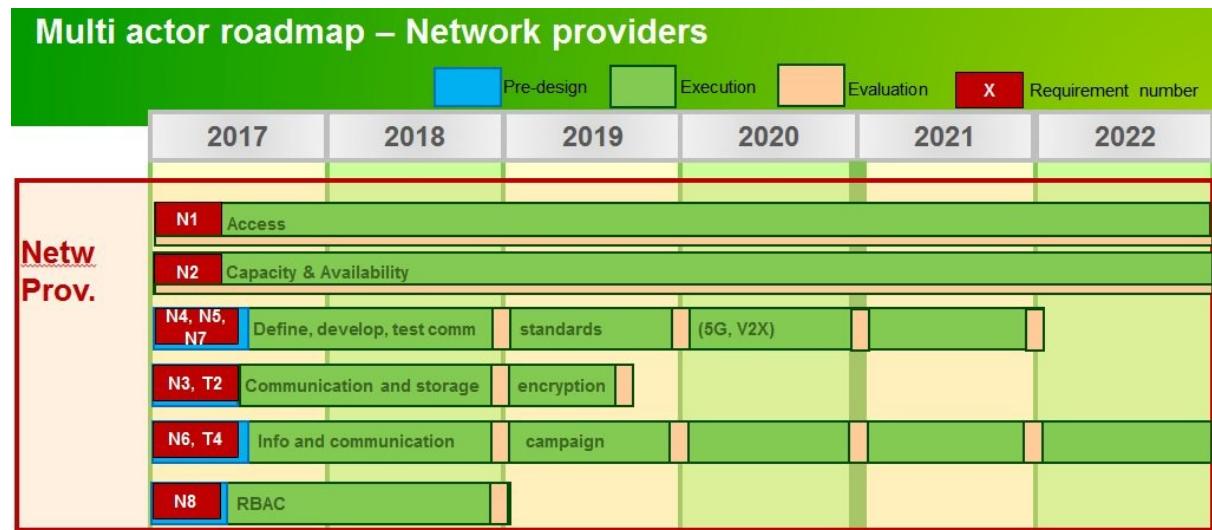
The roadmap for the branch organisations shows the steps they can take to improve the security of the connected car.

		Pre-design	Execution	Evaluation	X	Requirement number	
		2017	2018	2019	2020	2021	2022
Branch Org.	B2	Communication and storage	encryption				
	B1, B3, T4, U1, U7, U8	Info and communication	campaign				
	B4	RBAC					
	U2	Investigate	compare, publish	results pen tests			
	B5	European Auto ISAC					
	B6, T8	Annual hacking challenge					

Branch organisations should inform their customers on the cyber security issues of the connected car. They can also initiate an annual car hacking challenge. The automotive industry can benefit from the outcome of the results. An important activity of the branch organisation is to initiate and erect an European auto ISAC to share security information.

4.5 Network provider

The network providers are a prerequisite for a successful implementation of the autonomous car. The roadmap for the network provider shows the necessary steps to take in order to fulfil the expected timeline of the automotive branch. The network provider should incorporate the necessary security requirements into their network solution. That means that encryption must be used and that the new technical developments for V2X communication incorporates the latest security insights.



4.6 Car users

The car user / consumer is not an organised entity. That means that the requirements for the multi actor roadmap concerning the car users, are addressed to the other actors in the automotive industry.

5 Reflection

This chapter consists of two paragraphs. In the first paragraph we look back at the research. In this paragraph we also discuss the issues of reliability and validity of this research. In the second paragraph we look with a helicopter view at the “bigger picture” in which this research fits. We indicate trends and predict possible misuse and abuse cases.

5.1 Looking back

During this research some interesting situations occurred. The first thing we noticed is that after the interview was finished, the interviewed persons asked if it was possible to obtain the survey questionnaire. The reason behind this question, was the fact that the survey contained a handy format for internal discussions in the organisation. A second observation is the fact that the automotive industry is divided into groups that do not cooperate that well. The separation of the parties that consisted of SIMS are an example of this. The communication and the message in the media is not the communication you hear when you talk to people. People in the automotive industry do want to work together to solve issues concerning mutual agreed standards and are open minded about security improvements. The problem is that a lot of actors do not know where to start. They disagree on the underlying principles like “who owns the collected car data” and are not able to solve this puzzle among themselves. This study can be of help in breaking the current deadlocks that exist in improving the cyber security of connected cars.

There are also some concerns that have to be addressed in this research. The first concern involves the credibility of the gathered data. The credibility of the research outcome is solved by checking the outcome of the findings in three different ways. The first step is to match the findings on existing literature. The second step is to verify the outcome with interview data. We interviewed 13 different actors within the Dutch automotive industry. This wide variety of interviews ensured different viewpoints on the research topic. The problem with this is that it might be possible that we did not discover the relevant actors and thus did not gather all the different relevant viewpoints on the subject of cyber security of contacted cars. On the other hand, how many interviews is enough to obtain all the different viewpoints? Our criterion of “enough interviews have been conducted” was the fact that people started to repeat each other and started to refer to each other. The third step is to match the outcome of the interviews with the outcome of the survey. Because we started with the available literature and in a next step checked these results in expert interviews and the survey, the credibility issue seems to be addressed.

The next concern is to generate enough survey input to get a reliable survey result. Our goal was to obtain at least 50 completed surveys of 50 individual respondents. We need this to generate an outcome that is significant enough to draw conclusions based on the gathered data. The first part of the survey had 90 respondents, the second survey part had 86 respondents and the third part of the survey had 84 respondents. Overall, 84 individual respondents filled out and submitted the full survey. This is enough to use the gathered survey data.

A third concern is the transferability of the findings into a broader perspective. Can we generalise the Dutch findings into an European or worldwide perspective? Because the Dutch automotive industry has almost no car factories on its soil, we used the input of the car manufacturers that sell cars on the Dutch market. We consulted these worldwide operating

car manufacturers and the outcome of the interview and survey findings is in line with the literature findings, we think the outcome can be generalised into a broader perspective.

Although the survey was anonymous, almost all respondents were under the impression that the researcher could see what their personal response on the survey was. This might have triggered some “social acceptable” behaviour responses. The outcome of the survey seems to be reliable because of the large number of respondents and the fact that the items are in line with the outcome of the interviews and literature.

The survey was initially tested in the TNO interview. Based on this, the survey was reduced to 30 questions. The effect was that some questions were dropped and altered. The items that are dropped are indicated in the future research paragraph. Before the survey was published on the internet, the survey was fine-tuned based on peer review input. After publication the survey was not altered because this causes unwanted effects in the survey results.

The presented roadmap requirements are based on literature, interviews and the survey. The validation of the roadmap requirements is challenging because the roadmap timelines and the requirements might vary in each organisation. The presented roadmap timelines might vary due to the ICT complexity, business case, law & regulations, prioritisation by management, organisation culture, knowledge of the people that have to execute the project and the willingness to cooperate within the organisation.

Respondent percentage	Survey question	Description
67	1.3	Car manufacturers should improve car security.
46	1.4	Car manufacturers should take the lead to improve car security.
44	1.6	The government should set the standards for cyber security testing of connected cars.
98	1.5	Connected cars should be tested on the cyber security status....
42	2.1	including vulnerabilities by an independent organisation.....
78	2.2	and the car manufacturers must pay for these tests.
93	1.7	The security test results should be made public.....
73	1.8	after a waiting period.....
42	1.10	on a website of an independent organisation.
55	3.3	The car user has a right to know all cyber security issues of the connected car.
72	2.4	Wireless is the most likely attack vector on a connected car.
83	2.10	Encryption of the CAN bus data contributes to the security of the connected car.
47	3.4	The car manufacturers must support security patches for the connected car as long as there is any connected car left on the road of that brand.
82	3.6	The respondents expect security issues with the introduction of the mandatory E call (Emergency call) in connected cars.
88	3.7	The respondents expect security issues with the introduction of the optional B call (Break down call) in connected cars.
83	3.8	The respondents expect security issues with the introduction of the optional S call (Service call) in connected cars.
54	3.9	The car user must be able to switch the optional B call (Break down call) and S call (Service call) on or off whenever he/she wants.

Table 11 Summary of the survey results

The summary results of the survey are depicted in the table above. Many respondents agree on matters like security testing, publication of test results etc. The respondents are clear in their judgement on these matters. What is interesting, is that when we ask these respondents detailed information on how to solve these issues, no clear answer is given and the answers vary. That is also the reason why not all survey results are depicted in this table. The answers on the detailed solutions vary too much. For detailed survey information see appendix 2.

5.2 Looking forward

In this second paragraph of this chapter, we look forward into the future. We look with a helicopter view at the “bigger picture” and extrapolate our findings into possible future events. We indicate trends and predict possible misuse and abuse cases.

5.2.1 Car manufacturers

Car manufacturers have the key to improve the security of connected cars. As discussed the car manufacturers are a bit reluctant to take action, because of economic factors. Literature, interviews and the survey seem to confirm this. The trend within the automotive industry is that the connected car will become reality and that the autonomous car is blinking its headlights on the horizon. The automotive industry should realise that the only way they can execute the ambitious autonomous car program is, when the end users have faith in the solutions the car manufacturers present. When the end users don't trust the connected car, the autonomous car will never appear on the road. It is in the best interest of the automotive industry to address the consumer concerns in order to be able to take the next step towards the autonomous car. The outcome of the survey indicates that the car manufacturers should take the first step to improve the cyber security of the connected car.

So what are the possible misuse cases we can expect the upcoming years? Well, the trend is to automate the connected car into the autonomous car. The current model of people driving a car themselves will slowly disappear. The first prediction we feel confident to make, is that connected cars can and will be hacked. When we look at the ICT sector that is struggling for decades to protect its ICT systems, we can conclude that protection alone is not enough. Protection, detection, redundancy and a defence in depth response is necessary to obtain some form of security. The end user expects a safe and secure car. The automotive industry must find a way to break the criminal business case. This means a redesign of the current ICT architecture of the connected car. That also means that the current first generation of connected cars is not cyber secure and probably never will be.

The second outlook we can predict is that new forms of criminal cases will appear that perfectly fit the new technological possibilities of the connected car. A criminal case we can think of is for example the introduction of ransomware for the autonomous cars. You can pay a small fee if you want to use your car. Or criminals might use ransomware to lock cars of a certain brand. The next step is to persuade the car manufacturer to pay and release their cars. Insurance fraud and root cause analysis in law suits will generate new jobs. We can think of forensic ICT experts that are specialised in analysing car software. These experts will play an important role in law suits, determining the root cause of car crashes. Forensic experts will investigate the car crash to see if the crash was an accident, insurance fraud, design flaw or an homicide executed by hacking the car. Was the car software patched timely and properly or is the car manufacturer liable for the damage?

The third prediction is that the automotive industry will fight a fierce battle via the media, lobbyists and other means, to limit the number of years the car manufacturers have to supply firmware and security updates of connected cars. The government should set the boundaries for the automotive branch by answering fundamental questions like: How many years should the car manufacturers support and update the car firmware? Who owns the collected car data?

There will be ethical discussions on the autonomous car decision model. People expect to be safe and secure in their car, but what if the autonomous car decision model decides that the proper action is to crash the car containing one person in order to save the lives of the five people in front of the car?

5.2.2 Government

The Dutch government can play a significant role in improving the security of the connected car. The Dutch RDW is capable to test and set requirements that connected cars must apply to. These requirements can be captured in standards and legislation. The second action the government can take is to create legislation to protect the end user, but also the car manufacturer. This legislation must fit within the EU regulation boundaries. The government can also facilitate the creation of car security standards, the automotive industry can use. The government should answer fundamental questions the automotive industry is unable to answer due to their business model. Is the collected car data owned by the car owner (consumer) or by the car manufacturer? A second question the government has to answer is, how long must the car manufacturer support security patches for the connected car.²⁰¹ The answer to these two questions have a huge business impact on the automotive industry.

An example of the inability to act timely and properly on car security aspects, this is the European roadmap to introduce the connected and the autonomous car. An international accepted connected car security framework does not exist and the participants are struggling who should take the lead. The self-regulation by the automotive industry can only work when the government is answering the fundamental questions and sets the boundaries for the automotive industry.

In our Dutch society the checks and balances of our political system seems sound. In political environments with a different balance the government might take a different approach that might lead to, from our point of view, unwanted privacy and security scenario's. An example of such a case could be the adaption of the connected car firmware in such a way that the government can track the movements of its citizens. Or the introduction of specific car software for citizens that live in a specific geographical area. Another scenario might be that the government locks your car when you do not pay your tax. These scenario's might seems strange to us, but a similar scenario on computer software is already used in some countries.²⁰²

The government must implement car security legislation including heavy fines to those parties that do not comply. An example of this model is the data breach legislation²⁰³ in the Netherlands. Companies took it seriously when non-compliance was penalised with heavy fines.

²⁰¹ See survey question 3.4

²⁰² Reuters, 2015

²⁰³ Laube, S. et al, 2015

Another action the government can perform is the pursuit of criminals hacking into the connected car. This should be prosecuted to prevent an atmosphere within society that it is allowed to hack connected cars. The criminal business case of car hacking must be studied and broken in order to safeguard the future of the autonomous car.

5.2.3 Insurance companies

The car insurance companies are not yet up to speed when it comes to anticipating on the introduction of the autonomous car. They do not log security related car incidents and they do not, visibly, develop new business models. Insurance and branch organisations are currently double hearted in the security and privacy discussion. On the one hand they stress the need for security and privacy. They try to protect the privacy of their clients by handing out ID covers etc. On the other hand the insurance companies introduce the insurance dongle to profile the road behaviour of the car user. This is a security and a privacy risk for the end user of the car. When the autonomous car is introduced and accepted by society, the insurance policies have to change. There will be significant less damage claims caused by driver related accidents. A significant number of insurance claims will be dealt with by the car manufacturers of autonomous cars. The regular car insurance prices will drop.

Questions that have to be answered are: What software is used in the car, how and when is this software patched? Is there, for example, a foreign vendor from the USA with open source - or proprietary software? What is the life expectancy of the hardware and the software that is used? Where and how is the collected data stored? How is the data protected during the collection phase and the storage phase. Does the organisation use RBAC? How long is the data stored? Can the car user request the removal of the data? Is the collected data transferred to the new insurance company when I switch my insurance policy to another insurance company? What are the metrics on which my insurance "profile" is built? In theory it is possible to issue a speeding ticket on the collected data: You know the road (GPS location record), you have the distance, you have a time stamp and you know the speed of the car. Government and insurance companies can work together in this and both benefit. The current car data sharing system is voluntary based. The system can be made mandatory by a future government. With the introduction of new technologies like this a lot of promises are made that are later revoked. How can we prevent the slippery slope of broken promises on data collection, profiling, data sharing and government misuse?

5.2.4 Branch organisations

When we look at the branch organisations we see a shattered picture. They struggle with the privacy and security question in relation to the connected car. It is due to their organisation, business model and the wish to generate profit. Other initiatives like SIMS and Connekt seem to work fine and we see that these kind of initiatives deliver usable standards. Progress is made to the agreed standards when parties agree upon the required outcome. When parties do not agree upon the underlying principles and the outcome affects the business case of the parties involved, this kind of self-regulation does not work. The termination of the SIMS initiative in 2016 is an example of that. The SIMS initiative ended because of the fact that the parties involved did not agree on the fundamental view of data ownership. In those situations the government has to step in. As indicated in the paragraph above, the government should take decisive actions and dictate the boundaries the automotive industry has to follow. The government has to answer fundamental questions in order to give guidance to the automotive industry to be able to further self-regulate.

European and world wide initiatives seem to focus on the introduction of the connected and autonomous car. It is unfortunate to conclude that the car data collection and the car ICT security are not in this picture. That means that we, as a society, have to repair the car security omission in the future at a much higher cost. A start would be to erect an, European, auto ISAC where automotive parties can share their security information in order to improve the current car designs.

5.2.5 Network provider

The automotive branch focuses on the introduction of new features for the end user in the connected car. The availability of the network is a precondition for a smooth operation of these features. The network providers and vendors of hard- and software are working hard to keep up with this increasing demand for speed, bandwidth, reliability and availability. The roadmaps of these vendors stretch into 2022 and beyond. We mention these roadmaps in our presentation, but due to confidentiality matters we cannot mention them in this research.

5.2.6 Car users

The car users are often a “forgotten group” in car hacking literature. Research tend to focus on the technical aspects or on the profiling features of the attacker. Literature shows that the car user has little security awareness. The car user feels safe and secure in his car. When the car user subject is discussed, the advice is often to “do an awareness campaign” and we’re done. We think it’s more complicated than that. Each user group must be specifically addressed in order to reach them. We think that a general awareness campaign will have little effect. We put the view and interests of the car user into the roadmap of the automotive actors.

The essence is that car users want and expect to be physical safe in a connected car. Consumer trust is at stake when system security can be compromised and threaten the physical safety of the car user. Consumer trust is the key element in the development and introduction of autonomous cars. Consumers are not aware that their connected car contains fundamental security flaws that might endanger their physical safety. The automotive industry should take this element seriously and act accordingly.

6 Conclusion

6.1 Conclusion

In order to improve the cyber security of connected cars we have to find common ground. The common ground on which the actors agree, is the introduction of the autonomous car to be used by regular consumers in our society. In order to introduce the autonomous car consumers must have faith that the autonomous car is safe and cyber secure. In order to maintain consumer trust, consumer concerns about safety, liability and security & privacy, must be addressed by the automotive industry.

In order to improve the cyber security of the connected car we constructed a multi actor roadmap. We derived the requirements for this roadmap from the defined sub questions.

In the first question was about the technical possibilities to hack and break the security of the connected car. We showed that there are a lot of possible technical attack vectors in which the security of a connected car can be breached. These attack vectors can be clustered into four main categories, direct physical, indirect physical, wireless and sensors.

The second question was about defining and categorising the possible attackers of a connected car and their motives to hack cars. This gave us insight into the criminal motivation and understanding the criminal business case that has to be broken in order to make connected cars more secure.

In the next step, in which we answered the third question, we identified the, economic, factors and incentives of the actors in the automotive industry when they are confronted with security issues of connected cars. This gave us the next set of requirements and building blocks to construct the multi actor roadmap to improve car security.

Although the gathered elements are reusable in any country of the world, we constructed a roadmap for the Netherlands in order to show that this approach works. Countries around the world struggle to implement adequate legislation that deals with the issues of the connected - and autonomous car.

There are several studies on the technical aspects of the security of connected cars. This study combines the existing research on the technical security aspects of connected cars with the actor and behaviour aspects in the automotive industry. We added a new factor into the SABSA framework. We added the factor "relevance". By doing this we solved the issue in the SABSA framework that results in a distorted picture of the possible attackers. The relevance factor solves the issue that some things are theoretical possible, but lacks relevance in real life. The requirements that can stop attackers from hacking connected cars are put into the roadmap.

Because of our approach to see a connected car as a computer on wheels, we were able to see, identify and combine the technical vulnerabilities, inhibitor factors of the attackers and the economic incentives of the actors in the automotive industry. Current literature only looks at the technical vulnerabilities, or presents an analysis of the attackers. This research combines both elements and adds an extra layer of economic factors. We examined the economic incentives underneath the visible actions of the actors in the automotive industry. From these elements we could determine the requirements that we used in the overall roadmap which shows which actor can initiate which actions in what timeframe.

The last element we added is the end user factor. The end user is in our point of view an important factor that should be incorporated and involved in the discussion about connected car security. We added relevant requirements into the roadmap in order to make sure the end user is involved.

When we look beyond our research, we see that five important elements must be solved in order to generate a more cyber secure car. The first element is that the government must answer the question of car data ownership and the question on how long cars must be patched by the car manufacturers. The second element is the implementation by the branch organisations of an auto ISAC in Europe. The fundamental redesign of the ICT architecture of the connected car by the car manufacturers is the third element. The fourth element is the logging of car related cyber security incidents by the insurance companies. Network providers must implement a secure 5G standard the automotive industry can use to communicate to and from the connected car. The last element is that car users must start asking questions about the cyber security of their car.

6.2 Future Research

Because the introduction of autonomous cars can have disruptive effects in society, additional research is needed. Future research is needed on the following topics that we excluded in this research.

We identified the, economic, factors that can contribute to improve the cyber security of connected cars. Which factors contributes most to the improvement of cyber security of connected cars? Other elements of research are the comparison between countries on car security, legislation, liability and the best way to inform the general public on security matters. What is the effect of the introduction of autonomous cars on the business model of car insurance companies? Autonomous cars prevent collisions a much as possible. What is the effect of that on the car insurance policies? Insurance companies will only encounter damage by vandalism, theft and events of mother nature. Driver errors, that seem to be the cause of many accidents, are ruled out.

Another interesting topic is examining the effect of the introduction of autonomous cars on bodyshops that repair cars. Less of these bodyshops are needed when autonomous cars automatically avoid bumping into each other. What will the new role of the car dealer become? Will car dealers become the new ICT patch stations for your car to update your firmware and anti-virus definitions?

Another research question that can be examined is the question whether we need a drivers licence in the future. What is the effect of the introduction of autonomous cars on institutions like CBR²⁰⁴ that takes driver exams and hands out driver licences. Do we need a driver licence when the autonomous car takes all the decisions?

What will be the effect of the autonomous car on the taxi branch? Do you need a human driven taxi in the future, when autonomous robot cars can drive you anywhere?

In line with this, the question becomes who is liable for the damage when your car crashes? What is the effect of the introduction of autonomous cars on the liability question. At what exact point, and under what conditions, is the driver no longer liable for the damage caused, because the car took all the decisions?

What safeguards can we construct to prevent misuse of the collected car data by the car manufacturers, government and insurance companies? How can we prevent the misuse of autonomous cars by terrorists that want to attack a city centre?

²⁰⁴ CBR, Centraal Bureau Rijvaardigheidsbewijzen, <https://www.cbr.nl/>

We have to come up with an answer on fundamental questions like: How long does the car manufacturer have to support, patch and update the software of a car? The answer to this question has huge implications on the security of the car ICT systems and thus to the physical safety of the car user. It has also an impact on the business case of the car manufacturer.

Bibliography

- ADAC, A. D. A.-C. (2015). BMW Connected Drive security loopholes. *ADAC*, (January), 1–3. Retrieved from <http://www.fiaregion1.com/download/news/bmw-security-loopholes.pdf>
- Anderson, M. (2014). Black Hat 2014 : Hacking the Smart Car. *IEEE Spectrum*. Retrieved from <http://spectrum.ieee.org/cars-that-think/transportation/systems/black-hat-2014-hacking-the-smartcar>
- Anonymous. (2015). Bugcrowd | Your Elastic Security Team, better security testing through bug bounties and managed security programs. Retrieved May 15, 2016, from <https://bugcrowd.com/tesla>
- Anonymous. (2016). Anti-Submarine Warfare (ASW) Continuous Trail Unmanned Vessel (ACTUV) Sea Hunter. Retrieved May 12, 2016, from <http://www.navaldrones.com/ACTUV.html>
- ANWB. (2015). De “connected” voertuig en uw data. *ANWB.nl*, 1. Retrieved from <http://www.anwb.nl/bestanden/content/assets/anwb/pdf/auto/connected-car/my-car-my-data-connected-voertuig-en-uw-data.pdf>
- ANWB. (2016). Nieuwe autoverzekering bij schadevrij rijden tot 30% extra korting | ANWB. Retrieved from <http://www.anwb.nl/verzekeringen/autoverzekering/veilig-rijden>
- Blobel, F., & Spath, P. (2005). The Tale of Multilateral Trust and The European Law of Civil Procedure. *European Law Review*, 30(4), 528–547.
- BOVAG. (2016). Datahuwelijjk tussen BOVAG en RAI Vereniging voorbij. BOVAG. Retrieved from <http://leden.bovag.nl/Actueel/Nieuws/2016/Datahuwelijjk-tussen-Bovag-en-RAI-Vereniging-voorbij>
- Bresser, H.; Kamps, E. (2016). Bresser, H., Kamps, E., Bovag, Interview 2016-06-09. Bunnik.
- Brown, R. (2013). Regulating crime prevention design into customer products: Learning the lessons from electronic vehicle immobilisation. *Trends & Issues in Crime and Criminal Justice*, (453), 1–8. Retrieved from https://www.researchgate.net/profile/Brown_Rick/publication/277142920_Regulating_crime_prevention_design_into_consumer_products_Learning_the_lessons_from_electronic_vehicle_immobilisation/links/5563c12208ae6f4dcc98baa6.pdf
- Burns, A., McDermid, J., & Dobson, J. (1992). On the meaning of safety and security. *Computer Journal*, 35(1), 3–15. <http://doi.org/10.1093/comjnl/35.1.3>
- Cambridge University. (2016). autopilot Meaning in the Cambridge English Dictionary. Retrieved from <http://dictionary.cambridge.org/dictionary/english/autopilot>
- Canadian Automated Vehicles Centre of Excellence. (2015). *Preparing for Autonomous Vehicles in Canada*.
- CBS. (2015). CBS StatLine - Huishoudens in bezit van auto of motor; huishoudkenmerken. Retrieved from <http://statline.cbs.nl/Statweb/publication/?DM=SLNL&PA=81845ned&D1=1,3&D2=a&D3=0-2,13-31&D4=l&VW=T>
- CBS. (2016). CBS StatLine - Motorvoertuigenpark; inwoners, type, regio, 1 januari. Retrieved from <http://statline.cbs.nl/StatWeb/publication/?DM=SLNL&PA=7374hv&D1=2-11&D2=0&D3=a&HDR=T&STB=G2,G1&VW=T>
- Checkoway, S., Mccoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., ... Kohno, T. (2011). Comprehensive Experimental Analyses of Automotive Attack Surfaces. *System*, 6–6. Retrieved from http://www.usenix.org/events/security/tech/full_papers/Checkoway.pdf
- Chrysler, Illinois, U. D. C. for the southern district of. Class action Chrysler Group LLC Case No. 3:15-cv-855 (2015). Retrieved from https://regmedia.co.uk/2015/08/06/chrysler_complaint.pdf
- Cimpanu, C. (2015). BMW, Mercedes and Chrysler Cars Vulnerable to OwnStar Hacking Attacks. Retrieved from <http://news.softpedia.com/news/bmw-mercedes-and-chrysler-cars-vulnerable-to-ownstar-hacking-attacks-489319.shtml>
- Cimpanu, C. (2016). Zero-Days in BMW Web Portal Let Hackers Tamper with Customer Cars. Retrieved from <http://news.softpedia.com/news/zero-days-in-bmw-web-portal-let-hackers-tamper-with-customer-cars-506103.shtml>
- Connecting Mobility. (2016). Final report C-ITS Platform (EU). Retrieved from <http://ec.europa.eu/transport/themes/its/news/2016->
- Connekt. (2014). Connekt Security Expert Meeting, 2014, dec 18.
- Consumentenbond. (2016). Geldgids, nov 2016. *Consumentenbond Geldgids*, p 6 jo 20 – 23.
- Cornell, D. (2016) Car Hacking: Software In A Song Can Be Used To Control Modern Vehicles <http://www.inquisitr.com/2743398/car-hacking-software-in-a-song-can-be-used-to-control-modern-vehicles/>
- Deutsche Telekom. (2016). Deutsche Telekom: Connected cars meet next generation communications tech. Retrieved from <https://www.telekom.com/en/company/special--5g-haus/special--5g-haus/connected-cars-meet-next-generation-communications-tech-416198>

- Dimitrovski, T. et al. (2016). *TNO report Wi-Fi monitoring - Next Generation Hotspot Q3 2016*.
- Dokic, j; Muller, B; Meyer, G. (2015). European Roadmap Smart Systems for Automated Driving. *European Technology Platform on Smart Systems Integration*, 1–39.
- Doll, G. (2016). Doll, G. RDW. interview 2016-05-19. Groningen.
- Downs, A. (1972). Up and down with ecology -- the “issue-attention” cycle. *The Public Interest*, (28), 38–50. <http://doi.org/citeulike-article-id:8241790>
- Enev, M., Takakuwa, a, Koscher, K., & Kohno, T. (2016). Automobile Driver Fingerprinting. *Proceedings on Privacy Enhancing Technologies*, 2016(1), 34–50. <http://doi.org/10.1515/popets-2015-0029>
- FireEye. (2016). Connected cars: the open road for hackers, (June), 1–8. Retrieved from www.FireEye.com
- Fox-Brewster, T. (2015). Hacker Says Attacks On “Insecure” Progressive Insurance Dongle In 2 Million US Cars Could Spawn Road Carnage. Forbes. Retrieved from <http://www.forbes.com/sites/thomasbrewster/2015/01/15/researcher-says-progressive-insurance-dongle-totally-insecure/#229934ea7c9f>
- Gallagher, S. (2016). GM embraces white-hat hackers with public vulnerability disclosure program | Ars Technica. Retrieved May 15, 2016, from <http://arstechnica.com/security/2016/01/gm-embraces-white-hats-with-public-vulnerability-disclosure-program/>
- Geraets, N. (2016). Geraets, N., NXP, Interview 2016-07-21. Eindhoven.
- Geurts, P., Beveren van, J. (2016). Geurts, P., Beveren van, J., Achmea, Interview 2016-06-02 and 2016-06-12. Leusden.
- Gonder, J., Burton, E., & Murakami, E. (2015). Archiving Data from New Survey Technologies: Enabling Research with High-precision Data While Preserving Participant Privacy. *Transportation Research Procedia*, 11, 85–97. <http://doi.org/10.1016/j.trpro.2015.12.008>
- Gordon, L. A., & Loeb, M. P. (2002). The Economics Of Information Security Investment. *Transactions on Information and System Security*, 5(4), 438–457. <http://doi.org/10.1145/581271.581274>
- Greenberg, A. (2015a). After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix | WIRED. Retrieved from <https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/>
- Greenberg, A. (2015b). Hackers Remotely Kill a Jeep on the Highway—With Me in It | WIRED. Retrieved from <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>
- Gutierrez, M. (2014). The Insights into Car Hacking. Retrieved from [http://web.eng.fiu.edu/~aperezpo/DHS/Std_Research/Car Hacking - eel 6931 final.pdf](http://web.eng.fiu.edu/~aperezpo/DHS/Std_Research/Car%20Hacking%20-%20eel%206931%20final.pdf)
- Hall, G. (2016). Google Station aims to provide free Wi-Fi around the world. - Silicon Valley Business Journal. Retrieved from <http://www.bizjournals.com/sanjose/news/2016/09/27/google-launches-google-station-to-bring-free-wi.html>
- Heide, A., & Henning, K. (2006). *the “Cognitive Car” a Roadmap for Research Issues in the Automotive Sector. IFAC Proceedings Volumes* (Vol. 39). IFAC. <http://doi.org/10.3182/20060522-3-FR-2904.00008>
- Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research, 28(1), 75–105. <http://doi.org/10.2307/25148625>
- Hoop, de A. (2016). Hoop, de A. Stichting Verzekeringsbureau voertuigcriminaliteit, interview 2016-05-09. Apeldoorn.
- Hunt, T. (2016). Troy Hunt: Controlling vehicle features of Nissan LEAFs across the globe via vulnerable APIs. Retrieved from <https://www.troyhunt.com/controlling-vehicle-features-of-nissan/?m=1>
- Husted, N. et al. (2011). Smartphone Security Limitations : Conflicting Traditions, 1–8. Retrieved from <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.449.5918&rep=rep1&type=pdf>
- Hutchins, E. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains, (July 2005), 1–14.
- IHS Markit. (2014). Self-Driving Cars Moving into the Industry’s Driver’s Seat. *IHS Online Newsroom*, 1–2. Retrieved from <http://news.ihsmarkit.com/press-release/automotive/self-driving-cars-moving-industrys-drivers-seat>
- Jiang, T., Petrovic, S., & Husain, S. (2015). Self-Driving Cars - Disruptive or Incremental ? *Applied Innovation Review*, (1), 3–22. Retrieved from <http://cet.berkeley.edu/wp-content/uploads/Self-Driving-Cars.pdf>
- Juffermans, N. (2016). Juffermans, N., Connekt, Interview 2016-06-29. Delft.
- Kerkhof, van M. (2016). Kerkhof, van M. PON Automotive. Interview 2016-05-11. Leusden.
- Kim, P., Alex, C., & Leslie, T. J. (2014). Testing Mobile Applications for Vulnerabilities, 31–36. Retrieved from <http://www.comp.nus.edu.sg/~hugh/CS3235/PREVIOUSPROJECTS/CS3235-SemI-2014-15-Projects.pdf#page=35>

- Kleberger, P., Olovsson, T., & Jonsson, E. (2011). Security aspects of the in-vehicle network in the connected car. In *IEEE Intelligent Vehicles Symposium, Proceedings* (pp. 528–533). <http://doi.org/10.1109/IVS.2011.5940525>
- Kotter, J. (1996). Leading Change: Why Transformation Efforts Fail. *HarvardBusinessReview*, (March-April), 57–68. <http://doi.org/10.1109/EMR.2009.5235501>
- Kyriakidis, M., Happee, R., & De Winter, J. C. F. (2015). Public opinion on automated driving: Results of an international questionnaire among 5000 respondents. *Transportation Research Part F: Traffic Psychology and Behaviour*, 32, 127–140. <http://doi.org/10.1016/j.trf.2015.04.014>
- Laube, S., & Bohme, R. (2015). The Economics of Mandatory Security Breach Reporting to Authorities. *14th Annual Workshop on the Economics of Information Security (WEIS)*, 1–26.
- Lessig, L. (2006). CODE version 2.0. *CODE Version 2.0*, 1–424. Retrieved from <http://codev2.cc>
- LG; Volkswagen. (2016). LG and Volkswagen commit to jointly develop connected car platform | LG Newsroom. Retrieved from <http://www.lgnewsroom.com/2016/07/lg-and-volkswagen-commit-to-jointly-develop-connected-car-platform/>
- Li, J. (2016). CANSsee - An Automobile Intrusion Detection System, 1–64. Retrieved from <http://conference.hitb.org/hitbsecconf2016ams/materials/D2T1 - Jun Li - CANSsee - An Automobile Intrusion Detection System.pdf>
- Lodge, D. (2016). Hacking the Mitsubishi Outlander PHEV hybrid | Pen Test Partners. Retrieved from <https://www.pentestpartners.com/blog/hacking-the-mitsubishi-outlander-phev-hybrid-suv/>
- Luh, R. (2013). Six Ways to Kill by Hacking, 1–27. Retrieved from http://www.googlehupf.at/rluh/wp-content/uploads/ITSecX_6WaysToKill_EN.pdf
- Mahaffey, M. R. K. (2015). Def con 23 Security Conference. Las Vegas. Retrieved from https://youtu.be/KX_0c9R4Fnq
- Miller, C., & Valasek, C. (2014). A Survey of Remote Automotive Attack Surfaces. *Defcon 22*. Retrieved from <http://illmatics.com/remote attack surfaces.pdf>
- Motivaction. (2016). Mentality model | Motivaction International. Retrieved from <https://www.motivaction.nl/en/mentality/mentality-segmentation>
- Nighswander, T., Ledvina, B., Diamond, J., Brumley, R., & Brumley, D. (2012). GPS software attacks. *Proceedings of the 2012 ACM Conference on Computer and Communications Security - CCS '12*, 1–12. <http://doi.org/10.1145/2382196.2382245>
- Oosterbaan, W. ; Lei. van der G. (2014). *Cybersecurity autonoom rijdende voertuigen*.
- Overheid. (2014). Overheid.nl | Consultatie Zelfrijdende auto. Retrieved from <https://www.internetconsultatie.nl/zelfrijdendevoertuigen>
- Overheid. (2016). wetten.nl - Regeling - Regeling voertuigen - BWBR0025798. Retrieved from <http://wetten.overheid.nl/BWBR0025798/2016-03-02#Hoofdstuk5>
- OWASP. (2016). Cross-site Scripting (XSS) - OWASP. Retrieved from [https://www.owasp.org/index.php/Cross-site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))
- Petit, J. et al. (2015). Remote Attacks on Automated Vehicles Sensors : Experiments on Camera and LiDAR. *Blackhat.com*, 1–13. Retrieved from <https://www.blackhat.com/docs/eu-15/materials/eu-15-Petit-Self-Driving-And-Connected-Cars-Fooling-Sensors-And-Tracking-Drivers-wp1.pdf>
- RAI. (2016). SIMS geslaagd in haar missie. RAI. Retrieved from <https://www.raivereniging.nl/artikel/persberichten/2016-q3/0715-sims-geslaagd-in-haar-missie.html>
- Randsdorp, Y; Zondervan, I. (2012). Cyber Security Awareness. Een onderzoek naar kennis , bewustzijn en gedrag ten aanzien van cyber security. *Motivaction*, (November), 1–82. Retrieved from https://www.motivaction.nl/downloads/eindrapportage-cyber-security-awareness_tcm126-464957_1.pdf
- Rechtin, M. (2014). What Toyota learned from its recall crisis. Retrieved May 12, 2016, from <http://www.autonews.com/article/20140525/OEM11/305269965/what-toyota-learned-from-its-recall-crisis>
- Reuters. (2015). North Korea's "paranoid" computer operating system revealed | World news | The Guardian. Retrieved from <https://www.theguardian.com/world/2015/dec/27/north-koreas-computer-operating-system-revealed-by-researchers>
- Rocha, L. (2016). killchain.png. Retrieved from <https://countuponsecurity.files.wordpress.com/2014/08/killchain.png>
- Ross, P. (2016). Volvo's Self-Driving Program Will Have Redundancy For Everything - IEEE Spectrum. Retrieved May 14, 2016, from <http://spectrum.ieee.org/cars-that-think/transportation/self-driving/volvos-selfdriving-program-will-have-redundancy-for-everything>
- SAE On-Road Automated Vehicle Standards Committee. (2014). Taxonomy and definitions for terms related to on-road motor vehicle automated driving systems. *SAE Standard J3016*, (2014-01-16).

- Retrieved from http://www.sae.org/misc/pdfs/automated_driving.pdf
- Sherwood, J. (2004). Enterprise Security Architecture - SABSA. *Information Systems Security*, 6(4), 1–27. <http://doi.org/10.1080/10658989809342548>
- Sherwood, N. A. (2015). *Enterprise security architecture: a business-driven approach*. Retrieved from <http://proquest.safaribooksonline.com/?fpi=9781578203185>
- SIMS. (2015). *Stichting standaardisatie- en informatiebeleid mobiliteit sector (sims) Jaarverslag 2015*. Retrieved from <https://www.raivereniging.nl/ecm/?id=workspace://SpacesStore/b541085f-96ad-484e-b1d0-6c96e7c85806;1.0>
- Singh, S. (2015). Critical reasons for crashes investigated in the National Motor Vehicle Crash Causation Survey. (Traffic Safety Facts Crash Stats. Report No. DOT HS 812 115). Washington, DC: National Highway Traffic Safety Administration. *NHTSA. Traffic Safety Facts Crash•Stats. Report No. DOT HS 812 115*, (February), 1–2. Retrieved from <http://www-nrd.nhtsa.dot.gov/pubs/812115.pdf>
- Smith, B. W. (2013). Human Error As a Cause of Vehicle Crashes. *The Center for Internet and Society*, (December), 1–2. Retrieved from <http://cyberlaw.stanford.edu/blog/2013/12/human-error-cause-vehicle-crashes>
- Smith, C. (2016). *Car Hackers Handbook. A Guide for the Penetration Tester*. Nostarch. Retrieved from <https://www.nostarch.com/carthacking>
- Smulders, A. (2016). Smulders, A. TNO. interview 2016-05-03. Den Haag.
- Sombekke, J. (2016). Sombekke, J. SIMS, Interview 2016-05-24. Hoevelaken.
- Spangenberg, F. (2016). Het perspectief van de gebruikers Smart Driving en Mentality.
- Stanford University. (2016). Automated Driving: Legislative and Regulatory Action - CyberWiki. Retrieved November 13, 2016, from https://cyberlaw.stanford.edu/wiki/index.php/Automated_Driving:_Legislative_and_Regulatory_Action
- Steg, L. (2003). Can Public Transport Compete With the Private Car? *IATSS Research*, 27(2), 27–35. [http://doi.org/10.1016/S0386-1112\(14\)60141-2](http://doi.org/10.1016/S0386-1112(14)60141-2)
- Tesla. (2016). A Tragic Loss | Tesla. Retrieved from https://www.tesla.com/nl_NL/blog/tragic-loss?redirect=no
- TNS. (2016). *Cybersecurity awareness en skills in Nederland*. Retrieved from <https://www.alertonline.nl/media/toolkit/onderzoek/Cybersecurity-Awareness-en-Gedrag-2016.pdf>
- Toyota, Oklahoma, D. court of O. C. S. of. Class action Toyota Motor Corporation Case No. CJ-2008-7969 (2008).
- Toyota, Oklahoma, D. court of O. C. S. of. Class action Toyota Motor Corporation Case No. CJ-2008-7969 Verdict (2013). Retrieved from <https://www.beasleyallen.com/webfiles/toyota-sua-jury-verdict-form-1.pdf>
- TU Automotive. (2016). Cyber Security in the Connected Vehicle Report 2016, 1–46. Retrieved from www.tu-auto.com/cybersecurity-report
- United Nations. (1968). Convention on Road Traffic, (1), 1–66. <http://doi.org/E/CONF.56/16/Rev.1/Amend.1>
- Valasek, C., & Miller, C. (2013). Adventures in Automotive Networks and Control Units. *Technical White Paper*, 1–99. Retrieved from http://www.ioactive.com/pdfs/IOActive_Adventures_in_Automotive_Networks_and_Control_Units.pdf
- Verizon. (2016). 2016 Data Breach Investigations Report. *Verizon Business Journal*, (1), 1–65. <http://doi.org/10.1017/CBO9781107415324.004>
- Visser, T. (2016). Visser, T. Stichting Aanpak Voertuigcriminaliteit. interview 2016-05-12. Hoevelaken.
- Volvo. (2016a). Nordic model offers the rest of world a template for autonomous driving: Volvo CEO. Retrieved May 12, 2016, from <https://www.media.volvocars.com/global/en-gb/media/pressreleases/188162/nordic-model-offers-the-rest-of-world-a-template-for-autonomous-driving-volvo-ceo>
- Volvo. (2016b). Volvo Cars to launch UK's largest and most ambitious autonomous driving trial - Volvo Car Group Global Media Newsroom. Retrieved May 12, 2016, from <https://www.media.volvocars.com/global/en-gb/media/pressreleases/189969/volvo-cars-to-launch-uks-largest-and-most-ambitious-autonomous-driving-trial>
- Weijer, B. van de. (2015). Hack leidt tot grote terugroepactie Range Rovers. *Volkskrant, July 14*. Retrieved from <http://www.volkskrant.nl/economie/land-rover-terugroepactie-niet-wegens-hack~a4100823/>
- Weinmann, R.-P. (2012). Baseband Attacks: Remote Exploitation of Memory Corruptions in Cellular

- Protocol Stacks. *Proceedings of the 6th USENIX Workshop on Offensive Technologies*, 1–10. Retrieved from <https://www.usenix.org/conference/woot12/workshop-program/presentation/weinmann>
- Weise, E. (2016). Nissan Leaf app deactivated because it's hackable. Retrieved from <http://www.usatoday.com/story/tech/news/2016/02/24/nissan-disables-app-hacked-electric-leaf-smart-phone-troy-hunt/80882756/>
- Wijk van, M. (2016). CAN-bus - MVWautotechniek.nl. Retrieved from <http://www.mvwautotechniek.nl/Motor/Canbus/canbus.htm>
- Zhang, T., Antunes, H., & Aggarwal, S. (2014). Defending connected vehicles against malware: Challenges and a solution framework. *IEEE Internet of Things Journal*, 1(1), 10–21. <http://doi.org/10.1109/JIOT.2014.2302386>
- Zijden, van der B., Mason, A. (2016). Zijden, van der B., Mason, A., BMW, Interview 2016-06-13. Rijswijk.

Appendices

Appendix 1: Survey

Survey part 1

This survey is about cyber security for connected cars. Before you start this survey it is good to know that the following definitions are used:

Connected car = Any car that has remote communication possibilities to the internet.

Safety = The condition of being protected from (physical) harm

Security = The state of being free from danger or threat

Hacking = Gaining unauthorised access to computer systems.

Survey part 1: 1 Cybersecurity for cars

Please elaborate on your own experience here

1. Are you aware of the possibility of hacking connected cars? If yes, do you have an example from your own experience? Please elaborate.

Yes

No

Please elaborate on your own experience here

2. Did you (or your organisation) detect a hacked connected car? If yes, how?

No, Never detected a hacked connected car

Technical (eg Logs, IDS-Intrusion Detection System etc)

Media

Hacker contacted us

Other, please specify ...

3. Is there a need to improve car security? If yes, by whom?

No, there is no need to improve car security

Government

Car manufacturers

Insurance companies

Car buyers / car users

Other, please specify ...

4. Who should take the lead to improve car security?

Government

Car manufacturers

Insurance companies

Car buyers / car users

Branch organisations automotive industry

Other, please specify ...

5. Do you think each connected car should be tested on the cyber security status of that specific brand and model? Please elaborate on your choice.

No, cyber security testing of connected cars is not necessary

Yes, cyber security testing of connected cars is necessary

Please elaborate on your choice here.

6. Who should set the standards for cyber security testing of connected cars?

- Government
- Car manufacturers
- Insurance companies
- Branch organisations automotive industry
- Other, please specify ...

7. Should the outcome of the cyber security tests of connected cars made public?

- Yes
- No

Please elaborate on your choice here.

8. If these cyber security tests are made public, should there be a "waiting" period before publication, in order to give car manufacturers the time to fix the vulnerabilities found?

- Yes, a waiting period is necessary to give the car manufacturers some time to fix the vulnerabilities found
- No, publication of the test results must be done as soon as possible

Please elaborate on your choice here

9. If there is a waiting period before the test results are published. How long should this "waiting" period be before publishing the test results?

- No waiting period
- A week
- A month
- Three months
- As long as it takes the car manufacturer to fix the vulnerability
- Other, please specify ...

10. If these cyber security tests are made public, what should be the appropriate means to do that?

- Website of the government
- Website Euro Ncap
- Website car manufacturer
- Website independent organisation
- Other, please specify ...

Survey part 2

This survey is about cyber security for connected cars. Before you start this survey it is good to know that the following definitions are used:

Connected car = Any car that has remote communication possibilities to the internet.

Safety = The condition of being protected from (physical) harm

Security = The state of being free from danger or threat

Hacking = Gaining unauthorised access to computer systems.

Survey part 2: 2 Cybersecurity

1. Who should test cars on cyber security aspects and vulnerabilities?

- Government (eg. RDW)
- Euro Ncap
- Independent organisation
- Other, please specify ...

2. Who should pay for the tests on the cyber security aspects and vulnerabilities of connected cars?

- Government
- Car manufacturers
- Insurance companies
- Car buyers / car users
- Other, please specify ...

3. What is, according to your opinion, the major reason why there is little attention for car security? Please, tick only one box.

- Lack of knowledge with car manufacturers
- No legislation
- No standards available (eg ISO)
- Customers do not ask for it
- Insurance companies do not ask for it
- Costly to implement in the car architecture and design
- Negative business case
- Other car manufacturers don't have (improved) car security as well
- Car hacking is not a real risk
- No media attention
- Other, please specify ...

4. What, in your opinion, is the most likely attack vector on a connected car?

- Direct physical (like direct Can bus access)
- Indirect physical (like USB device, CD etc)
- Wireless (like Bluetooth, cellular etc)
- Sensor fooling
- Other, please specify ...

5. What, in your opinion, is the best defence to prevent hacking of a connected car in general?

- Legislation, hacking is punishable by law
- Legislation, mandatory for car manufacturers to prevent and solve security vulnerabilities of connected cars and introducing penalties in case of non-compliance.
- Publication, "naming and shaming" of car manufacturers that introduce connected cars with security vulnerabilities
- Standardisation of measuring vulnerabilities in connected cars
- Other, please specify ...

6. What, in your opinion, is the best defence to prevent hacking of a connected car via direct physical access (direct Can bus access)?

- I don't know
- I think the best defence would be ...

7. What, in your opinion, is the best defence to prevent hacking of a connected car via indirect physical access (USB device, CD)?

- I don't know
- I think the best defence would be ...

8. What, in your opinion, is the best defence to prevent hacking of a connected car via wireless access (Bluetooth / cellular)?

- I don't know
- I think the best defence would be ...

9. What, in your opinion, is the best defence to prevent hacking of a connected car via sensor fooling?

- I don't know
- I think the best defence would be ...

10. Can the encryption of CAN bus data contribute to improved car security? Please elaborate.

- No, Encryption of CAN bus data does not help to improve car security
 - Yes, Encryption of CAN bus data improves car security
- Please elaborate on your choice here

Survey part 3

This survey is about cyber security for connected cars. Before you start this survey it is good to know that the following definitions are used:

Connected car = Any car that has remote communication possibilities to the internet.

Safety = The condition of being protected from (physical) harm

Security = The state of being free from danger or threat

Hacking = Gaining unauthorised access to computer systems.

Survey part 3: 3Car security

1. What can you (or your organisation) contribute to improve car security? Please elaborate.

- Nothing
- The possible contribution to improve car security can be ...

2. In the case of a detected cyber security vulnerability of a connected car, what is (of should be) the appropriate method to fix this?

- Immediate recall by the car manufacturer of all affected cars of that brand. The car manufacturer should install the necessary security patch for these cars immediately.
- The car manufacturer can push a security patch via the manufacturer remote wireless access to update the car firmware.
- A patch for that security vulnerability can be installed by the car manufacturer at the same time with the next scheduled car maintenance.
- All relevant security patches can be installed during the next mandatory APK check of the connected car.
- Other, please specify ...

3. Should the car user be notified by the car manufacturer that a cyber security vulnerability is detected in his/her connected car?

- No, there is no need to inform the car user of cyber security vulnerabilities. This will only create fear, uncertainty and doubt.
- No, the car manufacturer must only inform the car user of severe cyber security issues of that connected car.
- Yes, the car manufacturer must inform the car user, but only when a security patch is available for the detected vulnerability.
- Yes, the car user has a right to know all cyber security issues of his car.
- Other, please specify ...

4. How long must the car manufacturer support security patches for the connected car?

- The car manufacturer must support security patches for connected cars as long as there is any connected car left on the road of that brand.
- The car manufacturer is only obligated to support security patches for connected cars during the factory warranty period.
- The car manufacturer is only obligated to support security patches for connected cars in accordance with the law of that country.
- The car manufacturer is not obligated to support security patches for connected cars. It can be an additional service of the car manufacturer to the customers.
- Other, please specify ...

5. Who is (or should be) liable, in your opinion, for the damage (physical and economical) when a connected car is hacked?

- Hacker
- Car manufacturer
- Insurance company
- Car user
- Other, please specify ...

6. E call (Emergency call of your car to the emergency services when your car is involved in a car accident) will be available in all new European cars from march 2018. E-call is mandatory and signals accident data, your location and driving direction. Do you think there are security implications with the introduction of E-call in connected cars?

- No, this is a good thing
- Yes, the government will gather this data and can then track all movements of individual citizens
- Yes, Car manufacturers will gather this data and can then track all movements of individual customers. Misuse of this data for commercial purposes is a risk.
- Yes, Car insurance companies will gather this data and can then track all movements of individual customers. Misuse of this data for commercial purposes is a risk.
- Yes, but I don't know why. It just does not feel good.
- I don't know
- Yes, other reason, please specify ...

7. B call (=Breakdown call when your car breaks down) will be available in some new European cars. B-call is optional and can be switched on or off by the car manufacturer. Do you think there are security implications with the introduction of B-call in connected cars?

- No, this is a good thing
- Yes, the government will gather this data and can then track all movements of individual citizens
- Yes, Car manufacturers will gather this data and can then track all movements of individual customers. Misuse of this data for commercial purposes is a risk.
- Yes, Car insurance companies will gather this data and can then track all movements of individual customers. Misuse of this data for commercial purposes is a risk.
- Yes, but I don't know why. It just does not feel good.
- I don't know
- Yes, other reason, please specify ...

8. S call (=Service call when your car is scheduled for maintenance) will be available in some new European cars. S-call is optional and can be switched on or off by the car manufacturer. Do you think there are security implications with the introduction of S-call in connected cars?

- O No, this is a good thing
- O Yes, the government will gather this data and can then track all movements of individual citizens
- O Yes, Car manufacturers will gather this data and can then track all movements of individual customers. Misuse of this data for commercial purposes is a risk.
- O Yes, Car insurance companies will gather this data and can then track all movements of individual customers. Misuse of this data for commercial purposes is a risk.
- O Yes, but I don't know why. It just does not feel good.
- O I don't know
- O Yes, other reason, please specify ...

9. What, in your opinion, is the best solution to prevent security risks of the introduction of B call (car break down call) and S call (car service call for maintenance)?

- O The car manufacturer must choose the best option for the car user. Eg. When the car comes out of the factory all options for a maximum customer satisfaction allowed for that country are switched on.
- O The car manufacturer must inform and choose the best option for the car user. Eg. The car manufacturer informs the customer in the showroom of the options and agrees which options to turn on or off.
- O The car user must be able to switch these options on or off whenever he/she wants
- O The government must introduce appropriate legislation to prevent misuse of this kind of data.
- O Other, please specify ...

10. Do you have any other remarks on this subject that we missed in this survey?

- O No
- O Yes, see my remarks below

Appendix 2: Survey structure, process and results

The survey was conducted from 4-5-2016 to 11-11-2016.

The survey consists of 30 questions.

Question 1-10 on <https://nl.surveymonkey.com/r/KTDZPLY>

Question 11-20 <https://nl.surveymonkey.com/r/7JTX6Z2>

Question 21-30 <https://nl.surveymonkey.com/r/7XLJQV3> The initial survey version was even longer, but peer reviews and an initial test with TNO revealed that the survey was too long and complicated. The goal of the survey is to compare the view of the respondents with the view of the interviewed experts on the security aspects of the connected car. The online survey was published using SurveyMonkey.²⁰⁵ The survey was split in three parts of each 10 questions. This makes it easier for the respondents to finish the survey in their own time. The downside of this is that the analysis of the survey results is more complex. Another downside is that some respondents did not finish the whole survey. The survey was mailed to selected people with the request to participate. The survey was sent mail addressing each person personally. The survey was also published online on the website: <http://carsecurity.agency> and the website <http://networks.centre4innovation.org/csa/herbert/> The survey was also posted on LinkedIn site of the researcher. Another step to generate enough survey data was using the cyber security experts of the CSA, Cyber Security Academy. The survey was handed out on paper in the course on “actors and behaviour in cyberspace” on May 13, 2016 of which twelve people responded. All respondents have a bachelor or master education background.

The first part of the survey had 90 respondents, the second part of the survey had 86 respondents and the third part of the survey had 84 respondents.

The table below shows the number of surveys send and the response rate.

Where	Send	Response	Response Percentage	Remark
CSA	13	12	92	1 female, 11 male. Survey on paper
Telecom	76	48	63	4 female, 44 male. Survey by mail
ICT	12	10	83	3 female, 7 male. Survey by mail
Website	∞	1	n.a.	Survey on 3 websites
Interview	13	13	100	Survey on paper + Interview
Total	114	84	73	

Table 12 Survey response overview on surveys that are completed in full (n=84).

The initial assumption that the sending the survey by mail with a personal touch should deliver a high response seems to be correct.

Several respondents indicated that it took about an hour to fill out the survey. It took so long because they wanted to describe possible solutions or indicate additional problem statements to the posed questions.

Asking people in person or with a personal email to respond to the survey delivers the highest response. The possible downside is that the respondents think the researcher can see their personal responses on the survey. This might trigger “social accepted” answers to the survey questions.

The question that triggered the most “discussion” was 3.4 (survey part 3 question 4). “How long must the car manufacturer support security patches for the connected car?” People

²⁰⁵ <https://nl.surveymonkey.com/>

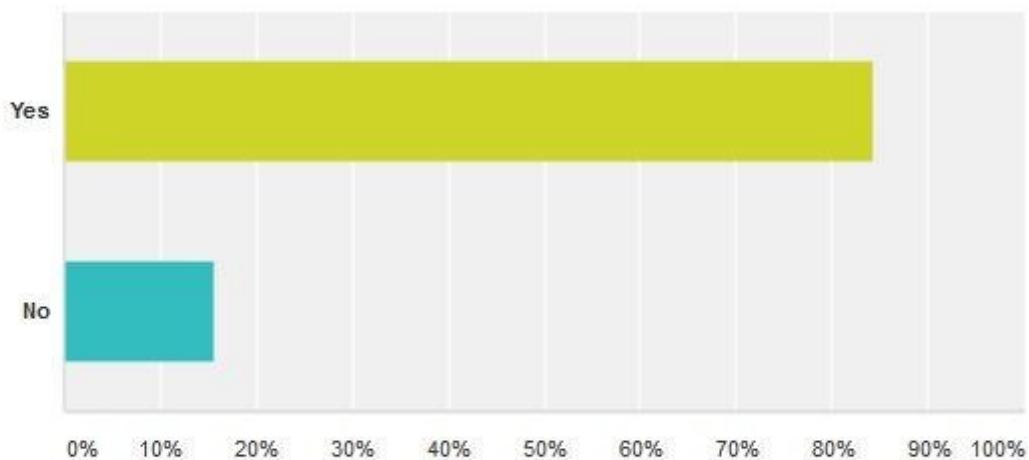
realised what the implications of the answer to this question can be for the automotive industry and society as a whole.

The question 3.7 on C-call, 3.8 B-call and 3.9 about S-call were seen by a lot of respondents as the same question.

The general conclusion of the survey is that although we agree on the high level questions, as soon as we look into the specific details all people seem to have a different opinion. The opportunity to add some text in the “free text format field” was extensively used by the participants.

1.1 Are you aware of the possibility of hacking connected cars? If yes, do you have an example from your own experience? Please elaborate.

Beantwoord: 90 Overgeslagen: 0

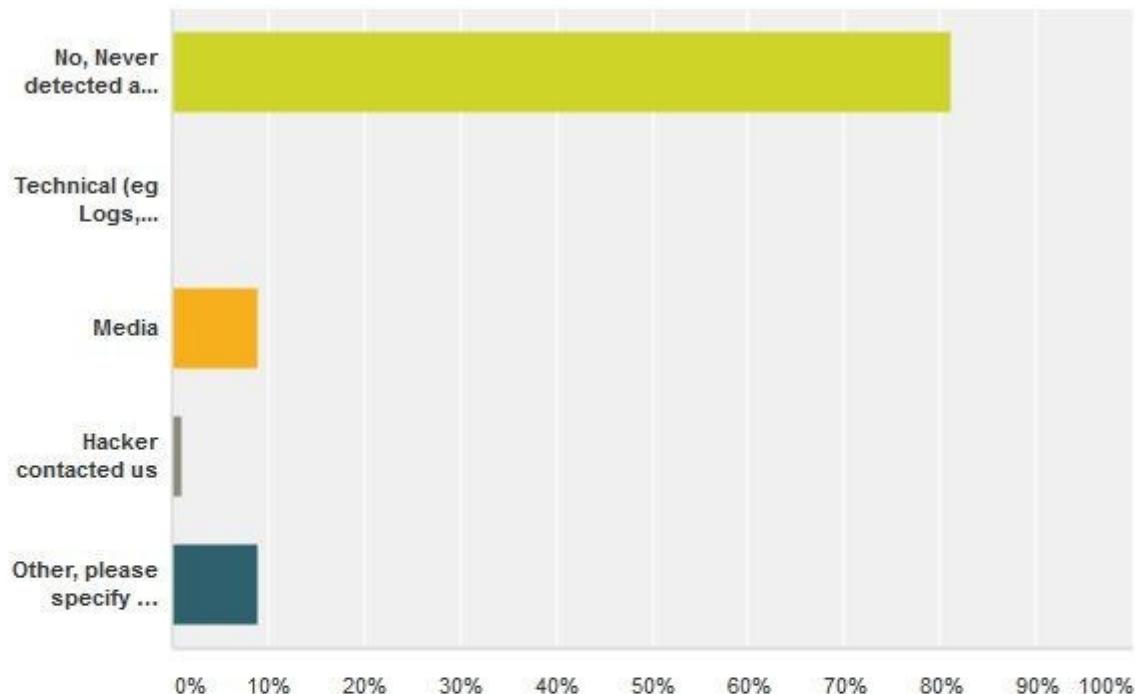


Antwoordkeuzen	Reacties
Yes	84,44%
No	15,56%
Totaal	90

Opmerkingen (60)

1.2 Did you (or your organisation) detect a hacked connected car? If yes, how?

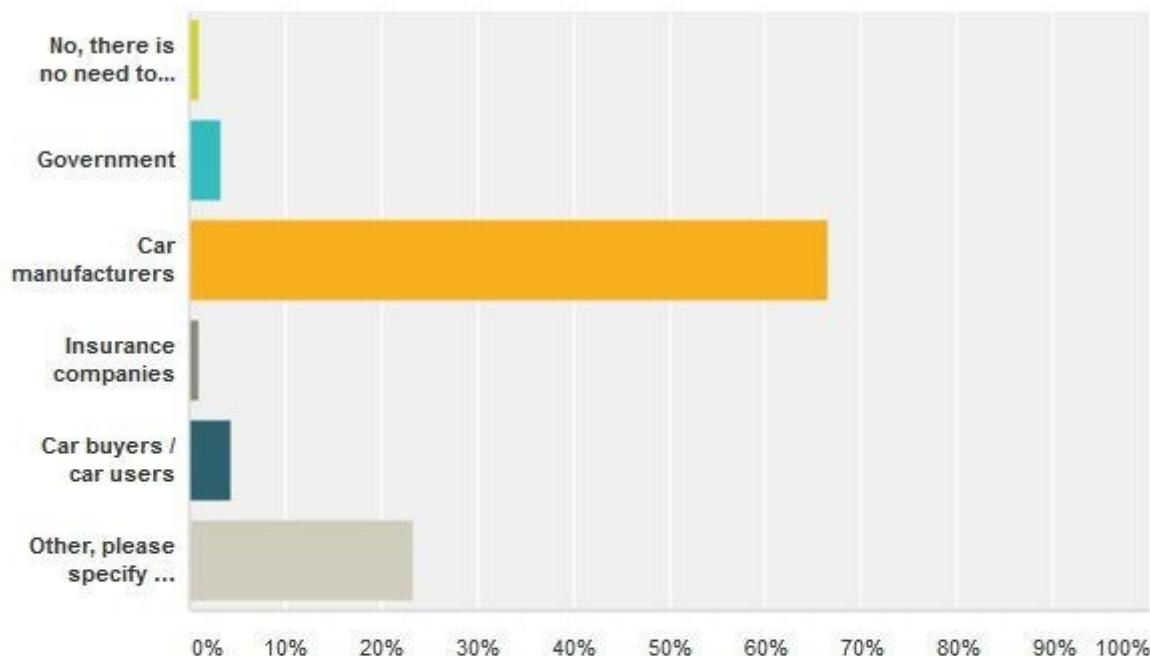
Beantwoord: 90 Overgeslagen: 0



Antwoordkeuzen	Reacties	Percentage
No, Never detected a hacked connected car	73	81,11%
Technical (eg Logs, IDS-Intrusion Detection System etc)	0	0,00%
Media	8	8,89%
Hacker contacted us	1	1,11%
Other, please specify ...	8	8,89%
Totaal	90	

1.3 Is there a need to improve car security? If yes, by whom?

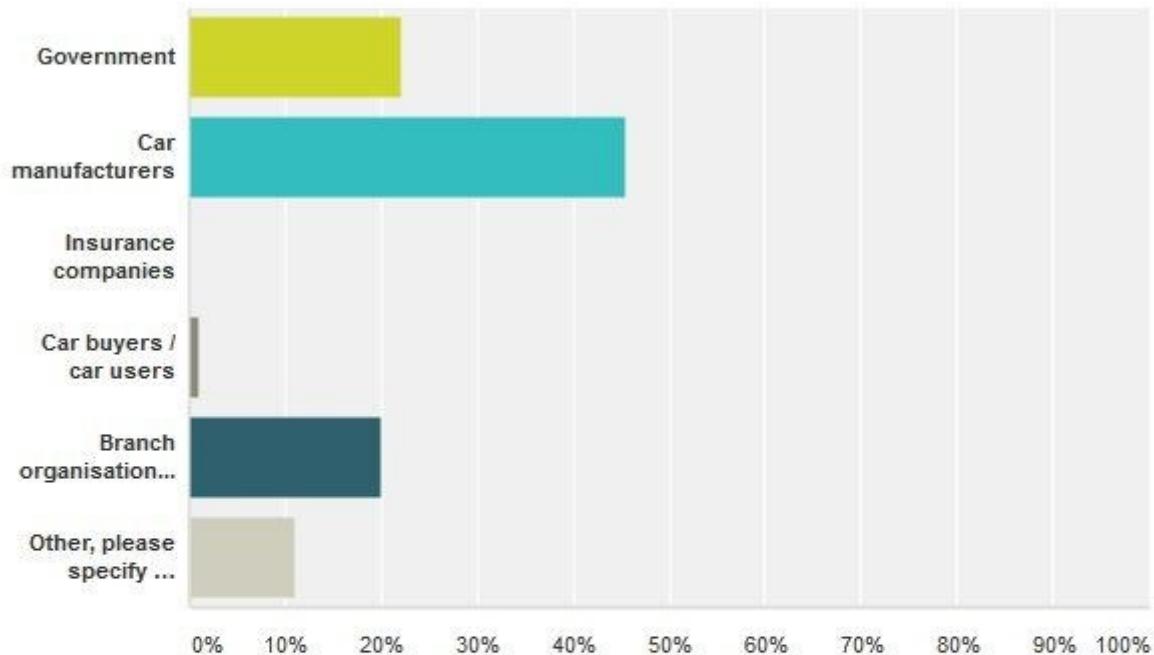
Beantwoord: 90 Overgeslagen: 0



Antwoordkeuzen	Reacties	%
No, there is no need to improve car security	1	1,11%
Government	3	3,33%
Car manufacturers	60	66,67%
Insurance companies	1	1,11%
Car buyers / car users	4	4,44%
Other, please specify ...	21	23,33%
Totaal	90	

1.4 Who should take the lead to improve car security?

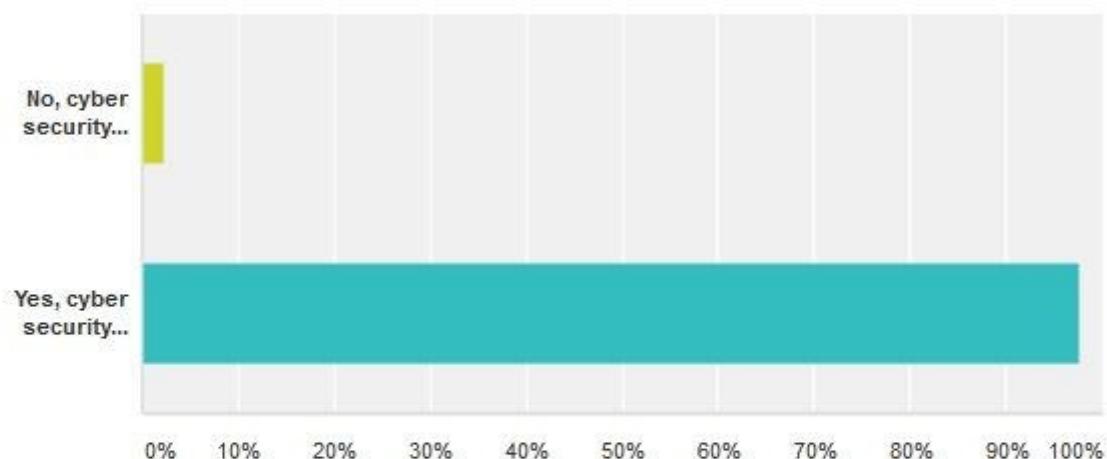
Beantwoord: 90 Overgeslagen: 0



Antwoordkeuzen	Reacties	%
Government	20	22,22%
Car manufacturers	41	45,56%
Insurance companies	0	0,00%
Car buyers / car users	1	1,11%
Branch organisations automotive industry	18	20,00%
Other, please specify ...	10	11,11%
Totaal	90	

1.5 Do you think each connected car should be tested on the cyber security status of that specific brand and model? Please elaborate on your choice.

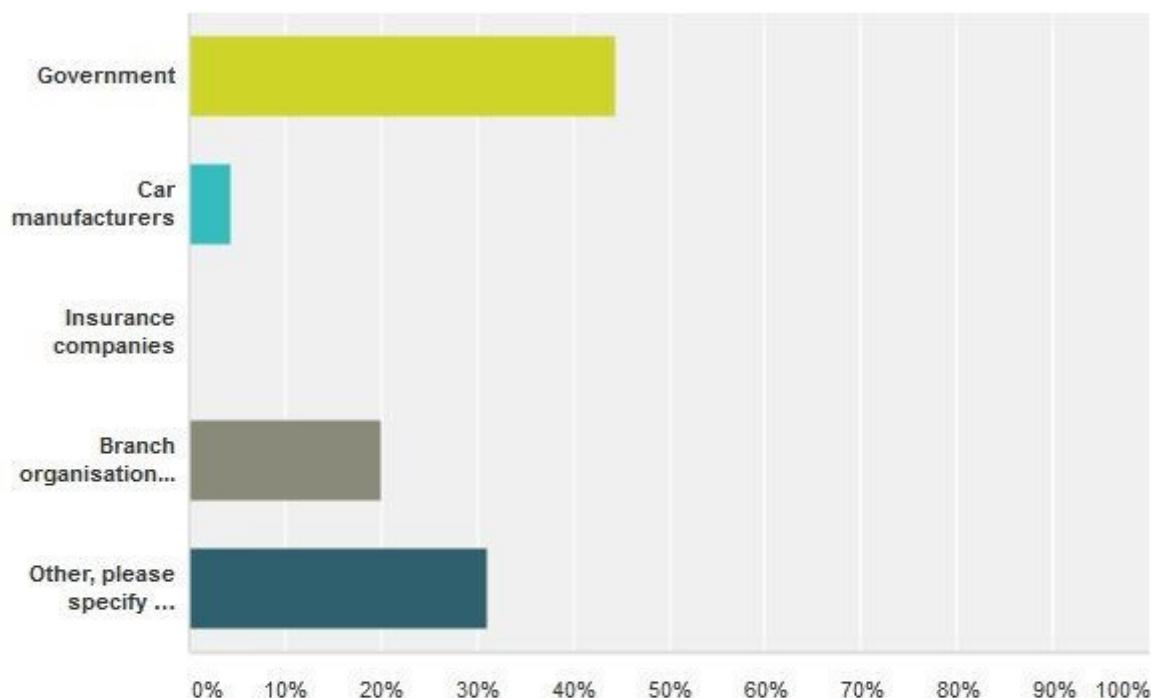
Beantwoord: 88 Overgeslagen: 2



Antwoordkeuzen	Reacties
No, cyber security testing of connected cars is not necessary	2,27%
Yes, cyber security testing of connected cars is necessary	97,73%
Totaal	88
Opmerkingen (57)	

1.6 Who should set the standards for cyber security testing of connected cars?

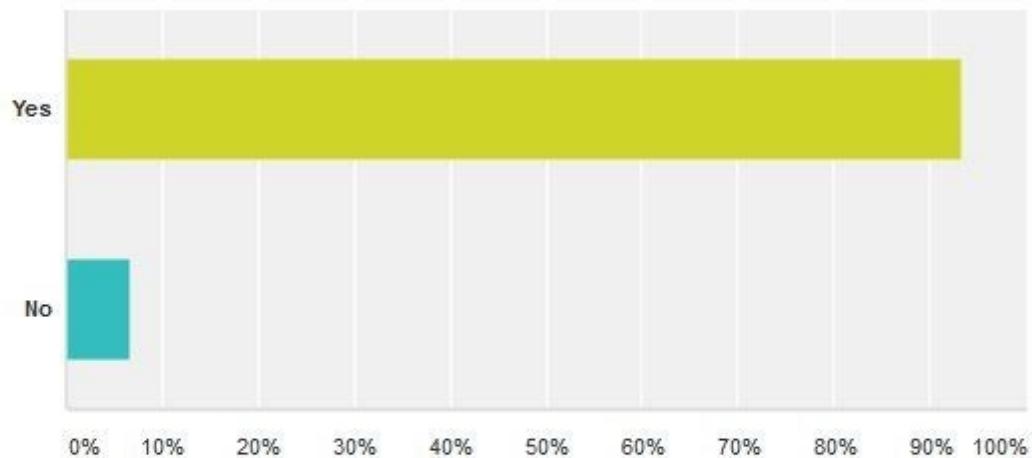
Beantwoord: 90 Overgeslagen: 0



Antwoordkeuzen	Reacties	
▼ Government	44,44%	40
▼ Car manufacturers	4,44%	4
▼ Insurance companies	0,00%	0
▼ Branch organisations automotive industry	20,00%	18
▼ Other, please specify ... Please specify ...	Reacties	31,11%
Totaal		90

1.7 Should the outcome of the cyber security tests of connected cars made public?

Beantwoord: 90 Overgeslagen: 0

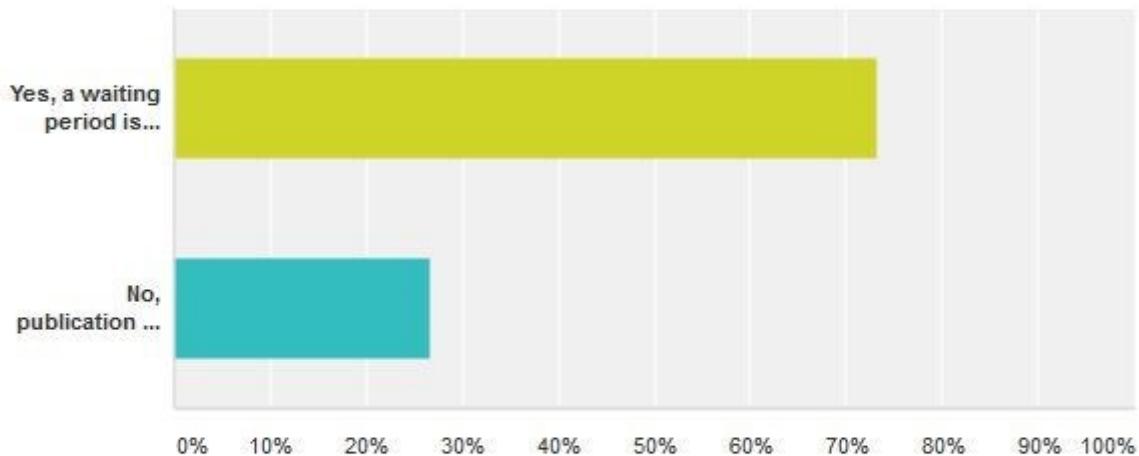


Antwoordkeuzen	Reacties
Yes	93,33%
No	6,67%
Totaal	90

Opmerkingen (52)

1.8 If these cyber security tests are made public, should there be a "waiting" period before publication, in order to give car manufacturers the time to fix the vulnerabilities found?

Beantwoord: 90 Overgeslagen: 0

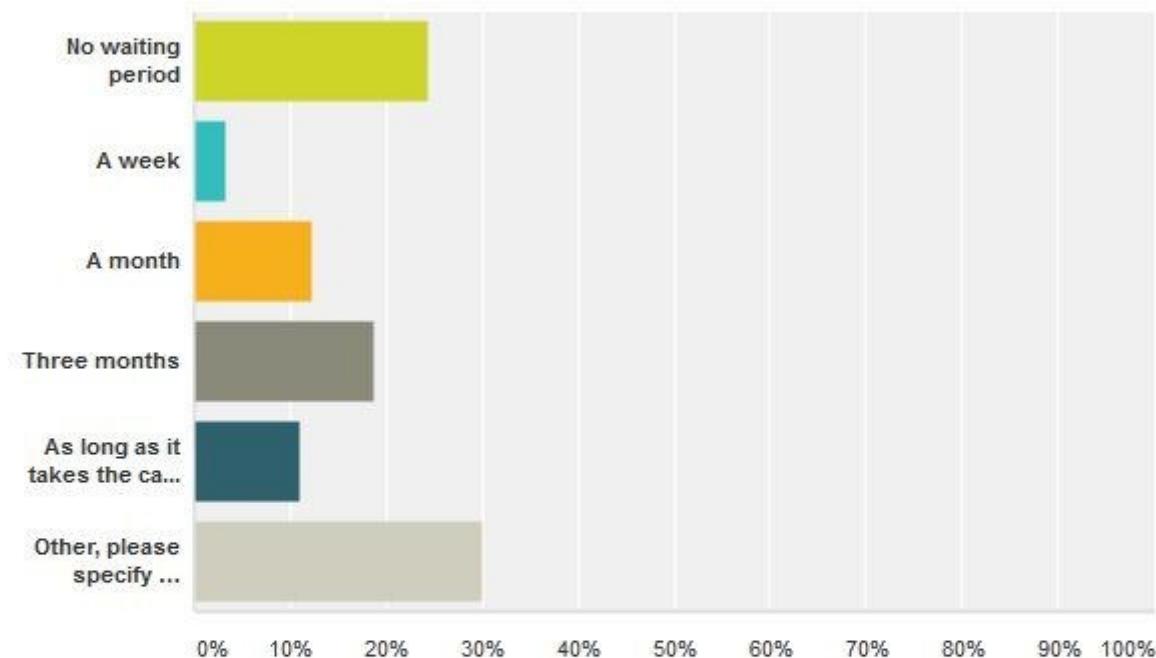


Antwoordkeuzen	Reacties
Yes, a waiting period is necessary to give the car manufacturers some time to fix the vulnerabilities found	73,33% 66
No, publication of the test results must be done as soon as possible	26,67% 24
Totaal	90

Opmerkingen (45)

1.9 If there is a waiting period before the test results are published. How long should this "waiting" period be before publishing the test results?

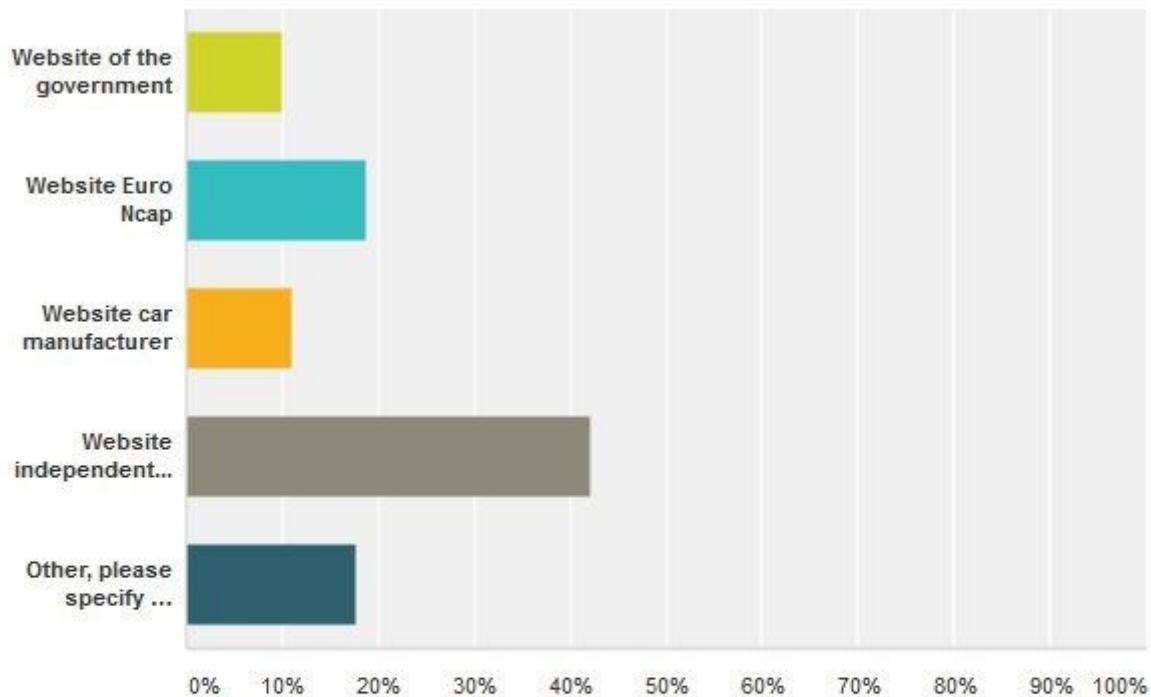
Beantwoord: 90 Overgeslagen: 0



Antwoordkeuzen	Reacties	%
No waiting period	22	24,44%
A week	3	3,33%
A month	11	12,22%
Three months	17	18,89%
As long as it takes the car manufacturer to fix the vulnerability	10	11,11%
Other, please specify ...	27	30,00%
Totaal	90	

1.10 If these cyber security tests are made public, what should be the appropriate means to do that?

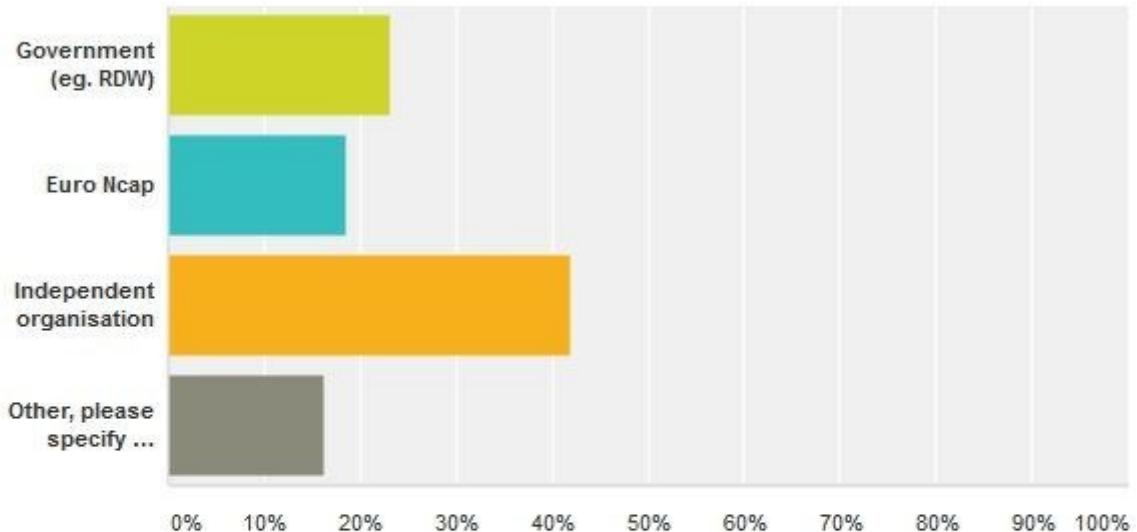
Beantwoord: 90 Overgeslagen: 0



Antwoordkeuzen	Reacties	%
Website of the government	9	10,00%
Website Euro Ncap	17	18,89%
Website car manufacturer	10	11,11%
Website independent organisation	38	42,22%
Other, please specify ...	16	17,78%
Totaal	90	

2.1 Who should test cars on cyber security aspects and vulnerabilities?

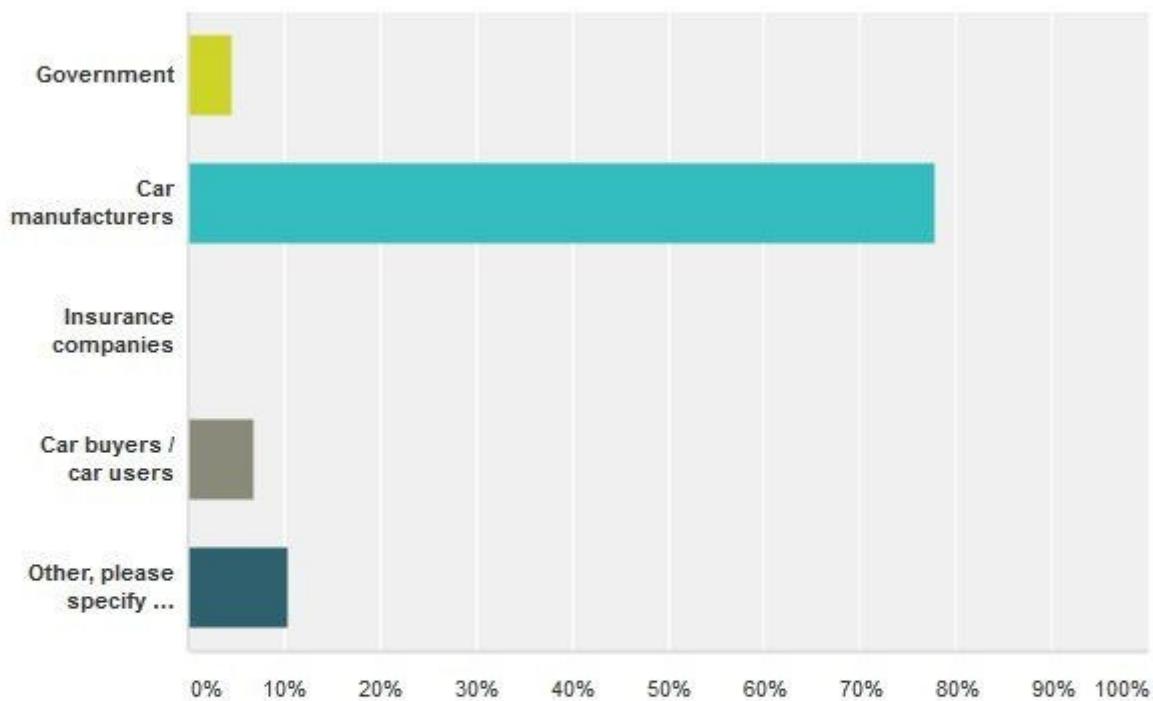
Beantwoord: 86 Overgeslagen: 0



Antwoordkeuzen	Reacties	%
Government (eg. RDW)	20	23,26%
Euro Ncap	16	18,60%
Independent organisation	36	41,86%
Other, please specify ...	14	16,28%
Totaal	86	

2.2 Who should pay for the tests on the cyber security aspects and vulnerabilities of connected cars?

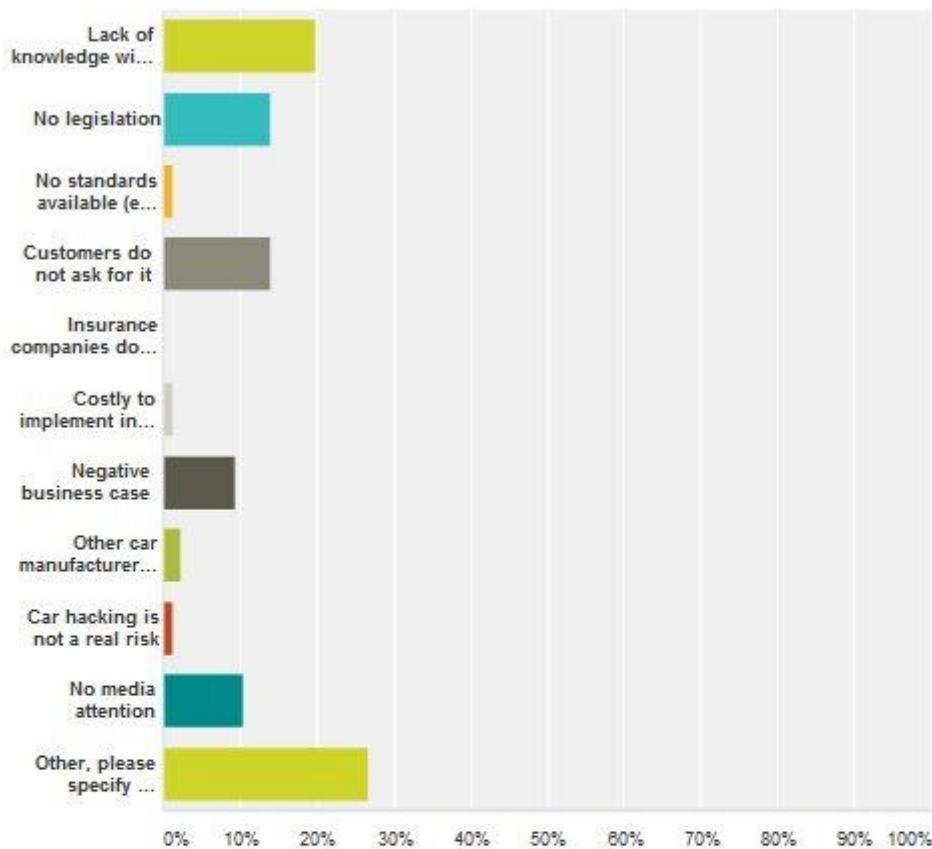
Beantwoord: 86 Overgeslagen: 0



Antwoordkeuzen	Reacties	%
Government	4	4,65%
Car manufacturers	67	77,91%
Insurance companies	0	0,00%
Car buyers / car users	6	6,98%
Other, please specify ...	9	10,47%
Totaal	86	100%

2.3 What is, according to your opinion, the major reason why there is little attention for car security? Please, tick only one box.

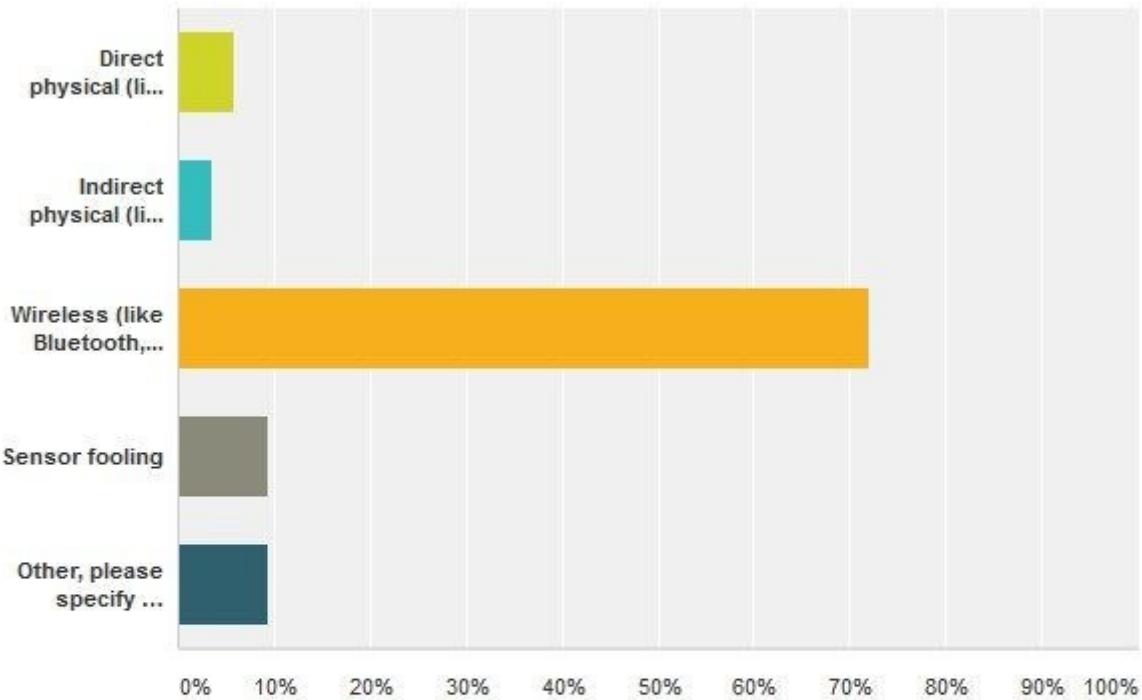
Beantwoord: 86 / Overgeslagen: 0



Antwoordkeuzen	Reacties	%
Lack of knowledge with car manufacturers	17	19,77%
No legislation	12	13,95%
No standards available (eg ISO)	1	1,16%
Customers do not ask for it	12	13,95%
Insurance companies do not ask for it	0	0,00%
Costly to implement in the car architecture and design	1	1,16%
Negative business case	8	9,30%
Other car manufacturers don't have (improved) car security as well	2	2,33%
Car hacking is not a real risk	1	1,16%
No media attention	9	10,47%
Other, please specify ...	23	26,74%
Totaal	86	

2.4 What, in your opinion, is the most likely attack vector on a connected car?

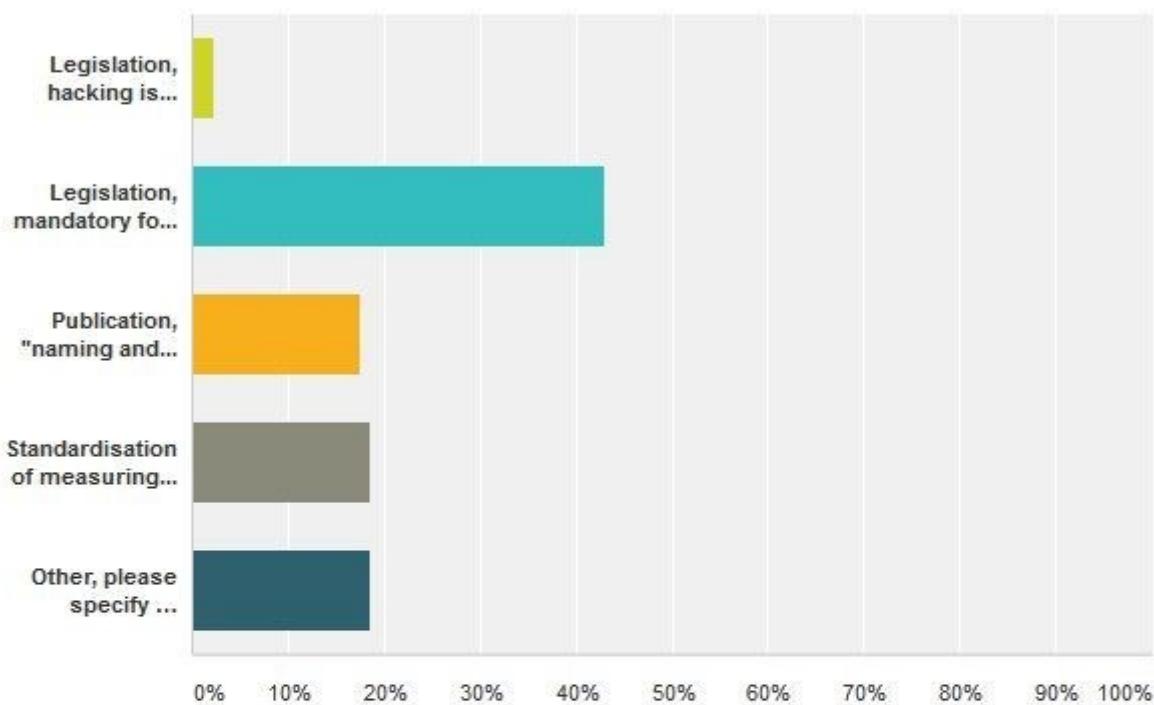
Beantwoord: 86 Overgeslagen: 0



Antwoordkeuzen	Reacties
▼ Direct physical (like direct Can bus access)	5,81%
▼ Indirect physical (like USB device, CD etc)	3,49%
▼ Wireless (like Bluetooth, cellular etc)	72,09%
▼ Sensor fooling	9,30%
▼ Other, please specify ...	9,30%
Totaal	86

2.5 What, in your opinion, is the best defence to prevent hacking of a connected car in general?

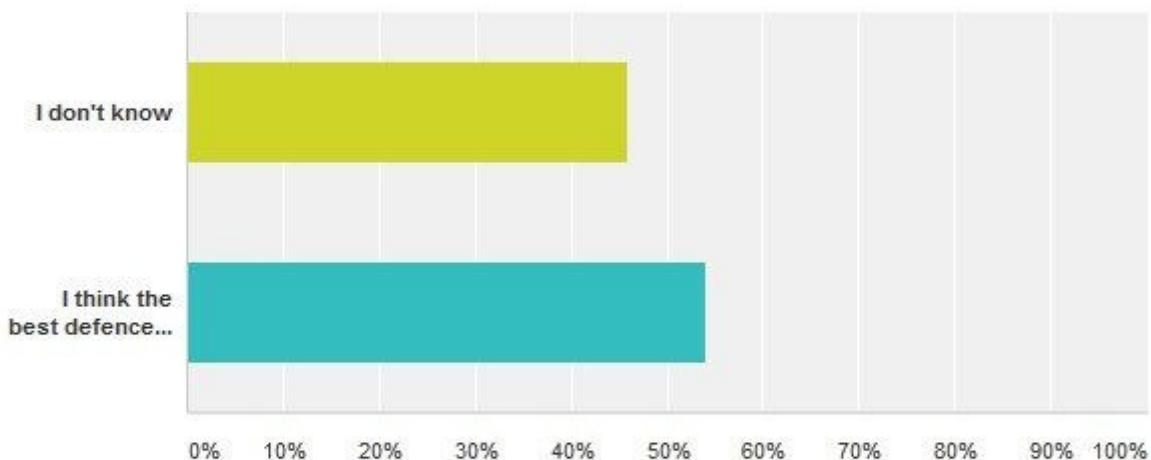
Beantwoord: 86 Overgeslagen: 0



Antwoordkeuzen	Reacties
Legislation, hacking is punishable by law	2,33% 2
Legislation, mandatory for car manufacturers to prevent and solve security vulnerabilities of connected cars and introducing penalties in case of non-compliance.	43,02% 37
Publication, "naming and shaming" of car manufacturers that introduce connected cars with security vulnerabilities	17,44% 15
Standardisation of measuring vulnerabilities in connected cars	18,60% 16
Other, please specify ...	18,60% 16
Totaal	86

2.6 What, in your opinion, is the best defence to prevent hacking of a connected car via direct physical access (direct Can bus access)?

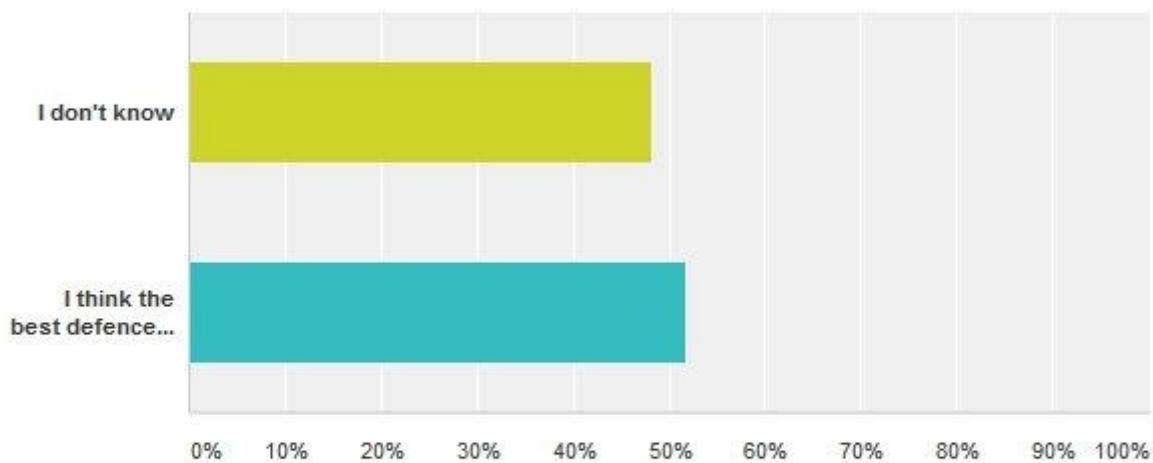
Beantwoord: 85 Overgeslagen: 1



Antwoordkeuzen	Reacties	%
I don't know	39	45,88%
I think the best defence would be ...	46	54,12%
Totaal	85	

2.7 What, in your opinion, is the best defence to prevent hacking of a connected car via indirect physical access (USB device, CD)?

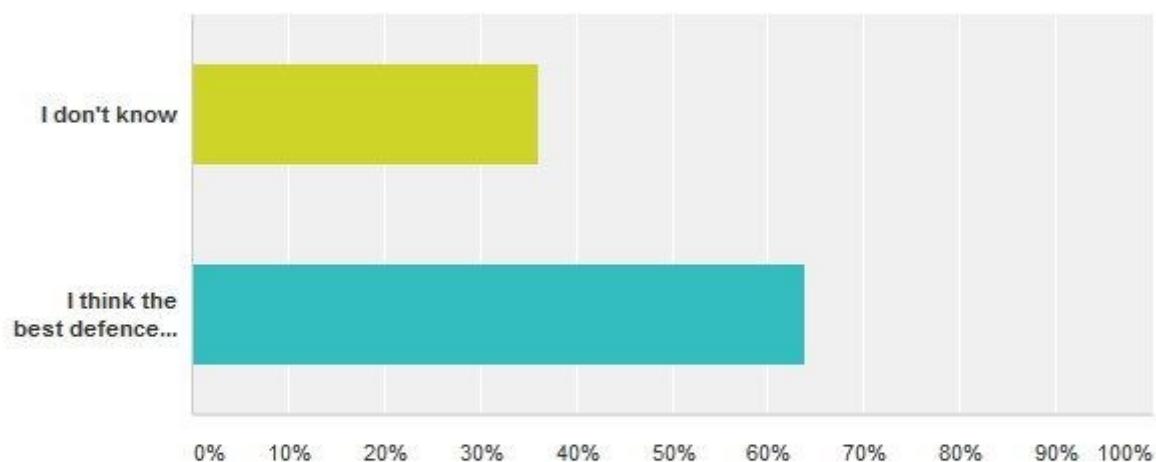
Beantwoord: 85 Overgeslagen: 1



Antwoordkeuzen	Reacties	%
I don't know	41	48,24%
I think the best defence would be ...	44	51,76%
Totaal	85	

2.8 What, in your opinion, is the best defence to prevent hacking of a connected car via wireless access (Bluetooth / cellular)?

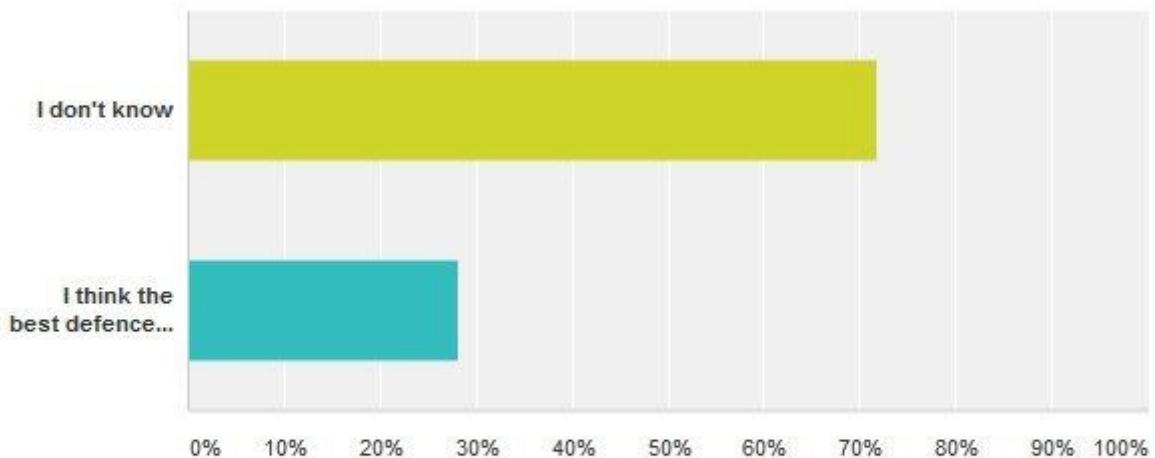
Beantwoord: 83 Overgeslagen: 3



Antwoordkeuzen	Reacties	%
I don't know	30	36,14%
I think the best defence would be ...	53	63,86%
Totaal	83	

2.9 What, in your opinion, is the best defence to prevent hacking of a connected car via sensor fooling?

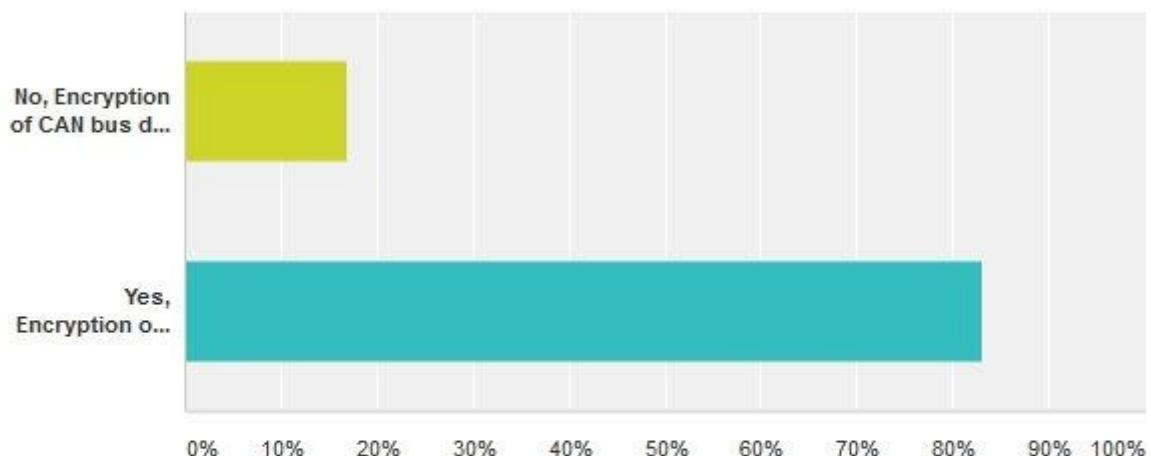
Beantwoord: 85 Overgeslagen: 1



Antwoordkeuzen	Reacties	%
I don't know	61	71,76%
I think the best defence would be ...	24	28,24%
Totaal	85	

2.10 Can the encryption of CAN bus data contribute to improved car security? Please elaborate.

Beantwoord: 83 Overgeslagen: 3

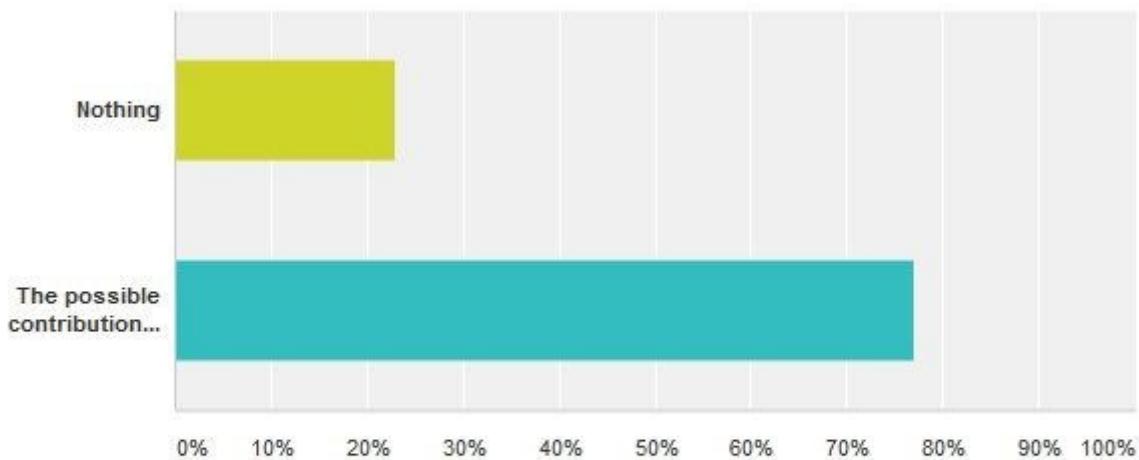


Antwoordkeuzen	Reacties	%
▼ No, Encryption of CAN bus data does not help to improve car security	14	16,87%
▼ Yes, Encryption of CAN bus data improves car security	69	83,13%
Totaal	83	

Opmerkingen (51)

3.1 What can you (or your organisation) contribute to improve car security? Please elaborate.

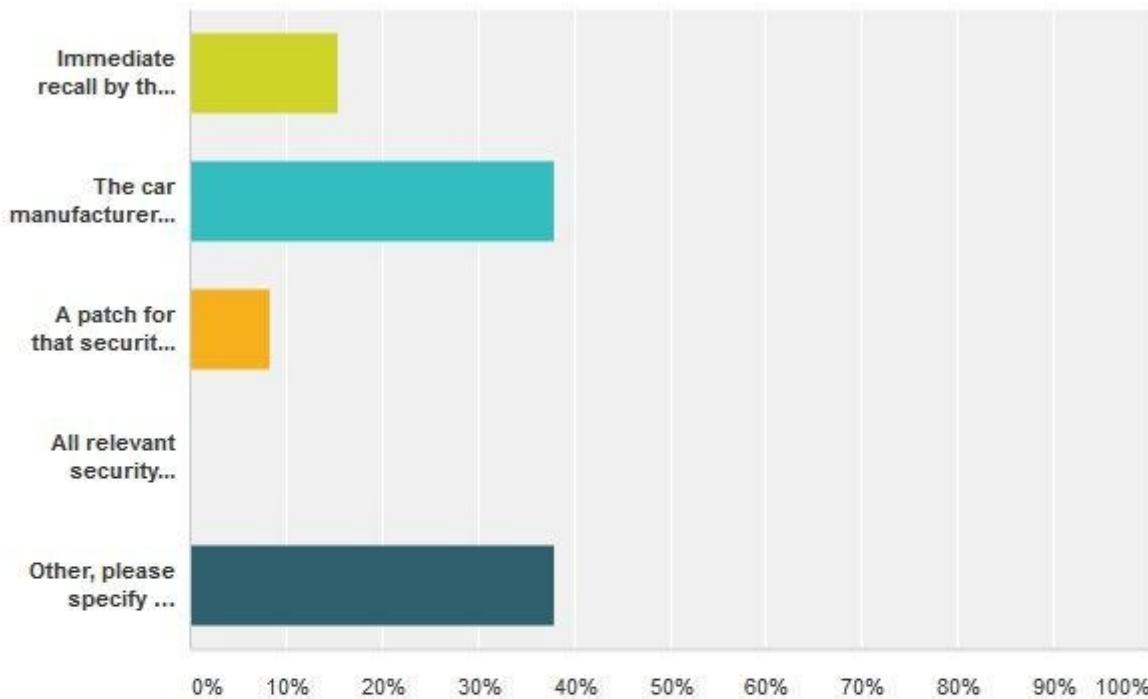
Beantwoord: 83 Overgeslagen: 1



Antwoordkeuzen	Reacties	%
Nothing	19	22,89%
The possible contribution to improve car security can be ...	64	77,11%
Totaal	83	

3.2 In the case of a detected cyber security vulnerability of a connected car, what is (or should be) the appropriate method to fix this?

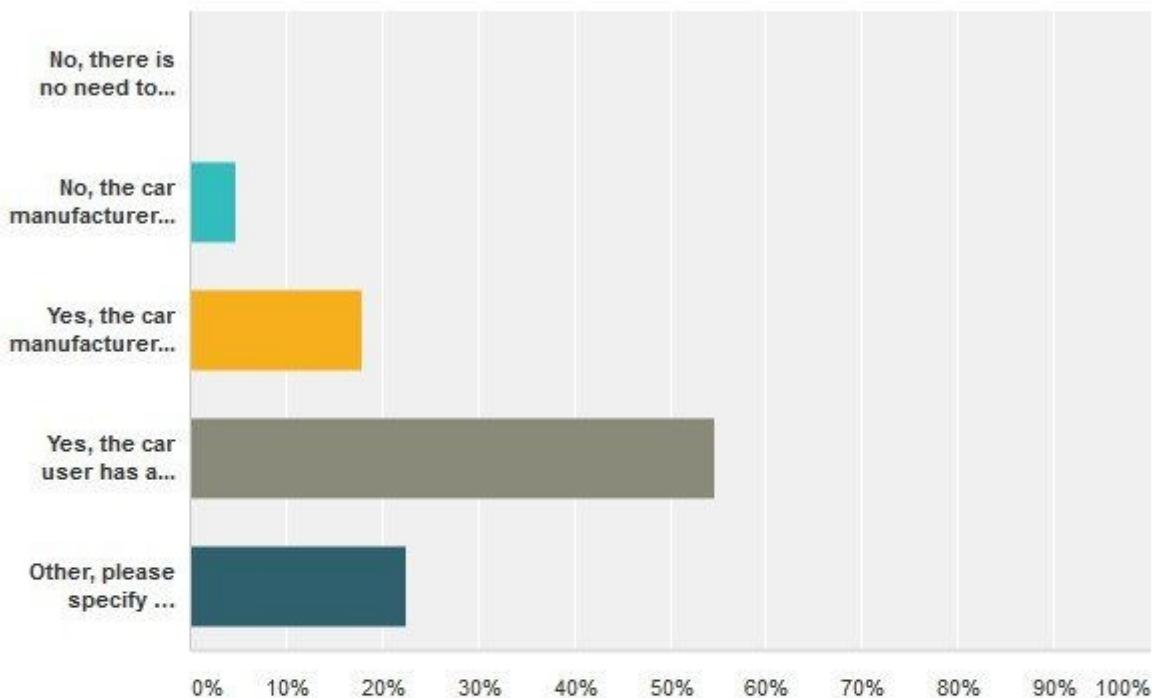
Beantwoord: 84 Overgeslagen: 0



Antwoordkeuzen	Reacties
Immediate recall by the car manufacturer of all affected cars of that brand. The car manufacturer should install the necessary security patch for these cars immediately.	15,48% 13
The car manufacturer can push a security patch via the manufacturer remote wireless access to update the car firmware.	38,10% 32
A patch for that security vulnerability can be installed by the car manufacturer at the same time with the next scheduled car maintenance.	8,33% 7
All relevant security patches can be installed during the next mandatory APK check of the connected car.	0,00% 0
Other, please specify ...	Reacties 38,10% 32
Totaal	84

3.3 Should the car user be notified by the car manufacturer that a cyber security vulnerability is detected in his/her connected car?

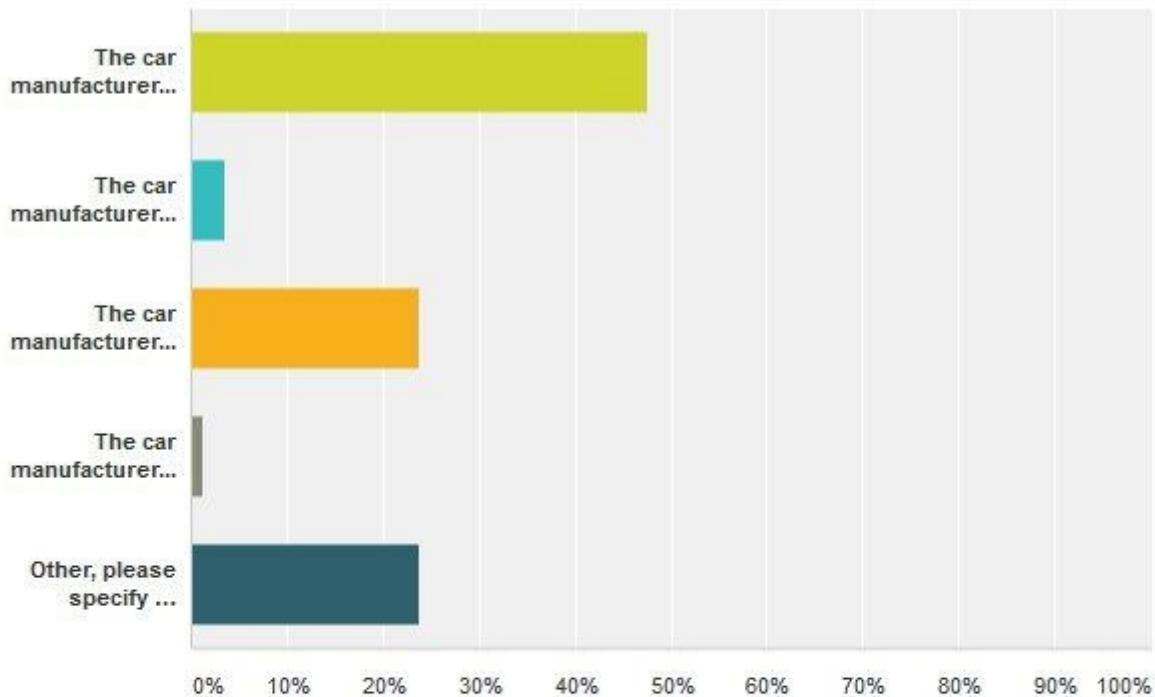
Beantwoord: 84 Overgeslagen: 0



Antwoordkeuzen	Reacties	%
▼ No, there is no need to inform the car user of cyber security vulnerabilities. This will only create fear, uncertainty and doubt.	0	0,00%
▼ No, the car manufacturer must only inform the car user of severe cyber security issues of that connected car.	4	4,76%
▼ Yes, the car manufacturer must inform the car user, but only when a security patch is available for the detected vulnerability.	15	17,86%
▼ Yes, the car user has a right to know all cyber security issues of his car.	46	54,76%
▼ Other, please specify ...	19	22,62%
Totaal	84	

3.4 How long must the car manufacturer support security patches for the connected car?

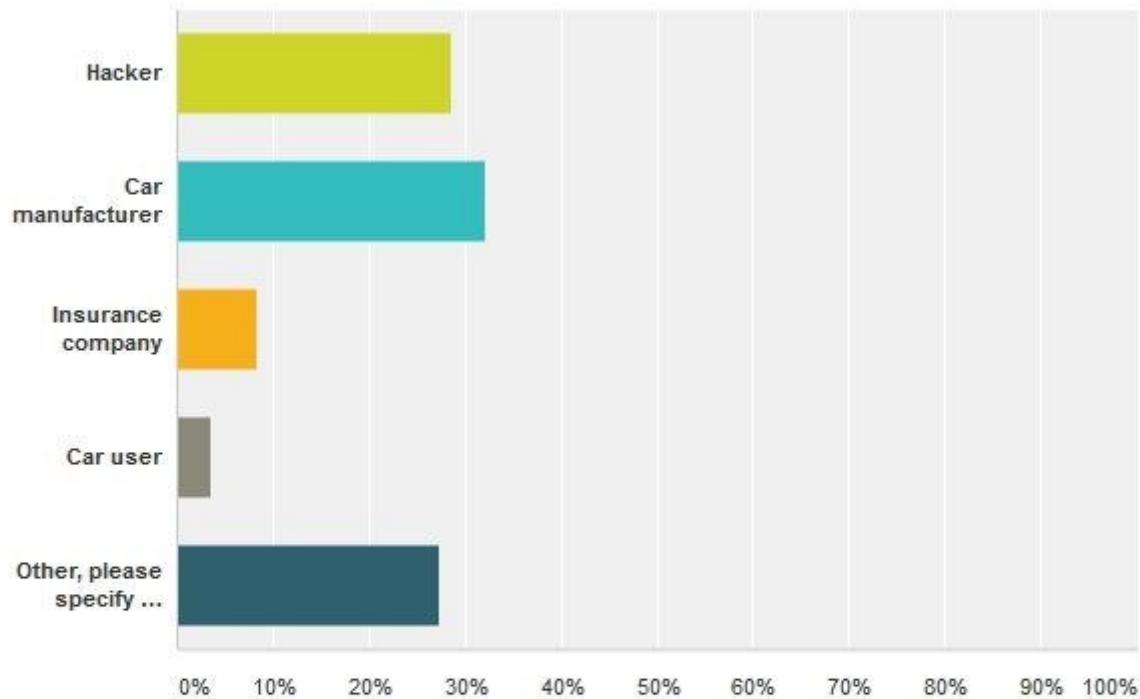
Beantwoord: 84 Overgeslagen: 0



Antwoordkeuzen	Reacties
▼ The car manufacturer must support security patches for connected cars as long as there is any connected car left on the road of that brand.	47,62% 40
▼ The car manufacturer is only obligated to support security patches for connected cars during the factory warranty period.	3,57% 3
▼ The car manufacturer is only obligated to support security patches for connected cars in accordance with the law of that country.	23,81% 20
▼ The car manufacturer is not obligated to support security patches for connected cars. It can be an additional service of the car manufacturer to the customers.	1,19% 1
▼ Other, please specify ...	Reacties 23,81% 20
Totaal	84

3.5 Who is (or should be) liable, in your opinion, for the damage (physical and economical) when a connected car is hacked?

Beantwoord: 84 Overgeslagen: 0

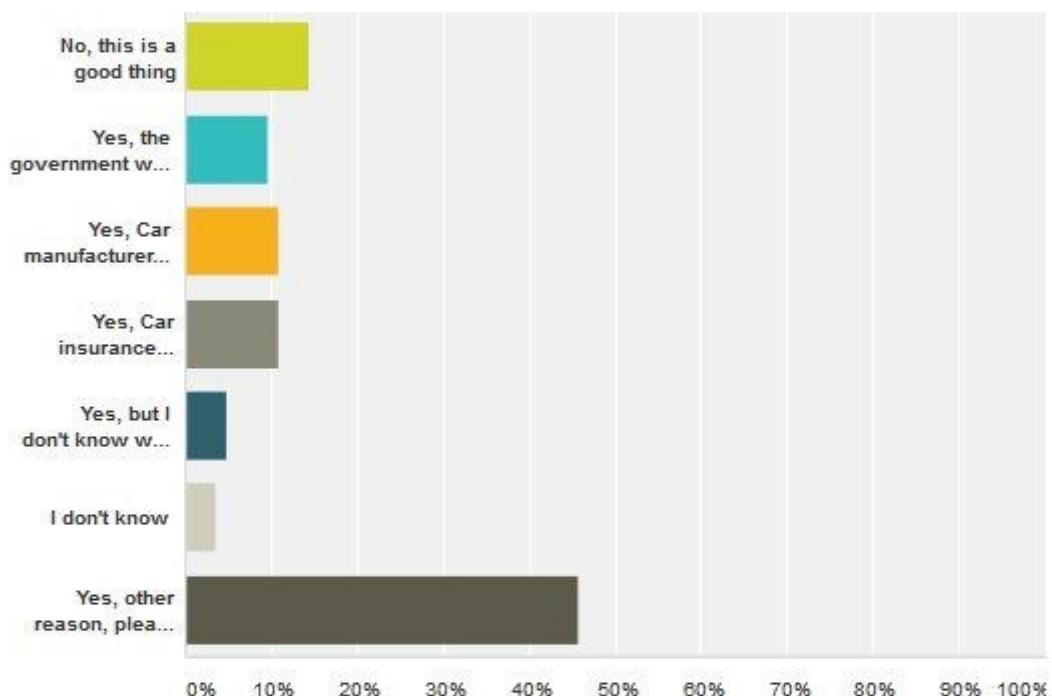


Antwoordkeuzen	Reacties	%
Hacker	24	28,57%
Car manufacturer	27	32,14%
Insurance company	7	8,33%
Car user	3	3,57%
Other, please specify ...	23	27,38%
Totaal	84	

3.6 E call (Emergency call of your car to the emergency services when your car is involved in a car accident) will be available in all new European cars from march 2018.

E-call is mandatory and signals accident data, your location and driving direction. Do you think there are security implications with the introduction of E-call in connected cars?

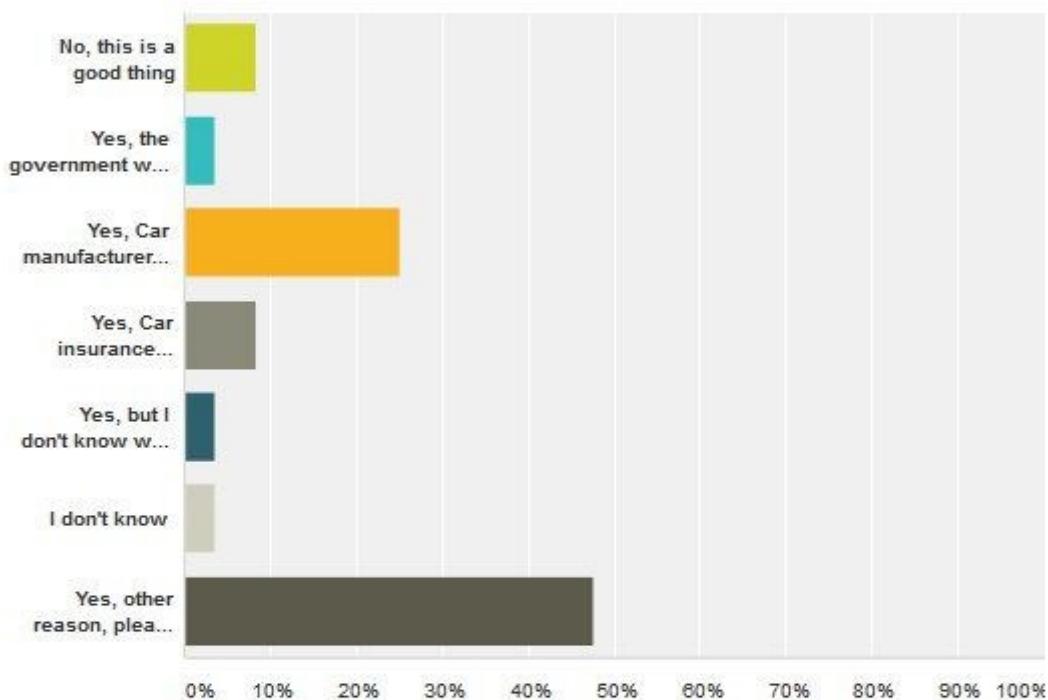
Beantwoord: 83 Overgeslagen: 1



Antwoordkeuzen	Reacties	%
No, this is a good thing	12	14,46%
Yes, the government will gather this data and can then track all movements of individual citizens	8	9,64%
Yes, Car manufacturers will gather this data and can then track all movements of individual customers. Misuse of this data for commercial purposes is a risk.	9	10,84%
Yes, Car insurance companies will gather this data and can then track all movements of individual customers. Misuse of this data for commercial purposes is a risk.	9	10,84%
Yes, but I don't know why. It just does not feel good.	4	4,82%
I don't know	3	3,61%
Yes, other reason, please specify ...	38	45,78%
Totaal	83	

3.7 B call (=Breakdown call when your car breaks down) will be available in some new European cars. B-call is optional and can be switched on or off by the car manufacturer. Do you think there are security implications with the introduction of B-call in connected cars?

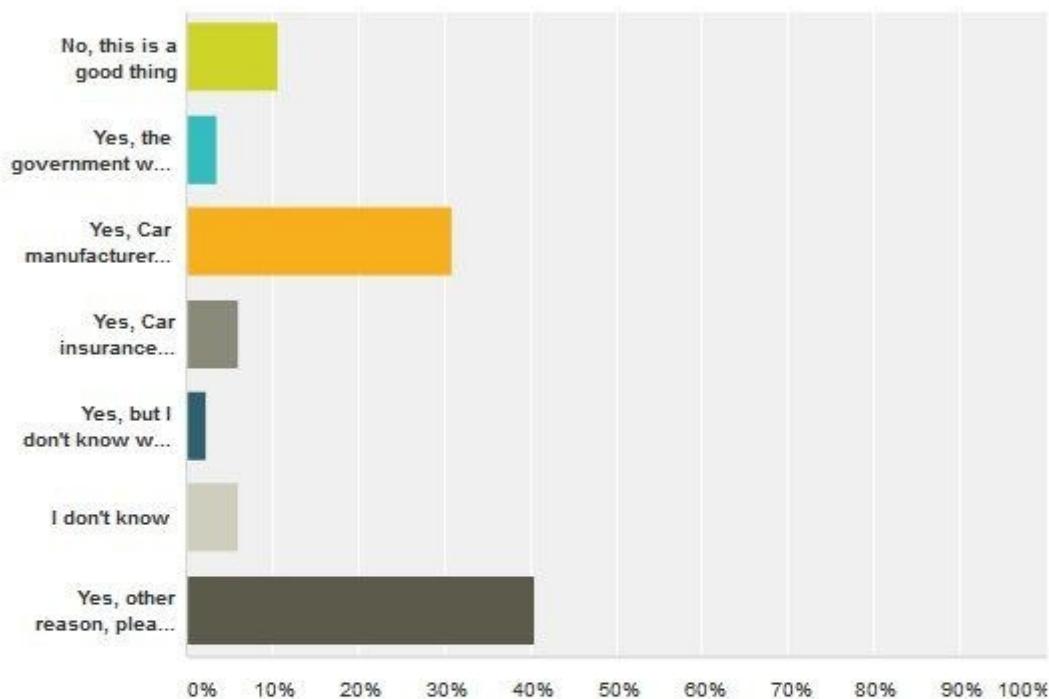
Beantwoord: 84 Overgeslagen: 0



Antwoordkeuzen	Reacties
No, this is a good thing	8,33% 7
Yes, the government will gather this data and can then track all movements of individual citizens	3,57% 3
Yes, Car manufacturers will gather this data and can then track all movements of individual customers. Misuse of this data for commercial purposes is a risk.	25,00% 21
Yes, Car insurance companies will gather this data and can then track all movements of individual customers. Misuse of this data for commercial purposes is a risk.	8,33% 7
Yes, but I don't know why. It just does not feel good.	3,57% 3
I don't know	3,57% 3
Yes, other reason, please specify ...	47,62% 40
Totaal	84

3.8 S call (=Service call when your car is scheduled for maintenance) will be available in some new European cars. S-call is optional and can be switched on or off by the car manufacturer. Do you think there are security implications with the introduction of S-call in connected cars?

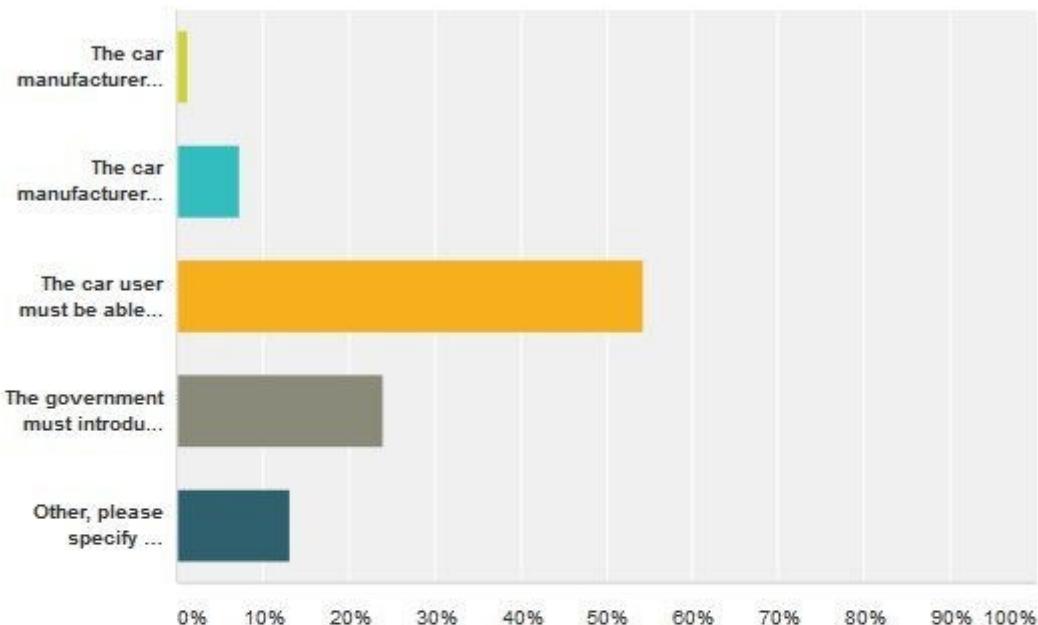
Beantwoord: 84 Overgeslagen: 0



Antwoordkeuzen	Reacties
No, this is a good thing	10,71% 9
Yes, the government will gather this data and can then track all movements of individual citizens	3,57% 3
Yes, Car manufacturers will gather this data and can then track all movements of individual customers. Misuse of this data for commercial purposes is a risk.	30,95% 26
Yes, Car insurance companies will gather this data and can then track all movements of individual customers. Misuse of this data for commercial purposes is a risk.	5,95% 5
Yes, but I don't know why. It just does not feel good.	2,38% 2
I don't know	5,95% 5
Yes, other reason, please specify ...	40,48% 34
Totaal	84

3.9 What, in your opinion, is the best solution to prevent security risks of the introduction of B call (car break down call) and S call (car service call for maintenance)?

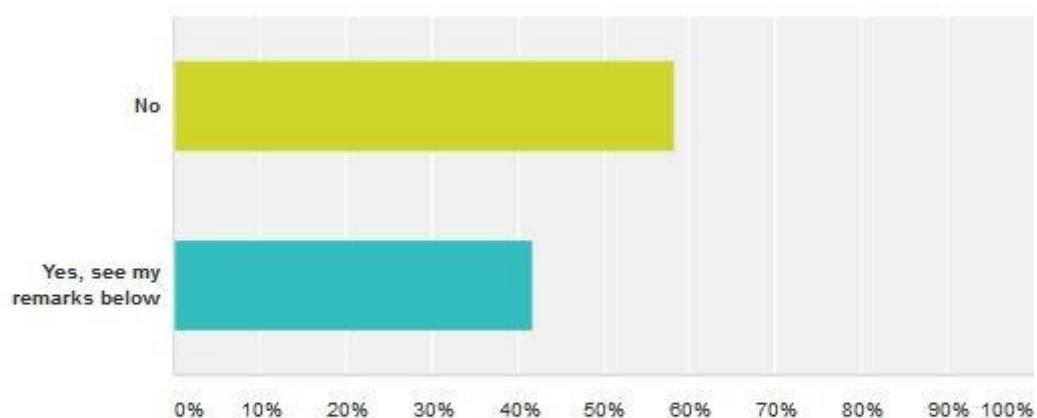
Beantwoord: 83 Overgeslagen: 1



Antwoordkeuzen	Reacties
The car manufacturer must choose the best option for the car user. Eg. When the car comes out of the factory all options for a maximum customer satisfaction allowed for that country are switched on.	1,20% 1
The car manufacturer must inform and choose the best option for the car user. Eg. The car manufacturer informs the customer in the showroom of the options and agrees which options to turn on or off.	7,23% 6
The car user must be able to switch these options on or off whenever he/she wants	54,22% 45
The government must introduce appropriate legislation to prevent misuse of this kind of data.	24,10% 20
Other, please specify ...	13,25% 11
Totaal	83

3.10 Do you have any other remarks on this subject that we missed in this survey?

Beantwoord: 84 Overgeslagen: 0



Antwoordkeuzen	Reacties	%
No	49	58,33%
Yes, see my remarks below	35	41,67%
Totaal	84	

Appendix 3: Requirements overview

This appendix shows an overview of all connected requirements. These requirements form the basis of the multi actor roadmap.

The roadmap requirements we derive from the analysis “Threat actors & awareness” are:

T1	The Dutch government must ensure that there is enough chance for the threat actor, or non-compliant to legislation automotive business, of being caught and brought to justice when a threat actors compromises the security of a connected car. This triggers the inhibitor factor “fear of capture”.
T2	As the previous chapter shows it is fairly easy to gain access to a connected car and compromise its security. The ease of access is also an amplifier for threat actors to hack a connected car. Improving the technical access barriers by encrypting the communication to and from the connected car is one element that will block this amplifier. The action for this lies with the network provider and the car manufacturer.
T3	Making it harder to break the security measures of the connected car will increase the cost of the attacker. An example of this is the implementation of segmentation in the connected car system design. This works as an inhibitor that blocks the amplifier “low cost of participation”. The action for this lies with the car manufacturer.
T4	In the communication and information campaign must send the message that tampering with a connected car endangers the lives of the people in that car. This will influence the public opinion that it is not ok to breach the security of connected cars. This will work as an inhibitor that blocks the amplifier “belief in sympathetic public opinion”. This communication and information action lies with all actors involved, car manufacturers, government, insurance companies, branch organisations, network providers.
T5	Splitting the CAN bus of the car into two separate systems (one for motor management and one for other systems like entertainment and navigation) makes it harder for an attacker to gain access to the motor management of the car. This triggers the inhibitor “high level of technical difficulty”.
T6	Annual cyber security threat awareness campaign by the government to educate the general Dutch public on cyber security issues.
T7	Each car manufacturers must implement and publish a responsible disclosure policy
T8	Car manufacturers must start a, preferably European, “hall of fame” for those ethical hackers that exposed cyber security vulnerabilities in connected cars and complied to the responsible disclosure policy.

Table 3 Requirements Threat actors

The roadmap requirements for the Car manufacturers we derive from the analysis are:

C1	Design a connected car architecture where the motor management systems are fully separated from the other car systems.
C2	Design at least four security zones into the system design. Example of these security zones: Red (the outer shell of the car facing the outside communication), Orange and Green (the data of the car user that should be protected). The Blue zone is the management interface for firmware updates etc.
C3	Use system redundancy into the car architecture design. Examples of this can be found in the aircraft industry.
C4	The car manufacturers cooperate with branch organisations, insurance companies and government in developing (international) standards on security requirements, communication and storage standards.
C5	Use detection systems to detect anomalies in the internal network of the connected car.

C6	In an autonomous car, the “intelligence” must decide on at least two out of three systems that agree that the chosen action is safe for the car user.
C7	Each connected car should be tested on security issues by the car manufacturer before market launch.
C8	Code review and proper “punishment” of developers that built in “Easter eggs”.
C9	Change of culture within the development department that Easter eggs in software code are not ok.
C10	Development and publishing of responsible disclosure agreement to ensure that external white hat hackers contribute to the connected car security and are not punished. (see Tesla example, appendix 5)
C11	The Car manufacturer limit the number of employees and third parties that have access to the stored data as much as possible. RBAC
C12	Clear and understandable communication to the end user on terminology, processes, security and use of the features the connected car contains. Example: the Tesla Autopilot case.

Table 4 Requirements Car manufacturers

The roadmap requirements for the Government we derive from the analysis are:

G1	Appropriate legislation on liability of connected cars & autonomous vehicles, platooning, privacy issues, insurance, driving licence, standards and security requirements.
G2	The government cooperates with branch organisations, insurance companies and car manufacturers in developing (international) standards on security requirements, communication and storage standards.
G3	See T6. Annual cyber security threat awareness campaign by the government to educate the general Dutch public and businesses on cyber security issues.
G4	The Car manufacturer limit the number of employees and third parties that have access to the stored data as much as possible. RBAC
G5	The government must answer fundamental questions with a huge business impact to guide the automotive industry. Examples are: Is the collected car data owned by the car owner (consumer) or by the car manufacturer? How long must the car manufacturer support security patches for the connected car. ²⁰⁶

Table 5 Requirements Government

The roadmap requirements for the Insurance companies we derive from the analysis are:

I1	The insurance companies log all cyber security incidents related to connected cars.
I2	The insurance companies do a trend analysis on the gathered data and share this with government policy makers.
I3	Insurance companies define and communicate a set of minimum security requirements a connected car must have.
I4	In case insurance companies collect data from connected cars: The Insurance companies use encryption in communication and storage.
I5	In case insurance companies collect data from connected cars: The entire chain of collected data by the insurance companies are audit proof.
I6	The insurance companies provide information to its customers on what data is stored, how long it is stored and who has access to that data.
I7	The insurance companies limit the number of employees and third parties that have access to the stored data as much as possible. RBAC ²⁰⁷ .
I8	The insurance companies cooperate with government, branch organisations and car manufacturers in developing (international) standards on security requirements, communication and storage standards.

²⁰⁶ See survey question 3.4

²⁰⁷ RBAC – Role based access control

I9	The insurance companies store the collected data as long as needed and as short as possible.
----	--

Table 6 Requirements Insurance companies

The roadmap requirements for the Branch organisations we derive from the analysis are:

B1	The branch organisation provides information and advice to its members
B2	The branch organisation uses encryption in communication and storage.
B3	The branch organisations cooperate with government, insurance companies and car manufacturers in developing (international) standards on security requirements, communication and storage standards.
B4	The branch organisations limit the number of employees and third parties that have access to the stored data as much as possible. RBAC
B5	Start an European Auto ISAC to share cyber security knowledge within the (European) automotive industry
B6	Organise an annual hacking challenge for connected and autonomous cars. This information can be used to improve the connected car designs.

Table 7 Requirements Branch organisations

The roadmap requirements for the Dutch Network providers we derive from the analysis are:

N1	The network provider provides access to the network (access) and ensures that the latest security patches for vulnerabilities are implemented.
N2	The network provider delivers enough bandwidth on the access network for the required data stream (capacity & availability)
N3	The network provider uses encryption in communication and storage. (confidentiality)
N4	The network provider uses agreed communication standards in order to ensure that the message is received by the data collector as required (ensure integrity of the message)
N5	The network provider provides a handover to another network of another country when the connected car leaves Dutch territory and drives into another country.
N6	The network provider informs its customers on the terms and conditions of the provided service within the boundaries of the law.
N7	Create, test and innovate new standards to standardise the network data traffic like on LTE V2X and ITS-G5 (802.11p)
N8	The network provider limit the number of employees and third parties that have access to the stored data as much as possible. RBAC

Table 9 Requirements Network providers

The roadmap requirements for the car Users / consumers we derive from the analysis are:

U1	Ask questions about car security to your connected car dealer. Example: Can you show to me how cyber secure this car is compared to other connected car brands? How do I obtain security patches for my connected car? How long do I get security patches and firmware updates for my connected car? Action by branch org, government, car manufacturer
U2	Ask branch organisations to investigate, compare and publish the results of cyber security penetration tests on different types of connected cars.
U3	Ask questions about car security to your representative in parliament. Example: What kind of protective legislation (e.g. liability and security) is there in place that protects me in my connected car? What does the government do to ensure that my connected car is and stays secure? What security requirements did the government impose on the car manufacturers to ensure that the connected car is cyber secure? Action of government to provide adequate answers and actions.
U4	Ask questions about car security to your insurance company Example: how many times is this type of car stolen or had security breaches? Can you publish the annual statistics on connected car brands on how many security hacks /

	breaches there were? Action of insurance companies to provide adequate answers and actions.
U5	Ask your insurance company to deliver what information / collected data is logged and stored about the user behaviour when using the car.
U6	Car manufacturers should make an uniform policy to patch the connected car software in a quick and secure way.
U7	The car users should be aware and informed not patch his own car via an uncontrolled USB device. Action by car manufacturers, government and branch organisations.
U8	Inform each of the 8 Mentality groups in an annual event about their expected behaviour regarding cyber security aspects of the connected car. Each group must be addressed separately in their own language within their own communication channels. Action by government, car manufacturers and branch organisations.

Table 10 Requirements Users

Appendix 4: Interview overview

The list of interviews:

	Company	Name	Date	Remark
1	Achmea	Geurts, P; Beveren, van J	2016-06-02, 2016-06-10	Leusden, Insurance company. Achmea is the largest car insurance company in the Netherlands
2	ANWB	Smith, F; Jong, de R	2016-06-07	Den Haag, Branch organisation
3	Bovag	Bresser, H; Kamps, E	2016-06-09	Bunnik, Branch organisation
4	BMW	Zijden, van der, B; Mason, A	2016-06-13	Rijswijk, Car manufacturer
5	Connekt	Juffermans, N	2016-06-29	Delft, Branch organisation
6	Deloitte	Blogg, H; Tilmans, B	2016-06-16	Amsterdam, Consultancy firm with a firm reputation on security issues.
7	NXP	Geraets, M	2016-07-21	Eindhoven, Chip manufacturer that creates chips (ECU) for (connected) cars.
8	PON Automotive	Kerkhof, M. van	2016-05-03, 2016-05-11	Leusden, Car manufacturer
9	RDW, Rijksdienst voor het wegverkeer	Doll, G	2016-05-19	Groningen, Government
10	SIMS - Standaardisatie- en Informatiebeleid MobiliteitsSector	Sombekke, J	2016-05-24	Hoevelaken, Branch organisation, cooperation between Bovag and RAI.
11	Stichting aanpak voertuigcriminaliteit	Visser, T	2016-05-12	Hoevelaken, Branch organisation
12	Stichting Verzekeringsbureau Voertuigcriminaliteit	Hoop, de A	2016-05-09	Apeldoorn, Branch organisation
13	TNO	Smulders, A	2016-05-03	Den Haag, Independent research company

Non responsive were: Volvo, HTCU, hacker GKG, researcher RV.

Appendix 5: Bug hunting program rewards

The bug hunting program by Tesla pays the following rewards as described on
<https://bugcrowd.com/tesla>

Tesla pays rewards ranging from \$100 to \$10,000.

The rewards are administered according to the following guidelines:

- XSS: \$200–\$500
- CSRF: \$100–\$500
- SQL: \$500–\$10,000
- Command injection: \$10,000
- Business logic issues: \$100–\$300
- Horizontal privilege escalation: \$500
- Vertical privilege escalation: \$500–\$10,000
- Forceful browsing/Insecure direct object references: \$100–\$500
- Security misconfiguration: Up to \$200
- Sensitive data exposure: Up to \$300
- Vehicle or product related vulnerabilities: case-by-case basis (report directly to vulnerability@teslamotors.com)

Tesla states that they support the open publication of security research. They do ask to wait before any publication so Tesla can do a final sync-up and check.