OULUN YLIOPISTO
UNIVERSITY of OULU

Security Threats from Connecting Mobile Phones to Connected Vehicles

University of Oulu
Faculty of Information Technology and Electrical Engineering / M3S
Bachelor's thesis
Benjamin Kämä
07.05.2020

Tiivistelmä

Tutkimus käsittelee turvallisuusuhkia, joita aiheutuu puhelimien yhdistämisestä autoihin. Uudet tekniset innovaatiot ja ohjelmiston kasvava rooli ovat tehneet moderneista autoista tietokoneiden kaltaisia. Ohjelmisto on mahdollistanut uusien ominaisuuksien lisäämisen autoihin. Lisäksi autoihin on lisätty myös uudenlaisia sensoreita. Nykyään autoihin voi yhdistää erilaisia käyttäjätilejä ja laitteita, minkä vuoksi autot keräävät käyttäjistään tietoa yhä enenevissä määrin. Autoihin on lisätty myös uudenlaista teknologiaa, jonka vuoksi autojen keräämät isot tietomäärät ovat saavutettavissa mistä tahansa maapallolla. Sen vuoksi olisikin tärkeä määrittää ovatko turvallisuus toimenpiteet pysyneet näiden uusien muutoksien mukana.

Tutkimus toteutettiin kirjallisuuskatsauksena. Materiaali tutkimusta varten kerättiin käyttämällä Google, Google Scholar ja Scopus hakukoneita. Lisäksi hakuja tehtiin myös IEEE Explore ja Web of Science sivustoilla, joita käytettiin myös paperien lataamiseen ResearchGate sivuston lisäksi. Materiaalia etsittiin myös jo valmiiksi valittujen julkaisujen lähdeluetteloista. Lähdemateriaaliksi valittiin aiheeseen relevantit julkaisut. Julkaisu valittiin mukaan tutkimukseen, jos sen aiheena oli joko autojen tieto- tai elektroninen turvallisuus, tai se käsitteli nimenomaan autojen ja puhelimien tai autojen ja jonkin muun yhteysteknologian turvallisuutta.

Autot suunniteltiin alun perin suljetuiksi järjestelmiksi, mistä aiheutuu turvallisuus uhkia moderneille yhteysteknologiaa sisältäville autoille. Tutkimuksessa uhkat jaettiin kolmeen eri kategoriaan. Ensimmäinen kategoria ovat puhelimet itse. Toinen kategoria on Bluetooth-yhteys, joka on pääasiallinen yhteystapa puhelimien ja autojen välillä. Kolmas kategoria on OBD-II-portti. Puhelimista aiheutuvat riskit tulevat niiden nopeasta tuotesyklistä ja lisäksi haittaohjelmat tulisi myös huomioida. Bluetooth riskit tulevat paritukseen ja löydettävyyteen liittyvistä ongelmista. On olemassa myös useita erilaisia Bluetooth hyökkäyksiä, jotka tulisi ottaa huomioon. OBD-II-porttiin liittyvät uhkat johtuvat siitä, että portista pääsee käsiksi autojen sisäiseen verkkoon. Uhkia aiheutuu myös OBD-II-portteihin liitettävistä lähettimistä ns. dongleista, joiden turvallisuusominaisuudet voivat pahimmassa tapauksessa olla olemattomia. Koska OBD-II-portista pääsee käsiksi autojen sisäiseen verkkoon, on näiden ongelmien korjaaminen äärimmäisen tärkeää.

Kaikki nämä kolme uhkakategoriaa voi mahdollistaa sen, että hyökkääjä saa auton järjestelmät täydellisesti haltuunsa. Ne voivat myös mahdollistaa informaation keräämistä autosta tai auton eri järjestelmien kuten telematiikan hallinnoimista. Voi olla jopa mahdollista, että hyökkääjää saa haltuunsa turvallisuuden kannalta kriittisiä järjestelmiä, kuten ohjaus- ja jarrutusjärjestelmät.

Tutkimuksen päämerkitys oli koota yhteen useita tutkimuksia, jotka osoittavat miksi puhelimien yhdistäminen yhteysteknologiaa sisältäviin autoihin sisältää uhkia, ja miksi nämä uhkat tulisi ottaa vakavasti. Tutkimus osoitti myös useita lähteitä sille kuinka isoja uhkia nämä voivat olla ja kuinka paljon hyökkääjät voivat saada autoa ja sen dataa hallintaansa.

Avainsanat

älyauto, turvallisuus, matkapuhelin, tavaroiden internet

Ohjaaja

FT, yliopistonlehtori Raija Halonen

Abstract

Technical innovations and constantly expanding role of software has made modern cars more like computers than ever before. Software has introduced new features to cars. With the addition of new features, also new sensors have been added as well. Together with connecting user accounts and devices to the vehicle, vehicles have started to gather more and more information on their users. New connective technology has made cars more connected than ever. The large amounts of information that cars now collect can be accessed from all over the globe with the use of internet. It should now be carefully determined whether safety and security measures have kept pace with the influx of these new changes.

This research was done as a literary review. Relevant material was collected by using search engines Google, Google Scholar and Scopus. IEEE Explore and Web of Science were used for searching for papers as well as for downloading them. ResearchGate was used for downloading the papers as well. Papers were also chosen by finding relevant papers from already chosen papers' list of references. Papers were selected based on their relevance to the topic. Papers that were on the topic of vehicle information or electronic security or specifically about vehicle security regarding connections with mobile phones or other connective technology were selected.

Cars were originally designed to be closed systems. There are technical weaknesses stemming from this original design idea, that now create holes in the security of connected vehicles. This research divided these threat categories to three parts. The first category is phones themselves. The second one is the threats that come from the main connection between phones and cars which is Bluetooth. The third category is the OBD-II port. Risks from phones come from the relatively fast product cycle they have. Malware also should be taken into consideration. Bluetooth risks come from pairing issues and discoverability, and there are several types of Bluetooth attacks that should be taken into consideration. The threats from OBD-II ports come from the access it gives to the internal network of the vehicle. Problems also rise from the way OBD-II port dongles are designed, as in the worst case their security features can be abysmal. Together with the access that the port provides, it should be critical to correct this issue.

All of these threat categories could enable attackers to gain complete access to the vehicle's systems. They can also collect information from the vehicle or control the vehicle's different systems like telematics unit, or even go as far as controlling the safety critical systems like steering and braking.

The main contribution of this research was presenting several studies that demonstrated reasons why the threat from connecting phones to connected vehicles is real and should be taken very seriously. A valuable contribution was also in showing several sources together on how serious these threats can be and how much control of the vehicle and its data attackers can achieve.

Keywords

connected cars, smart vehicles, security, mobile phones, IoT

Supervisor

PhD, University Lecturer Raija Halonen

Contents

1. Introduction

The automotive industry has faced a massive change with the introduction of Electronic Computer Units (ECU) and further connective technology into passenger vehicles, which are hereafter referred to as cars. Software together with hardware changes has made it possible to bring new functionalities into modern cars. On the other hand, software is at the heart of the difficulties facing the auto industry. (Broy, Krüger, Pretschner & Salzman, 2007) With the increase in connectivity has come an increase in potential threats and security risks. There are now multiple different ways cars collect information on their drivers and passengers, and hacking such a car can have severe consequences. (Ellison, Lacy, Maher, Nagao, Poonegar & Shamoon, 2012.) In recent years the technology has also made it possible to connect your mobile phone to your car further increasing the connective possibilities (Broy et al., 2007). Connecting new devices brings out new attack surfaces (Dardanelli et al., 2013). Thus, it is important to recognize what are all the possible security ramifications that come from this increased connectivity.

Modern cars' electrical systems are run by ECUs. Originally ECUs were connected only to their own sensors and actuators via bus systems, but later these systems evolved to connect several ECUs together. (Broy et al., 2007.) One of the bus technologies in use is the Controller Area Network (CAN) bus (Jakob, Kremer, Schulze, Grossmann, Menz, Schneider & Vouffo Feudjio, 2012).

Initially cars were designed to be closed systems (Bécsi, Aradi & Gáspár, 2015). Modern cars have several different connective technologies in them (Oancea and Simion, 2018; Koscher et al., 2010; Han, Divya Potluri & Shin, 2013; Bécsi et al., 2015). According to Han, Divya Potluri and Shin (2013) new cars can be called connected vehicles precisely because they can communicate with devices outside of their own network.

Problems arise when you connect other devices like phones to these systems, because as Jakob et al. (2012) wrote, the technical design of these bus systems, like the CAN bus, does not provide any security features at all. As CAN buses provide access between ECUs, (Broy et al., 2007; Jakob et al., 2012) it is understandably an enormous risk, if an out of the network device will be able to access the CAN bus. Zhang, Antunes and Aggarwal (2014) went so far as to state that OBD-II or On-Board Diagnostics ports give practically anyone access to the ECUs of the vehicle. As ECUs communicate through the CAN network, there are other ways to access these internal networks besides only OBD-II port, like some user-upgradable parts on vehicles or devices using for example Bluetooth technology (Koscher et al., 2010).

Several of the connective technology present in modern day cars can thus be viewed as an entry point for an attack (Oancea and Simion, 2018). A mobile phone can be a way to introduce malicious code to the vehicle (Zhang, Antunes & Aggarwal, 2014). What remains to be explored is what are all the possible security threats that can come from connecting phones to connected cars. This research aimed to examine the question what security threats arise from connecting mobile phones to connected cars.

Research methods used were searches made using several different search word combinations on search engines Google, Google Scholar and Scopus. IEEE Explore and Web of Science were used for searching papers and together with ResearchGate they were also used for downloading papers. Additional sources were found by searching the reference lists of previously found papers.

Paper selection criteria was their relevance to either vehicle information or electronic security in general or specifically about vehicle security regarding connectivity with mobile phones or connective technology in general.

The main contribution of this research was that the security threats posed by connecting phones to connected cars are real and that they can have devastating consequences. Mainly these threats concentrate on the how cars were initially designed to be closed systems and how phones break that system, what threats can come from Bluetooth connection, and the threat that come from OBD-II port connection which can give attackers access to the internal networks of the car. Because of the construction of e.g. the bus systems in modern cars, access to the car an eventually lead to attacker having access even to the safety critical systems.

First previous literature published on the subject was examined. It was followed by details of the used research methods used in this research. After the used research methods, the results of this research were discussed. Finally, conclusions were drawn from the results.

2. Prior research

Here follows prior research made on the topic, beginning with terminology on the subject followed by brief history and overview of current electrical systems of cars. Lastly different connective technologies were explored.

2.1. Terminology

To define security in general Whitman and Mattord (2012, s. 8) referred to Merriam Webster's dictionary. According to Merriam Webster security is "the quality or state of being free" where being free means being free from e.g. danger, fear or anxiety (Security, 2019). Whitman and Mattord wrote about security of organizations and they expanded security to consist of physical, personnel, operations, communications, network and information security. Their definition of physical, communications, network and information security can be applied to connected car security as well. Physical security according to the authors is protecting "--physical items, objects or areas from unauthorized access and misuse." Communications security was defined as protecting "—communications media, technology and contents". Network security protects "networking communications media, technology and content". According to the authors information security is about securing the confidentiality, integrity, and availability of information. Duri et al. (2002) seem to agree when they cited Russell and Gangemi (1991) on how security can be thought to encompass confidentiality or secrecy which includes privacy, integrity, and availability of information. Later they stated that privacy comes from individuals own ability to make decisions on what happens to the information collected about them. Bello, Mariani, Mubeen and Saponara (2019) agreed with the other authors when talking about secure by design in-vehicle networks, that data integrity and availability should be ensured. They also discussed the need for confidentiality and authentication.

Whitman and Mattord (2012, s. 11) defined threat as omnipresent "--objects, persons, or other entities that present a danger to an assets." Threats hence endanger the continuity of security of these assets. The threats surrounding connected cars can endanger both the safety of the vehicles themselves, but also the people and objects in and around them.

Another relevant term on the topic is vulnerability. Whitman and Mattord (2012, s. 11) defined it as "[a weakness] or a fault in a system or protection mechanism that opens it to attack or damage." These vulnerabilities can be exploited to realize threats in the form of attacks. An attack can come for example in the form of malware, which are according to Zhang et al. (2014) software that can be created to for example disrupt the computers, or in the case of connected cars, the attack can target functions or access information illegitimately. Different types of malware and the threats they pose to connected cars will be examined later in this research.

Han et al. (2013) considered vehicles connected when there is communication with an outside of the network device either through a wired or wireless interface or communication. This connection can be made either with trusted or untrusted entities. According to Broy, Krüger, Pretschner and Salzman (2007) a phone can be such a device and connecting a phone to a car transforms the car into an information and communication hub. Smart car is also a relevant term. Hubaux, Capkun and Jun Luo (2004) considered cars to be smart, if their capabilities include among other things processing capabilities and if they are capable of running security protocols wirelessly.

Oka, Furue, Langenhop and Nishimura (2014) stated that with all the connective technology modern cars have, they are “mobile IoT devices”. In addition to new technologies built into cars, software has also had an influence in making cars more complex, because like Broy et al. (2007) stated, because of software cars now have functionalities that were impossible to have just two decades ago.

2.2. Brief history and overview of modern automotive electrical systems

Car electronic systems consist of subsystems governed by embedded computers called Electronic Control Units or ECUs. Example ECUs for different subsystems are Engine Management System and Anti-lock Braking System. (What is an ECU?, 2019.) In addition to movement related functions ECUs control also for example systems relating to safety, like the airbags, or the in-cabin entertainment systems (CAN bus explained – A simple intro, 2019).

ECUs were originally called Engine Control Units. They were first introduced to cars in the 70s because of the California Clean Air Act and rising gas prices. They managed oxygen and fuel balance to moderate the amount of pollutants released. (Koscher et al., 2010.) Initially ECUs worked in isolation on specific tasks (Broy et al., 2007). More powerful ECUs were introduced in the middle of the 90s, for example with UNIX like environments, and in modern vehicles they have spread everywhere (Koscher et al., 2010). According to Shaout, Colella and Awad (2011) modern ECUs can handle such complex tasks as Advanced Driver Assistance Systems with functions such as Adaptive Cruise Control.

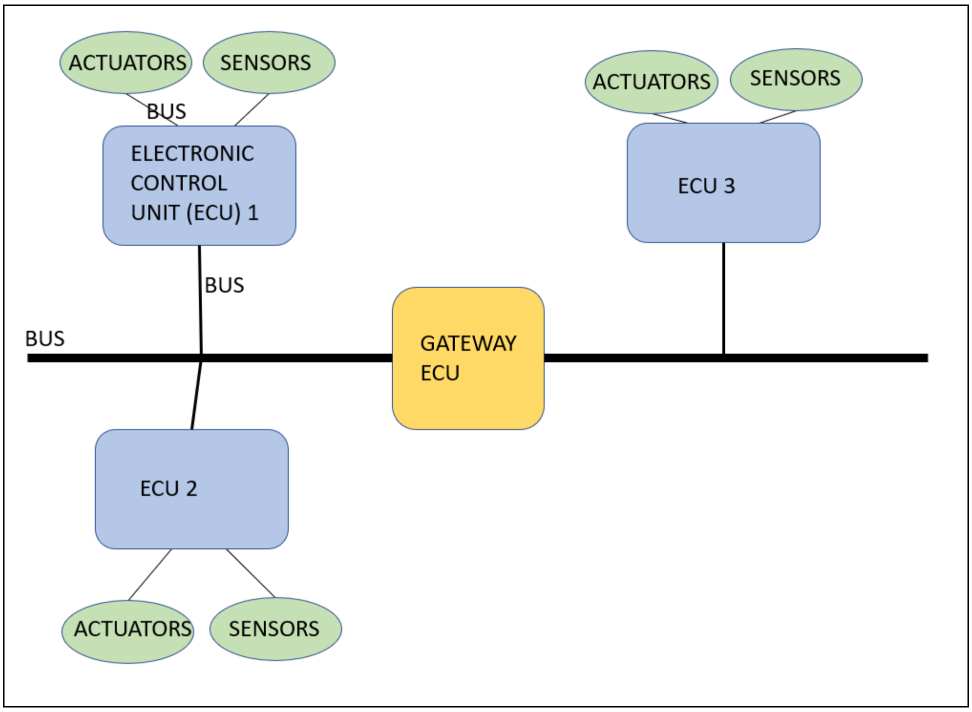

Figure 1. How electronic control units, actuators and sensors work together (Broy et al., 2007; Bates, 2014, s. 263-297; Huybrechts, Vanommeslaeghe, Blontrock, Van Barel, & Hellinckx, 2018).

As is illustrated in Figure 1 ECUs do not function by themselves, but they can have different types of sensors or actuators connected to them (Broy et al., 2007; Bates, 2014,

s. 263-297). Actuators enact ECUs electronic commands and they can be for example electronic motors or valves (Actuators, 2019). Sensors in cars sense different variables from their environment and then transmit these values electronically to the ECU. Examples of sensors are speed sensors, which can be used e.g. for sensing wheel speeds, and temperature sensors used e.g. for measuring the temperature of the engine oil. (Sensors, 2019.)

Bus systems enable communication between ECUs, sensors, and actuators (Broy et al., 2007; Bates, 2014, s. 263-297) as is seen above in Figure 1 where buses connect ECUs to each other and sensors and actuators to ECUs. Initially bus systems were introduced only for communication between ECUs and their sensors and actuators. Later they evolved into connecting different ECUs together to enable communication between them. (Broy et al., 2007.) In modern vehicles there are several different bus systems. Examples of bus types are CAN (Controller Area Network), LIN (Local Interconnect Network) and MOST (Media Oriented Systems Transport). (Jakob et al., 2012) Kleberger, Olovsson and Jonsson (2011) also mentioned FlexRay. The authors continued, that these buses can be further connected via gateway ECUs. In Figure 1 you can see a gateway ECU connect ECU 1, 2 and 3 together (Kleberger et al., 2011; Huybrechts et al., 2018). Koscher et al. (2010) also stated, that there can be different types of buses, like high-speed and low-speed buses, and they can be a part of different types of systems. Some of these systems can be safety-critical while others might be related to say the entertainment system. These systems however are often intertwined, because of the need for communication. Thus, there might be no clear separation between them, even though there might be a difference in terms of e.g. how safety-critical they are. (Koscher et al., 2010.)

CAN buses were developed in the 80's by Bosch as an inexpensive wired transmissions network (Glavin & Morgan, 2004). They are used by devices with interfaces like the dashboard or the infotainment unit (Han et al., 2013). CAN bus supports "publish-and-subscribe communications model" where every packet sent contains the ID header for its packet type, and all of the connected nodes receive the packet and then are able to decide whether to process the packet or not (Koscher et al., 2010.). Several different ECUs can accept the same packet (Han et al., 2013).

2.3. Connectivity

Initially cars were designed as closed systems (Bécsi et al., 2015). Modern cars on the other hand have several different types of connective technology in them. Oancea and Simion (2018) introduced three different attack surfaces that present different connection types to the modern connected vehicle. The first category given was short-range wireless access. Examples of this given by the authors were Bluetooth, RFID tags and remote keyless entry. The second category of attack surfaces was long-range wireless and their example of this was the telematics control unit. The third given category was physical access.

Koscher et al. (2010) also presented different classes for cars' I/O capabilities. They divided these to three categories. The first is indirect physical access, the second is short-range wireless access and the third one is long-range wireless access. The examples of indirect physical access Koscher et al. gave were connecting chargers, USBs, discs, or iPods. Another such example was connecting a laptop to a scanning tool which connects to the car's OBD-II port. OBD-II port was the connection type here. Their examples for short-range wireless were Bluetooth, remote keyless entry and RFID tags which were similar to the examples Oancea and Simion gave, although Koscher et al. mentioned RFID technology specifically as RFID car keys. They also mentioned WiFi, Tire Pressure Monitoring System (TPMS) and a new technology called Dedicated Short-Range Communications (DSRC) standard used for communication between different cars to avoid dangerous situations on the roads. Examples given by the authors on long-range wireless access were broadcast channels, like satellite and digital radio, and addressable channels that connect to the telematics system and provide cellular and data connection to the car. They also mentioned GPS but did not consider it as an avenue for attack.

The possibility of connecting other devices to cars was also noted by Han et al. (2013). They divided these connection types to wireless and wired connection. Their examples of wireless connections were Bluetooth and WiFi. Wired connection requires physical access, so this category is similar to the third category by Oancea and Simion. USB and OBD-II port were presented as examples of a wired connection type.

Bécsi, Aradi and Gáspár (2015) also presented wireless technology connecting phones and cars. They mentioned Bluetooth and WiFi like other authors have done, but they also mentioned NFC or Near Field Communication, which uses RFID technology, (NFC, 2019) and two other technologies not supported by most phone manufacturers called IrDA and ZigBee.

Other possible wired connections not mentioned by any of the authors are for example memory cards and 3.5 mm headphone jack[1].

2.4. More on OBD-II port

According to Koscher et al. (2010) OBD-II port is a physically accessible port present in most modern cars, partly because it is federally required to be present in American cars. OBD-II port connects directly to the internal network of the vehicle (Koscher et al., 2010.). Hence, it can be used by mechanics or hobbyists connecting devices for diagnostics purposes, for instance for checking error codes given by the car (Edelstein, 2017). According to Cheah, Bryans, Fowler and Shaikh (2017) it is possible to connect physical dongles to the port, and then connect your phone or a laptop to the dongle. They mentioned that there is no encryption on the data available from this port and there is no access control either.

2.5. Connecting mobile phones to cars

Mobile phones are usually connected for infotainment and safety reasons, for example to use the hands-free function or the sound system of the car (Zhang et al., 2014). Several of the connective technology mentioned earlier can be used to connect phones to cars, either directly like via Bluetooth (Bécsi et al., 2015) or USB-cable where Koscher et al. (2010) and Han et al. (2013) stated that modern cars have USB capabilities, or indirectly like via OBD-II port dongle that is inserted into the port and the phone connects to it with Bluetooth (Oka, Furue, Langenhop & Nishimura, 2014.).

[1] Infotainment. (n.d.) Retrieved 17.04.2020 from https://webspecial.volkswagen.de/vwinfotainment/int/en/index/infotainment-systems#/?detail=0d222804-fa14-4843-b38f-21e6fdff9dca

2.6. Bluetooth

According to Bécsi et al. (2015) Bluetooth dominates as the most used connection method when it comes to connecting mobile phones to cars. Glavin and Morgan (2014) discussed Bluetooth. It is a short-range, cheap, but low powered cable replacement technology that works in the 2.4GHz band. It uses Fast Frequency Hopping Spread Spectrum (FHSS), where there are 1600 hops per second over maximum of 79 channels. FHSS provides some security function, because the connecting device must know the sequence being used to gain access. A challenge-response scheme is then used to check for a PIN code when pairing with another device. (Glavin & Morgan, 2004.) In a Bluetooth layer communication is then enabled after pairing (Dardanelli et al., 2013).

3. Research methods

The material for this research was collected using various search engines and databases. The most used search engines were Google, Google Scholar and Scopus. Web of Science and IEEE Explore were also used, primarily together with ResearchGate for downloading source papers. Relevant research material was also identified by examining the reference lists of already found papers.

The search words used were “car security”, “car software security”, “vehicle software security”, “software security risks”, “car software security threat”, “smart car”, “car security mobile phones”, “connecting phones to cars”, “Bluetooth security cars”, “Bluetooth security vehicles” and “smart car security mobile phones”.’ General search words like “car security” gave too many search results, and they had to be narrowed down with addition of further specifying search words. For example, in Scopus adding the word “software” to the search word “car security” reduced hits to about a tenth of the initial amount of hits. Adding the word “phones” again further cut the amount of hits to about a tenth of the previous amount.

The criteria for selecting relevant material were that the paper was either about car information or electronic security in general, or that it was about car information or electronic security and specifically about connectivity either with mobile phones or connective technology in general for example about Bluetooth.

The aim was to find out how specifically connecting mobile phones can endanger smart car security and as a result put humans, vehicles, and their surroundings in danger. Specifically, the aim was to find out what causes these threats and how they were manifested.

4. Results

As Ellison, Lacy, Maher, Nagao, Poonegar and Shamoon (2012) stated, modern cars have turned into collectors of our personal data, and if such a vehicle would get hacked, the consequences could be most severe. Their statement is from an information standpoint only, but Kleberger et al. (2011) stated how in-vehicle networks are safety critical and if there were any issues with safety, the consequences could be most severe. This refers not just to information security, but the health and wellbeing of the people in and outside of the car. Thus, the security threats that can come from connecting phones to connected cars should be taken very seriously.

Checkoway et al. (2011) assessed how realistic these threats are to cars. They considered two cases, the first one being theft and the second one being surveillance. They were able to conclude that it is possible to steal a car by remotely disabling safety measures of the car, and by then having someone drive the car away. They tested this method and were successful. They also were able to find out that it is possible to record sounds from the in-cabin microphone via a compromised telematics unit, hence surveillance is also a credible threat. Han et al. (2013) on the other hand mentioned three different possible attack scenarios for connected vehicles. The first one was a compromised user device, which could for example be a mobile phone. The second was a case where the gateway is compromised, and the third was when both the user device and the gateway are compromised.

Phones can be connected to cars for a variety of reasons, like Oka et al. (2014) stated, it is possible to connect phones to e.g. the car's stereos or even read information from the vehicle like what is the engine speed. The goal for the attackers could be to gain access and steal this information, for example to steal financial or location information, call logs, habits of the driver etc. (Ellison et al., 2012; Zhang et al., 2014.). They might even gain access to audio from the car cabin (Ellison et al., 2012.) or get the car's GPS location (Oka et al., 2014). A goal could be that they might want to control and/or steal the vehicle or access the system's monitors, safety functions or "long distance communication channels" (Ellison et al., 2012).

4.1. Challenges

Like Ellison et al. (2012) stated, attackers do not need access to the car's cabin or for them to be near the car anymore. They refer to Checkoway et al. (2011) when they stated that it is now possible to mount an attack via the internet, or first gain access to the car and later use this access to do further damage via the internet. According to them, it is even possible to attack specific types of vehicles, and all of this is because modern cars are not designed as "externally networked IT systems".

As stated earlier, phones break the closed system of cars, (Bécsi et al., 2015.) which has obvious security implications. The issue with phones stem from a variety of problems, some because of phones themselves and others caused by the car systems, like as mentioned earlier that they were not designed for this. According to Bécsi et al. (2015) the phone product cycle is much faster than it is for cars. They also cited Shewale et al. (2014) when they stated that since phones are continuously under development there is a constant influx of new security threats. They also stated that the absence of upgrades causes this to be a very serious issue, and eventually updates for older systems will stop entirely, hence newer problems will not be fixed. They also mentioned that there is a lack of motivation in keeping phones secure. They even went as far as to state that "[m]obile security in general is very worrisome." Here they gave examples such as the threat from downloaded applications, text messages, internet browsers etc. Other security issues they mentioned were possible attacks through the permission system of phones or the kernel, the problems jailbreaking phones can initiate, and that phones are ideal targets for spoofing. It is even possible that the phone connecting to the car might not be the owners, but according to the authors it might even belong to some service or a third-party user, like in the case of car sharing. All in all they stated that "--mobile devices will always be the most vulnerable points of this communication chain in our opinion."

4.2. Security issues affecting the whole automotive industry

As Dardanelli et al. (2013) stated, all cars are designed primarily safety not security in mind. In this research this was understood to mean that the automotive industry is more concerned with for example physical safety like in the case of attempted theft or car crashes, than for instance information security. Dardanelli et al. added that this makes it difficult to add security mechanism to vehicles.

Checkoway et al. (2011) raised another typical issue for the automotive industry. There has been a lot of outsourcing in the industry and manufacturers also keep the knowledge about the code to themselves. This according to the authors leads to manufacturers using a lot of glue code to make the parts work together, which might not always be ideal. Checkoway et al. stated that this practice of outsourcing without sharing code is no longer appropriate when it comes to digital systems that can be compromised remotely. Gelles, Tabuchi and Dolan (2015) in their New York Times article raised the possibility of beginning to publish source code as a solution for security issues in modern cars.

In general, it is challenging to create software for the automotive industry, as Broy et al. (2007) described, because the requirements for automotive software are for it to work with low memory and power, thus it needs to be closely tuned to the processor and closely optimized as well. They stated that it makes it difficult to make changes to the code later as the code can be complex. It is also difficult to reuse the code and the optimization itself can cause bugs as well.

4.3. Security issues from connecting phones with Bluetooth

According to Bécsi et al. (2015) it is possible to connect phones to cars for example with Bluetooth or using WiFi, but that Bluetooth is the dominating connection type. The authors stated that when "basic protected pairing modes" are used, Bluetooth is not very easily hackable. However according to them WiFi or WiFi Direct would be more secure, as Bluetooth is easier to hack than either of these two technologies. Bécsi et al. did however state, that you cannot rely on the security technology inherent in these technologies as the ultimate protection.

Bluetooth has its own issues though. Oka et al. (2014) stated that Bluetooth devices are desirable attack targets because of the damage they can do and because there are pairing issues with Bluetooth. Glavin and Morgan (2004) discussed the issue of discoverability with Bluetooth devices, because it can be used to gain information for a following attack. Cheah et al. (2017) also stated that when devices are in discoverable mode, it is possible for attackers to sniff information like the Bluetooth address of the device. They also stated that if the device is discoverable for instance for a minute, this increases the likelihood of an attack. They talked about war-nibling where they used a device to monitor relevant Bluetooth devices. If the device is discoverable, you can find the Bluetooth address as mentioned earlier, but also find for example Bluetooth alias, class of device or Bluetooth service profiles. If the device was hidden, you would have to already know its Bluetooth address and do an active probe, but according to the authors when they were driving while war-nibbling, it was too short of a time frame to use this method. (Cheah, Bryans, Fowler & Shaikh, 2017.)

Three of the devices Cheah et al. (2017) found while war-nibling were specifically named "OBDII" which according to the authors means that they directly connected to the OBD-II port and had access to the internal network of the car. This as mentioned earlier, can have devastating consequences if it is a way to gain unauthorized access. The authors also mentioned, that if a device name is visible, it is possible to search online for the manual of the device and gain more information about it, like for example if there is a default PIN code. Checkoway et al. (2011) also stated that it is possible to brute force a PIN code in about 10 hours.

According to Dardanelli et al. (2013) the versions of Bluetooth using secure simple pairing (SSP) protocol have security issues because of weak cryptographic primitives. They also mentioned that most Bluetooth applications rely on static unchangeable PINs. Oka et al. (2014) also stated that earlier devices with Bluetooth had implementation errors. According to Cheah et al. (2017) there is also lag in Bluetooth adoption, so that newer versions might not be adopted as fast as they should.

Cheah et al. (2017) listed several different Bluetooth attacks that were adapted from J. P. Dunning's "Taming the blue beast: A survey of Bluetooth based threats". The attacks they mentioned were obfuscation, fuzzing, sniffing, Denial of Service (DoS), malware, unauthorized direct data access and man-in-the-middle attack. Glavin and Morgan (2004) also mentioned possible attack types. The attacks they mentioned were cypher attack, Bluejacking, Bluesnarfing and backdoor attack. Oka et al. (2014) also described how it is possible to gain access to the car's in-vehicle network by exploiting the Bluetooth stack in the car. According to the authors it would then be possible to "inject commands such as unlocking the doors".

Checkoway et al. (2011) did practical attack tests on vehicles. They were able to gain access to the telematics ECU's operating system, where they found what program handled Bluetooth. They were able to eventually find weaknesses that meant that all already paired Bluetooth devices could eventually "execute arbitrary code on the telematics unit." They assumed that attackers could compromise an already paired mobile device. They further investigated this and used a Trojan Horse application that spied for telematics units, and when it found one, it sent the authors' payload to it. The authors stated that there have already been other Trojan applications uploaded to the Android Marketplace. Android Marketplace is currently known as Google's Play store. Thus, they concluded that "smartphones can be a viable path for exploiting a car's short-range wireless Bluetooth vulnerabilities." They also explored a scenario, where an attacker did not already have a paired phone, where they used Bluesniffing to find the vehicle's Bluetooth MAC address and they were able to brute force the pairing PIN. After this they stated that an attacker could proceed as with the previous example and inject the malicious code.

4.4. Security issues stemming from OBD-II port and dongles

According to Cheah et al. (2017) the data available from OBD-II ports is not encrypted. There is also no access control. All but one of the OBD-II dongles they saw broadcasted their address immediately after connecting to an OBD-II port, which could be useful for attackers. They also discovered that the cheaper dongles used legacy pairing and the PIN code seemed to almost always be 1234. (Cheah et al., 2017.) A pin like that is very easily guessable.

Oka et al. (2014) found in their survey where they also examined OBD-II dongles, that the majority of the dongles examined had fixed unchangeable PIN codes with codes '0000', '1234' or '6789', and the discoverable mode was always on. According to the authors, if the device is always discoverable, the attacker could just send a pairing request. They could also guess the PIN. The problem with OBD-II ports and dongles is that phones can be connected to the port, with a suitable app via Bluetooth, and then gain direct access to the in-vehicle network. It would be possible for them to then to inject messages to the CAN network. (Oka et al., 2014.)

Koscher et al. (2010) connected a laptop to their test vehicle's OBD-II port. They then controlled the laptop remotely. They were able to attack the car so that they gained control of the engine, brakes, and various other units of the vehicle, even when the vehicle was running. They also were able to make packages cross from low-speed bus to high-speed bus. They successfully reprogrammed the telematics unit from a different device connected to the low-speed bus to act as a bridge between the different bus systems. They concluded that devices that can be connected to the low-speed bus can be used to "influence the operation of safety critical components." It should be noted here that it is also possible to connect phones directly to telematics units e.g. via Bluetooth (Checkoway et al. (2011).

4.5. Connecting phones to the infotainment unit

Oancea and Simion (2018) stated that the infotainment unit is the most important physical access entry point in a vehicle, because it is user friendly, and it is possible to connect components to it e.g. via USB, Bluetooth or WiFi. They also stated that should an attacker gain access to the unit, it would be even possible for them to influence functions like steering or braking. According to Checkoway et al. (2011) it is possible to use special WMA songs to gain full access to the vehicles CAN network. Since it is possible to play songs from a phone on the car's sound system by connecting phones to the infotainment unit[2], using music files can be another way to attack the vehicle.

4.6. The threat of malware

Zhang et al. (2014) stated that it is possible to get a malware from e.g. smartphones that could then be connected to the vehicle. According to the authors it is also possible to get them from downloaded files, applications, or e-mail attachments. Possible different malware types that they listed were viruses, worms, Trojan Horses, spyware, ransomware, and rootkit. According to the authors it is also possible for the malware to modify itself to change its appearance at replication. According to the authors because

[2] Antuan Goodwin. (2010). Step 1: Initiate paring on your car's stereo. Retrieved 09.04.2020 from https://www.cnet.com/roadshow/pictures/bluetooth-pairing-your-car-stereo-and-android-phone/

of the interconnectedness of systems, if one system is compromised, other systems are too. Their example of this was a DoS attack on other subsystems.

Oancea and Simion (2018) also mentioned the threat of malware and specifically ransomware and mining-attacks. According to the authors, mining-attacks could face for example resource restrictions because of the cars' constricted environment. They also mentioned it is possible to distribute malware via phones. After the device gets connected to the car it looks for its target ECU e.g. the infotainment unit. Here the path is from infected device, to the gateway ECU and finally the target ECU. It then could reach back to the attacker who designed the malware for instructions or begin giving orders to the target ECU via the bus system. Oancea and Simion gave an example of the effects of ransomware, where it would be possible for the malware to gain control of the steering and lock the steering wheel until a ransom is paid.

5. Discussion

It became clear during this research that the consequences for security issues can be very grave. As Kleberger et al. (2011) stated, the in-vehicle network should be protected. The attackers might aim to steal information from the car, or to gain control of the vehicle or its functions, or even to steal the car itself (Ellison et al., 2012; Zhang et al., 2014.). It is also possible that the attackers first gain information with various ways, but later perform the attack via internet without having in-cabin access (Checkoway et al., 2011).

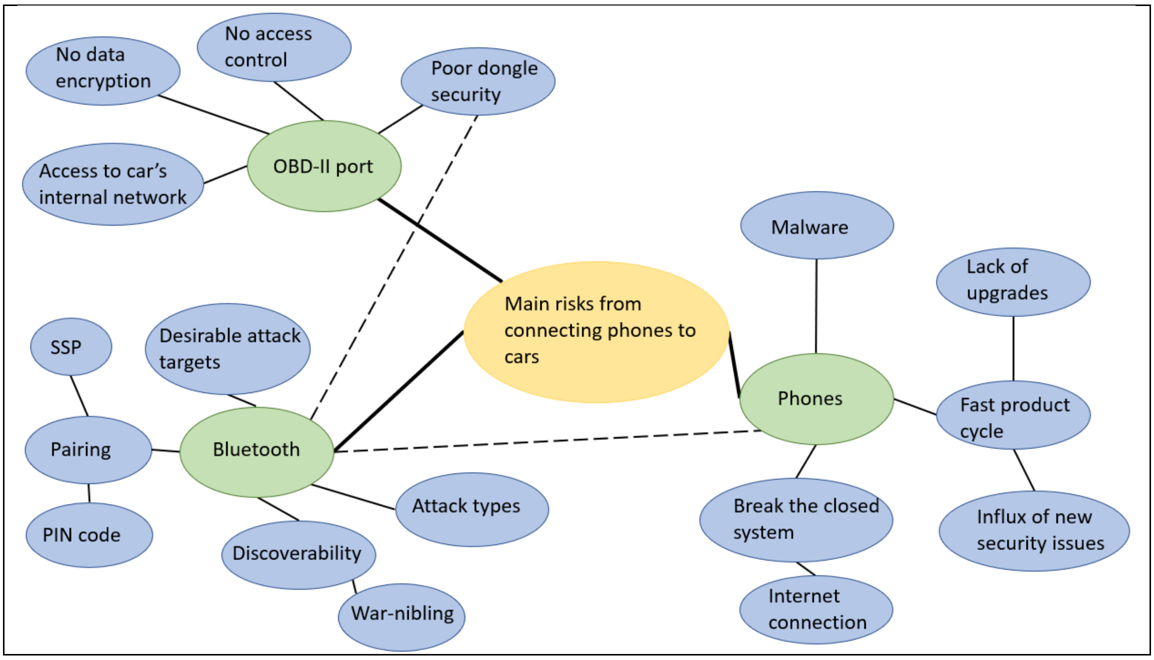

Figure 2. Main risks from connecting phones to cars.

The mains risks that come from connecting phones to cars can be divided into three main groups as can be seen in Figure 2. The first one is phones themselves, the second one is Bluetooth and the third category is OBD-II ports. The security of phones is very concerning to Bécsi et al. (2015). They break the closed system of cars and they can introduce threats a variety of different sources like applications, text messages or enable attacks through the permission system of the phones (Bécsi et al., 2015.). According to Checkoway et al. (2011) it is possible to attack cars via the internet. As modern-day mobile phones come equipped with internet connection, it should be further researched if connecting phones with internet to cars could enable the possibility of an attack mounted via the internet. It is also possible to download malicious software to phones via the internet like from the Google's Play store (Checkoway et al., 2011) hence the connection in Figure 2 between breaking the closed system of cars and internet connection. The problem with phones comes also partly from the nature of their quick product cycle. Because there is constant product development, there is also constant influx of new security threats, and as older systems might not get updated, these newer problems might remain unsolved. (Bécsi et al., 2015.)

As can be seen in Figure 2, malware is also connected to phones. According to Zhang et al. (2014) malware from phones can also be a possible threat to the car. Zhang et al. also stated that because of the interconnectedness of the whole system, if one system gets compromised, other systems are compromised as well. Malware can come from different sources like downloaded files or applications and there are several different types like for example viruses or Trojan horses (Zhang et al. (2014). Checkoway et al. (2011) for example used a Trojan horse with their successful practical attack test to attack the telematics unit of a car. Oancea and Simion (2018) agree it is possible to distribute malware like ransomware via phones, although they could face resource constrictions because of cars' constricted resources. Oancea and Simion also mention it is possible that the malware could contact the attack for instructions or target ECUs via the bus system. Oancea and Simion give an example of malware's potential as it can for instance lock the steering wheel and hold it to ransom.

As Bluetooth is the dominating connection type between phones and cars (Bécsi et al., 2015) it is the second major category of risks that come from connecting phones to cars. Hence the dotted line connecting phones and Bluetooth in Figure 2. The findings on Bluetooth and the vulnerabilities related to it were considerable. Oka et al. (2014) stated that Bluetooth devices are desirable targets, partly because of the damage that can be done if the attack is successful. This is true for cars as well as was demonstrated by Checkoway et al. (2011) who were able to gain access to a vehicle by using a Bluetooth device. As mentioned earlier the attackers might aim to steal information from the car or the car itself, or to gain control of the vehicle (Ellison et al., 2012; Zhang et al., 2014.) where the possibility of damage might be high hence making cars desirable targets.

The most serious findings were done by Checkoway et al. (2011) who did practical attack testing on vehicles. In Figure 2 pairing is connected to Bluetooth, because pairing is required for communication when using Bluetooth (Dardanelli et al., 2013) and while pairing with another device a PIN code is checked (Glavin & Morgan, 2004.). Checkoway et al. were able to gain access to the vehicle first by using an already paired Bluetooth device and a Trojan Horse application to spy on telematics units. Eventually they were able to send the payload to the car. They also tested an unpaired version of the attack, where they eventually were able to brute force a pairing PIN after which they could proceed with the attack as with an already paired device. PIN codes are also troubling because according to Dardanelli et al. (2013) most Bluetooth applications use static unchangeable PINs. In Figure 1 SSP or secure simple pairing is also a matter to be considered a threat, because according to Dardanelli et al. (2013) the versions of Bluetooth who are using this protocol have had security issues.

When considering Bluetooth related security threats discoverable mode should also be considered, as according to both Glavin and Morgan (2004) and Cheah et al. (2017) it can be used for example to gather information to use in further attacks. Cheah et al. did war-nibling where they used a device to monitor relevant Bluetooth devices and according to them if the device is discoverable, you can find the Bluetooth address, Bluetooth alias, class of device or Bluetooth service profiles. Hiding the device would mean that, attackers would have to already know its Bluetooth address and do an active probe, but there was not enough time for this while war-nibbling. (Cheah et al., 2017.)

The final issue considering Bluetooth in Figure 2 is attack types. There are several different attack types that can be used for Bluetooth attacks, like Denial of Service attacks or malware, that Cheah et al. (2017) adapted from J. P. Dunning's book. Glavin and Morgan (2004) also mentioned different attack types, like Bluesnarfing, which is defined according to Techopedia as action that allows hackers to gain access to information to the device's data[3]. According to Oka et al. (2014) it is possible to gain

[3] Bluesnarfing. (2013). Retrieved 30.04.2020 from https://www.techopedia.com/definition/5046/bluesnarfing

access to the car’s in-vehicle network by exploiting the Bluetooth stack in the car and then be possible to “inject commands such as unlocking the doors”.

The third major risk category illustrated in Figure 2 is OBD-II port. The reason why OBD-II port should be considered a major security threat for car safety is because it directly connects to the internal network of the car (Koscher et al., 2010.). Koscher et al. (2010) demonstrated well how devastating OBD-II port connection can be, when they were able to attack cars via OBD-II port with a laptop. They were able to control and brakes etc. even when the vehicle was running. They also were able to reprogram the telematics unit to act as a bridge between different bus systems, which led them to conclude that devices that can be connected to the low-speed bus can be used to “influence the operation of safety critical components.” It should be noted that this finding also relates heavily to the earlier finding of Checkoway et al. (2011) where they were able to successfully attack the telematics unit with and without already paired devices. Attackers could now potentially use either an unpaired or paired phone to connect to the telematics unit via Bluetooth, then attack the unit and at the same time gain access to the different bus systems of the vehicle. (Checkoway et al., 2011.) Oancea and Simion (2018) stated that should an attacker gain access to the telematics unit, it could be possible for them to influence e.g. the steering.

OBD-II port is also dangerous, because there is no access control and no data encryption (Cheah et al., 2017). According to Cheah et al. (2017) OBD-II port devices are “the most dangerous” precisely because if pairing is successful, then the attacker has now access to the car’s internal network. OBD-II port dongles are devices that are connected to the OBD-II port (Cheah et al., 2017). Cheah et al. presented a real-world threat assessment scenario where these dongles were connected to vehicles and the laptops or phones were connected to the dongles via Bluetooth. The dongles Cheah et al. inspected had numerous security weaknesses. For instance, they used easily guessable PINs. Cheah et al. had investigated different Bluetooth devices, including OBD-II port dongles and according to them several of the devices broadcasted their name which makes it possible to e.g. search for the default PIN online and use it to gain access to the internal network of the car. Even if they would not be able to find a default PIN from a manual, Checkoway et al. (2011) were able to brute force a PIN in about 10 hours. Oka et al. (2014) also found that the dongles they examined had fixed unchangeable codes, and the codes seemed to be very easily guessable. The seriousness of these faults comes from the fact that like Oka et al. stated, it is possible to connect phones to these dongles via Bluetooth using certain applications. These phones would then have direct access to the car’s in-vehicle network, and they could inject messages to the CAN network. (Oka et al., 2014.) The connection seen in Figure 2 between poor dongle security and Bluetooth is because as Oka et al. stated, Bluetooth can be used as a connection method when connecting phones to these dongles. Security issues concerning Bluetooth should then be evaluated as well, like for example Cheah et al. did when they checked the discoverable window the devices had, or like their and Oka et al. findings on for example PIN code security issues.

Besides these three major categories there were other security issues that contribute to the threats that come from connecting phones to cars. There are such as the car industry’s focus on safety over security (Dardanelli et al., 2013.), the rampant outsourcing without sharing code which leads to the use of glue code (Checkoway et al., 2011.), and there are also hardware constraints like power constraints on software development (Broy et al., 2007).

In summary the security threat that comes from connecting mobile phones to connected cars can be categorized in three ways: the threats from phones, the threats from the

Bluetooth connection and threats relating to the OBD-II port. Phones are a threat because they break the closed system of cars (Bécsi et al., 2015.), they are a potential source for malware (Zhang et al., 2014) and there are security issues stemming from the fast product cycle of phones (Shewale et al, 2014, as cited by Bécsi et al., 2015). It is also possible that the phone connected to the car might not be the car owner's phone, but instead the attacker's or a 3rd party user's phone (Bécsi et al., 2015). The security issues that stem from Bluetooth relate to pairing (Oka et al., 2014; Dardanelli et al., 2013) like issues with PIN codes (Cheah et al., 2017; Dardanelli et al., 2013). Discoverability can also be an issue (Glavin and Morgan, 2004). There are several attack types that relate to Bluetooth that should be considered (Cheah et al., 2017; Glavin and Morgan, 2004). The threats from OBD-II were severe, because it grants access to the in-vehicle network (Oka et al., 2014.) and for example Koscher et al. (2010) did successful attack testing with OBD-II port access.

The results showed that the consequences for attacks like these could be very serious. All three of these categories connect to each other as it is possible to connect phones to OBD-II port dongles via Bluetooth (Oka et al., 2014.) because Bluetooth is the dominating connection method between phones and cars (Bécsi et al., 2015). All of these could contribute to the attacker's gaining access and control of for example the vehicle itself or information considering it.

6. Conclusions

The conclusions of this research were that the risks that come from connecting phones to connected cars are realistic and can be devastating. The risks centered mainly on phones breaking the closed system of cars like with the introduction of malware from the phones, the problems with Bluetooth connection and the risks that OBD-II port connection can introduce. Attackers can gain entry to the in-vehicle network and take control of the vehicle and its systems, or access data from the vehicle with potentially disastrous consequences.

Limitations of the study were that since this was a literary review only, the information is only as current as the sources. It would have given a more current and possibly a more detailed or realistic picture of the whole topic, if there would have been direct information gathering on for example attacks that connected cars have faced in the recent years. Limitations also include that the knowledge on Bluetooth does not include information on the latest Bluetooth technologies. A considerable limiting factor in this research was that the limited number of phone specific studies done.

Recommendations for future research are that solutions should be found on how to minimize the risks that come from mobile phones breaking the closed system of cars, for example how to prevent the introduction of malware into the car’s system. Issues considering Bluetooth specific to car industry should possibly be investigated as well. It could also be beneficial to do future research on how to address the poor security of OBD-II port and the dongles that can be connected to it, specifically how to possibly restrict unauthorized access to the cars’ in-vehicle network.

List of References

Actuators. (n.d.) Retrieved August 15, 2019 from https://www.my-cardictionary.com/electronics/actuators.html

Bates, M. (2014). *Interfacing PIC Microcontrollers (2nd edition).* Oxford: Newnes.

Bécsi, T., Aradi, S. & Gáspár, P. (2015). Security Issues and Vulnerabilities in Connected Car Systems. doi:10.1109/MTITS.2015.7223297

Bello, L. L., Mariani, R., Mubeen, S. & Saponara, S. (2019). Recent Advances and Trends in On-Board Embedded and Networked Automotive Systems. doi:10.1109/TII.2018.2879544

Broy, M., Krüger, I. H., Pretschner, A. & Salzmann, C. (2007). Engineering Automotive Software. doi:10.1109/JPROC.2006.888386

CAN bus explained - A simple intro (2019). (n.d.) Retrieved July 31, 2019 from https://www.csselectronics.com/screen/page/simple-intro-to-can-bus/language/en

Cheah, M., Bryans, J., Fowler, D. S. & Shaikh, S. A. (2017). Threat Intelligence for Bluetooth-enabled Systems with Automotive Applications: An Empirical Study. doi:10.1109/DSN-W.2017.22

Checkoway, S., McCoy, D., Anderson, D., Kantor, B., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F. & Kohno, T. (2011). Comprehensive Experimental Analyses of Automotive Attack Surfaces.

Dardanelli, A., Maggi, F., Tanelli, M., Zanero, S., Savaresi, S. M., Kochanek, R. & Holz, T. (2013). A Security Layer for Smartphone-to-Vehicle Communication Over Bluetooth. doi:10.1109/LES.2013.2264594

Duri, S., Gruteser, M., Liu, X., Moskowitz, P., Perez, R., Singh, M. & Tang, J.-M. (2002). Framework for security and privacy in automotive telematics.

Edelstein, S. (2017). From dongles to diagnostics, here's all you need to know about OBD/OBD-II. Retrieved July 31, 2019 from https://www.digitaltrends.com/cars/everything-you-need-to-know-about-obd-obdii/

Ellison, G. Lacy, J. Maher, D. P, Nagao, Y., Poonegar, A. D. & Shamoon T. G. (2012). The Car as an Internet-Enabled Device, or how to make Trusted Networked Cars. doi:10.1109/IEVC.2012.6183244

Gelles, D. &., Tabuchi, H. &., & Dolan, M. (2015, Sep 26,). Complex Car Software Becomes the Weak Spot Under the Hood. The New York Times. Retrieved from https://www.nytimes.com/2015/09/27/business/complex-car-software-becomes-the-weak-spot-under-the-hood.html

Glavin, M. & Morgan, F. (2004). A Review of Bluetooth Security In The Automotive Environment. doi:10.1049/cp:20040594

Han, K., Divya Potluri, S. & Shin, K. G. (2013). On Authentication in a Connected Vehicle: Secure Integration of Mobile Devices with Vehicular Networks.

Hubaux, J. P., Capkun, S. & Jun Luo. (2004). The Security and Privacy of Smart Vehicles. doi:10.1109/MSP.2004.26

Huybrechts, T., Vanommeslaeghe, Y. Blontrock, D., Van Barel, G. & Hellinckx, P. (2018). Automatic Reverse Engineering of CAN Bus Data Using Machine Learning Techniques. doi: 751-761. 10.1007/978-3-319-69835-9_71

Jakob, F., Kremer, W., Schulze, A., Grossmann, J., Menz, N., Schneider, M. & Vouffo Feudjio, A.-G. (2012). Risk-based Testing of Bluetooth Functionality in an Automotive Environment. *Lecture Notes in Informatics (LNI), Proceedings – Series of Gesellschaft fur Informatik (GI).*

Kleberger, P., Olovsson, T. & Jonsson, E. (2011). Security Aspects of the In-Vehicle Network in the Connected Car. doi:10.1109/IVS.2011.5940525

Koscher, K. Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S, . . . Savage, S. (2010). Experimental Security Analysis of a Modern Automobile. doi:10.1109/SP.2010.34

NFC. (n.d.) Retrieved August 19, 2019 from http://www.rfidlab.fi/rfid-teknologia/nfc/

Oancea, I. & Simion, E. (2018). Challenges in Automotive Security. doi:10.1109/ECAI.2018.8679052

Oka, D. K., Furue, T., Langenhop, L. & Nishimura T. (2014). Survey of Vehicle IoT Bluetooth Devices. doi:10.1109/SOCA.2014.20

Security. (n.d.) Retrieved August 14, 2019 from https://www.merriam-webster.com/dictionary/security

Sensors. (n.d.) Retrieved August 15, 2019 from https://www.my-cardictionary.com/electronics/sensors.html

Shaout, A., Colella, D. & Awad, S. (2011). Advanced Driver Assistance Systems - Past, Present and Future. *7th International Computer Engineering Conference*. doi: 10.1109/ICENCO.2011.6153935

Zhang, T., Antunes, H. & Aggarwal, S. (2014). Defending Connected Vehicles Against Malware: Challenges and a Solution Framework. doi:10.1109/JIOT.2014.2302386

What is an ECU? (n.d.) Retrieved August 15, 2019 from https://tekeye.uk/automotive/what-is-an-ecu

Whitman, M. E., Mattord, H. J. (2012). *Principles of Information Security.* Cengage Learning.