ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ

Ανάλυση Φορέων Απειλών στην Αυτόνομη Οδήγηση

Σπυρίδων Καμινιάρης

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων
Γεώργιος Σταμούλης

Επιστημ. Σύμβουλος
Κίκιρας Παναγιώτης

Λαμία, 2019

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

UNIVERSITY OF THESSALY

SCHOOL OF SCIENCE

INFORMATICS AND COMPUTATIONAL BIOMEDICINE

Threat Vector Analysis in Autonomous Driving

Spiridon Kaminiaris

Master thesis

Supervisor
Georgios Stamoulis

Scientific adviser
Panagiotis Kikiras

Lamia, 2019

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΔΙΑΤΜΗΜΑΤΙΚΟ ΜΕΤΑΠΤΥΧΙΑΚΟ ΠΡΟΓΡΑΜΜΑ ΠΛΗΡΟΦΟΡΙΚΗ ΚΑΙ ΥΠΟΛΟΓΙΣΤΙΚΗ ΒΙΟΙΑΤΡΙΚΗ
ΚΑΤΕΥΘΥΝΣΗ ……..

«ΠΛΗΡΟΦΟΡΙΚΗ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗΝ ΑΣΦΑΛΕΙΑ, ΔΙΑΧΕΙΡΙΣΗ ΜΕΓΑΛΟΥ ΟΓΚΟΥ ΔΕΔΟΜΕΝΩΝ ΚΑΙ ΠΡΟΣΟΜΟΙΩΣΗ»

Ανάλυση Φορέων Απειλών στην Αυτόνομη Οδήγηση

Σπυρίδων Καμινιάρης

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων
Γεώργιος Σταμούλης

Επιστημονικός Σύμβουλος
Παναγιώτης Κίκιρας

Λαμία, 2019

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

«Υπεύθυνη Δήλωση μη λογοκλοπής και ανάληψης προσωπικής ευθύνης»

Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, και γνωρίζοντας τις συνέπειες της λογοκλοπής, δηλώνω υπεύθυνα και ενυπογράφως ότι η παρούσα εργασία με τίτλο [«τίτλος εργασίας»] αποτελεί προϊόν αυστηρά προσωπικής εργασίας και όλες οι πηγές από τις οποίες χρησιμοποίησα δεδομένα, ιδέες, φράσεις, προτάσεις ή λέξεις, είτε επακριβώς (όπως υπάρχουν στο πρωτότυπο ή μεταφρασμένες) είτε με παράφραση, έχουν δηλωθεί κατάλληλα και ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής.

Ο/Η ΔΗΛΩΝ/-ΟΥΣΑ

Ημερομηνία

Υπογραφή

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

Ανάλυση Φορέων Απειλών στην Αυτόνομη Οδήγηση

Σπυρίδων Καμινιάρης

Τριμελής Επιτροπή:

Γεώργιος Σταμούλης, (επιβλέπων/σα)

Παναγιώτης Κίκιρας,

……, …….

Επιστημονικός Σύμβουλος:
Παναγιώτης Κίκιρας

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

Contents

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

1. Introduction

1.1. Automotive history

The word “automobile” comes via the French automobile from the Ancient Greek word “αυτός” (autos, "self") and the Latin word “mobilis” ("movable") meaning the vehicle that moves itself.

Since the inception of wheel and till the 1800s people used animals to move between long distances. Automobiles, in the form we know them today, were invented in the late 1800s. Modern autos were evolved from the steam powered vehicles, and were rooted in the development of the gasoline engine in the 1860s and 1870s in France and Germany. (QAD CEBOS, n.d.)
From this period to our days, there are a few milestones worth mentioning that define what we know today as a "car".

- First gasoline engine - In 1879, Karl Benz was granted a patent for his first engine, which has been designed in 1878. His 'Motorwagen", as it was called, was built in 1885 in Mannheim, Germany. At almost the same time in November 1881, French inventor Gustave Trouve demonstrated a working three-wheeled automobile powered by electricity at the International Exposition of Electricity in Paris. It is worth mentioning that after the first success of the gasoline engine, there was widespread experimentation with steam and electricity. For a brief period, the electric automobile actually enjoyed the greatest acceptance because it was quiet and easy to operate, but the limitations imposed by battery capacity proved to be competitively fatal. Especially popular with women, electric cars remained in limited production until well into the 1920s.

- First car: In 1890, Daimler and Maybach founded "Daimler Motoren Gesellschaft (DMG)" in Cannstatt and sold their first automobile in 1892 under the brand name Daimler, which was a modified horse-drawn stagecoach retrofitted with an engine.

- First mass production assembly line :The large-scale production line of affordable cars was debuted by Ransom Olds in 1902 but it was on October 1, 1908 that Henry Ford debuted the first production Model T Ford at the company’s Piquette Avenue plant in Detroit. Building a brand based on quality and affordability, the Model T appealed to a wide range of American consumers. From 1908 to 1927 Ford built some 15 million Model T cars making it the longest production run of any automobile model in history until the Volkswagen Beetle surpassed it in 1972.

- Materials of construction :Around 1914, car bodies were made of steel versus wood. Automotive manufacturer, Dodge, introduced their first vehicle to the market on November 14, 1914, which featured what was then a real novelty – an all steel body. Today, steel is used for making most car bodies.

- Automatic Transmission :in 1939, General Motors debuted “Hydra-Matic” – an automatic transmission using hydraulic fluid, which allowed vehicle gears to shift automatically during vehicle operation. This upgrade meant drivers could forego manual gear shifting. is one of the most important innovations in the history of the automobile.

- Air Conditioning : According to Automobile Magazine, in-car air conditioners came on the scene around 1940. The Packard was the first car to have it, and by 1969 more than half the cars

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

manufactured included A/C units. Today, more than 99 percent of all new cars are air-conditioned.

- Electronic Fuel Injection : 1966 was the year of the electronic fuel injection system. This milestone meant better fuel delivery to the car engine and improved engine efficiency and eliminated the need to pump your accelerator or pull a choke knob to get fuel to the engine. The 1967 Volkswagen 1600 was the first car to include the new technology from Bosch.

- Seat Belts : Safety became a major focus in automobile manufacturing in 1968. Government standards required car manufacturers to equip front seats with shoulder and lap seat belts and back seats with lap belts. The shoulder and lap belts became standard in front and rear seats over time.

- Airbags : The installation of airbags in cars became a manufacturing mandate for passenger cars due to a 1991 law, according to History.com. While major automotive manufacturers added air bags in the 1970s, the technology was improved and widely accepted in the late 1990s.

- Hybrids : While hybrid cars have a long history, these vehicles didn't become a commercial success in America until the late 1990s and early 2000s. Hybrid technology makes cars less dependent on gasoline and more environmentally friendly. Honda and Toyota are well-known for manufacturing award winning hybrid vehicles.

- Electric Cars: Electric cars firstly introduced in the 1800's and a large number of very early production vehicles were using electricity as their power source. Limitations in battery technology, and thus limited mileage, prevented them from wide adaptation. At the beginning of the 21st century, concerns over emissions from vehicles using hydrocarbon fuels and advancements in battery technology increased interest in the production of electric cars. Although costly at first, at the end of 2010's, prices of fully electric vehicles are starting to match those of diesel or gasoline powered ones, and many countries have announced that they will ban all sales of non zero- emission cars by 2030 or later. (Boffey, 2019)

- Autonomous cars: The latest milestone in automotive industry and subject of this study is autonomous driving and autonomous vehicles. Recent advancements in electronics and in automotive industry have allowed the production of cars that do not need a driver or any human intervention to operate. It is expected that adaptation of autonomous vehicles will be very slow and gradual, due to the complexity of the technology and the cost of production, but these will eventually replace human-driven cars in the not so distant future.

As we can see from the above mentioned milestones, automobile technology has made great advancements in almost a century, but those advancements were greatly around mechanics, electrics, safety and comfort. The way we use and operate our vehicles remained the same since the inception of the gasoline engine until the rise of autonomous cars that enable the operation of a vehicle even without the presence of a human on-board.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

1.2. Computers on Wheels

The first electronic control units (ECUs) entered mass-production in GM and Ford vehicles in the 1970s and their job was to handle basic functions such as ignition timing and transmission shifting as newly introduced tighter fuel economy and emission regulations commanded.
By the 1980s, more sophisticated computerized engine-management systems enabled the use of reliable electronic fuel-injection systems. These severely bettered performance in cars, as engineers were able to design more complex motors to take advantage of the ECU's abilities, while computer-controlled machine tooling were able to mass-produce them to the high tolerances necessary.
To the wide spread use of ECUs and their added functionality and complexity, we owe today the advent of active safety systems such as anti-lock braking, traction and skid-control, where wheel sensors trigger the vehicle's reaction to loss of grip. ECUs also migrated into active suspension control systems, allowing for instantaneous reaction to the car's changing position on the road and adapting to varying surfaces.
In the last decade or so, they've been linked to sonar, radar and laser emitters performing functions such as blind-spot and pedestrian collision warnings, automated breaking and safe distance-keeping via smart cruise control. Sensors also provide parking guidance and fully automated parking, with the aid of an on-board computer tied to brakes, steering and throttle. (MERTL, 2018)
The average car today can have between 25 and 100 central processing units (CPUs) controlling these functions and more, often networked but sometimes operating independently. The level of sophistication is likely to rise as self-driving vehicles move closer to mass production.
Steering, braking and throttle control on most new cars are electric drive-by-wire units, whose inputs are filtered through ECUs, sometimes to enhance the driving experience, other times to help keep drivers secure.
It took time to get drivers used to the idea of stomping the brakes on an ABS-equipped car instead of pumping them in an emergency. But the systems have become more subtle and the interventions often undetectable, to the point where a driver might put it down to their own skill behind the wheel.

As mentioned, the modern automobile may have as many as 70 electronic control units (ECU) for various subsystems. Typically, the biggest processor is the engine control unit. Others are used for transmission, airbags, antilock braking/ABS, cruise control, electric power steering, audio systems, power windows, doors, mirror adjustment, battery and recharging systems for hybrid/electric cars, etc. Some of these form independent subsystems, but communications among others are essential. A subsystem may need to control actuators or receive feedback from sensors. The CAN standard was devised to fill this need. The network of sensors and ECUs on a car are called CANbus and are used by most of the cars built from 1995 and after. A short explanation of how a CANBus network works will be helpful to understand later how fully automated cars work and can be exploited. CAN allows cars to be smarter, cheaper, and capable of performing difficult and incredibly complex calculations that otherwise could not be possible. One key advantage is that interconnection between different vehicle systems can allow a wide range of safety, economy and convenience features to be implemented using software alone - functionality which would add cost and complexity if such features were "hard wired" using traditional automotive electrics.

Before the addition of electronics in cars and the introduction of CANbus the only security concerns in a car had to do with the way a driver would react to a dangerous situation, the safety features of a car, and the road and weather conditions. But as with any other electronic device, and especially in this case that electronics control a moving vehicle at great speeds, security concerns arise. Electronics outside of industrial environments are prone to malfunctions and can be a stepdoor for individuals and their malicious activities. Since ECUs have replaced basic functions of a car, it would be very easy for an attacker to take control of these functions and put in great danger the driver and the car's passengers.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

ECUs and CANbus have been the target of various attacks taking advantage of security holes in the electronic devices themselves or the CANbus protocol. Some of these vulnerabilities will be discussed in a later chapter of our analysis, since these technologies are still being used and most likely continue to be used in “tomorrow’s” automobiles.

1.3. Autonomous Cars

1.3.1. Definition

Recent advancements in technology like ECUs, GPS satellites, AI, and various sensors have enabled car manufacturers to bring autonomous cars closer to reality. We have all seen movies or read novels about cars that drive themselves and people that ride them just enter their destination leaving the car do the rest. Today we call these vehicles "autonomous" and they rely on various technologies that we will analyze later.

According to wikipedia "autonomous" (also mentioned as a self-driving car or driverless car) is a vehicle that is capable of sensing its environment and navigating without “much” human input.
Autonomous cars combine a variety of techniques to perceive their surroundings, including radar, laser light, GPS, odometry and computer vision. Advanced control systems interpret sensory information to identify appropriate navigation paths, as well as obstacles and relevant signage.

The potential benefits of autonomous cars include reduced infrastructure costs by minimizing road signage, increased safety, increased mobility for elderly and disabled people, increased customer satisfaction, and reduced crime. These benefits also include a potentially significant reduction in traffic collisions, resulting injuries and related costs for medical care, and also less need for insurance. Automated cars are predicted to increase traffic flow (by avoiding congestion). They will relieve passengers from driving and navigation, provide lower energy consumption, significantly reduce needs for parking space, reduce crime, and facilitate new business models for people and goods transportation and as a service, especially via the sharing economy. (DEEMSOFT, n.d.)

1.3.2. Levels of autonomous driving

The road to create a fully autonomous car today is not easy and various obstacles, both technological and ethical, as long as the supporting infrastructure (roads, signage, etc) have to be overcomed. Based on the various functions of a car that can be automated, in 2014 the Society for Automotive Engineers (SAE) has created an international standard (J3016) that outlines 6 levels of automation for automakers, suppliers, and policymakers to use to classify a system’s sophistication.

These levels of automation are shown and defined by the J3016 standard as below:

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

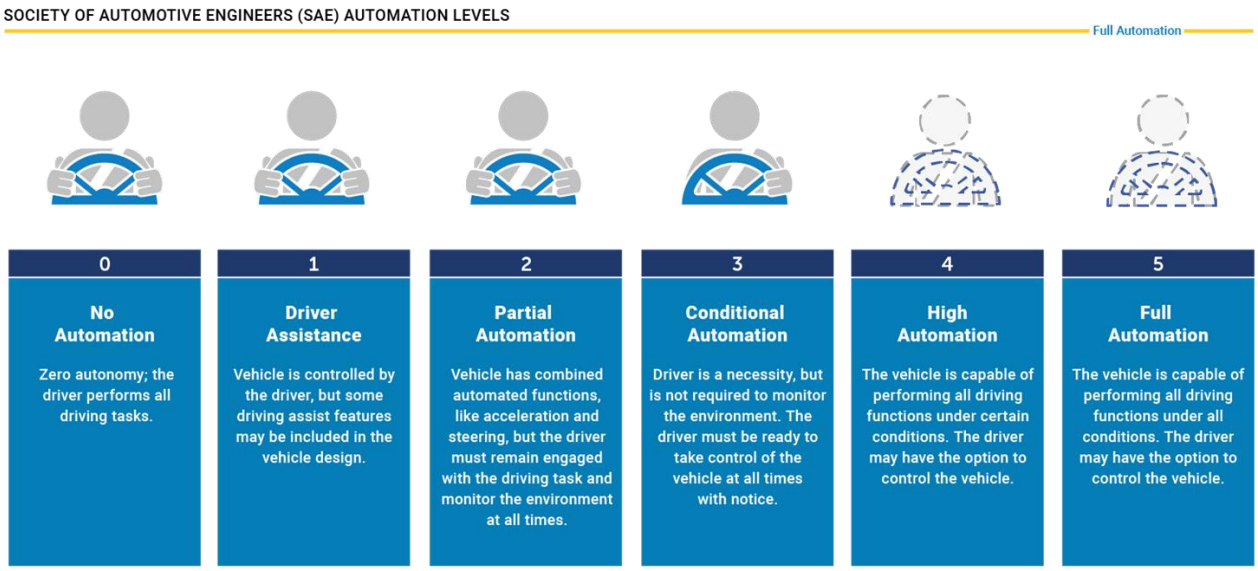


Figure 1.1: Automation levels (NHTSA, 2019)

SAE J3016 Definitions – Levels of Automation

SAE Level	Name	Narrative Definition	Execution of Steering/ Acceleration/ Deceleration	*Monitoring* of Driving Environment	Fallback Performance of *Dynamic Driving Task*	System Capability (*Driving Modes*)
Human driver monitors the driving environment						
0	No Automation	the full-time performance by the *human driver* of all aspects of the *dynamic driving task*, even when enhanced by warning or intervention systems	Human driver	Human driver	Human driver	n/a
1	Driver Assistance	the *driving mode*-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	Human driver and system	Human driver	Human driver	Some driving modes
2	Partial Automation	the *driving mode*-specific execution by one or more driver assistance systems of both steering and acceleration/deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	**System**	Human driver	Human driver	Some driving modes
Automated driving system ("system") monitors the driving environment						
3	Conditional Automation	the *driving mode*-specific performance by an *automated driving system* of all aspects of the *dynamic driving task* with the expectation that the *human driver* will respond appropriately to a *request to intervene*	System	**System**	Human driver	Some driving modes
4	High Automation	the *driving mode*-specific performance by an *automated driving system* of all aspects of the *dynamic driving task*, even if a *human driver* does not respond appropriately to a *request to intervene*	System	System	**System**	Some driving modes
5	Full Automation	the full-time performance by an *automated driving system* of all aspects of the *dynamic driving task* under all roadway and environmental conditions that can be managed by a *human driver*	System	System	System	**All driving modes**

© Copyright 2014 SAE

5

Figure 1.2: Definition of automation levels (SAE, 2018)

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

As we can imagine, cars on levels 3,4,5 and 6 that will be coming into production in the next few years, are also vulnerable to attacks since they are also using the same electronics and CANbus to communicate between ECUs. On the other hand, because autonomous cars rely more on technology and use more protocols and sensors to work and also require network connectivity to communicate to each other, are a lot more prone to attacks than cars on levels 0,1, and 2 that are in production and in use today.

These vulnerabilities and attack vectors will be the scope of this entire thesis.

1.4. Legislation and Ethics in autonomous driving

1.4.1. Legislation

Another major obstacle in making autonomous driving viable is legislation and to be more precise the lack of it. This situation affects the use of autonomous vehicles but also slows down testing.

Without government permits, testing self-driving cars on public roads is almost universally illegal. The Vienna Convention on Road Traffic, an international treaty that has regulated international road traffic since 1968, stipulates that a human driver must always remain fully in control of and responsible for the behavior of their vehicle in traffic.

Legislation needs also to be created addressing practical, legal and ethical questions and problems that arise from autonomous cars and driving.

Unlike with partially automated systems, which merely support the driver, such systems completely take over control of the vehicle. However, the driver must be ready to take over again if and when required. The new laws do not allow autonomous driving when all of the occupants are merely passengers. There is still a need for action at international level in this context.

New technologies also trigger new legal issues and this is no different in the case of automated and autonomous driving. In 2016 German government established an ethics commission to look at legal and ethical questions within the context of autonomous driving. In June 2017, the ethics commission adopted a final report comprising a total of 20 ethical rules, including the fact that protecting humans always takes priority. The ethics commission has also specified strict requirements in terms of data protection which are already taken into account today as part of the development of Daimler's automated and autonomous systems. In this process, three clear principles apply: transparency, self-determination, and data security. (German Federal Ministry of Transport and Digital Infrastructure - Ethics Commission, 2017)

Specifically, ethical rule 12 ensures that the public is entitled to be informed about new technologies and their deployment sufficiently, transparently and information should be publicly available and reviewed by professionally suitable independent body.

These ethical rules also suggest that lawmakers have to strike a balance between the data that are being collected and are essential for the functional safety of a vehicle, and informational self-determination. How much data will be disclosed to programmers or AI needs to be defined based on the principle that

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

the vehicle keepers and users are the owners of the vehicle data generated by its use, and they should decide if the data will be shared and forwarded or not.

American National Highway Traffic Safety Administration (NHTSA) has also issued guidelines for autonomous vehicles that include ethical considerations. (US National Highway Traffic Safety Administration, 2017)

Ethics discussions have also been developed and sustained by California Polytechnic State University and the Center for Automotive Research at Stanford. Google/Waymo and Ford have been active participants as well, and other autonomous vehicle manufacturers are joining in the discussion.

One other aspect of automated and autonomous driving is the question of liability in the event of an accident.

In Germany and some other countries, the legal situation is unclear as there is a three-pillar liability system in force involving drivers, owners and manufacturers. Drivers are responsible for driving and they must constantly monitor the vehicle when partially autonomous driving functions are active to intervene in serious cases. If drivers do not fulfill their duty of care and cause an accident as a result, they are liable for the resulting damage alongside the owner. Apart from this, manufacturers may be liable for damage caused by a product fault as part of product and manufacturer liability.

This combination of liability on behalf of drivers, owners, and manufacturers offers a balanced distribution of risk, ensures that victims are protected and has proven itself in practice. The liability model also provides a good foundation for new systems and the next stages in the development of autonomous driving. Autonomous driving has the potential to further improve safety on the roads and the flow of traffic, and it can therefore lead to an overall fall in the number of claims and liability cases.

As it was expected countries that their economy relies heavily in the motor industry or played a big role in the development of the car industry are the first to come up with and implement rules and laws about autonomous cars and driving.

European and North American countries such as the US, Germany, UK, and Netherlands were pioneers of self-driving vehicle licensing, and have introduced regulations for self-driving cars on public roads and issued autonomous testing permits. Asian countries quickly caught up and have been enacting similar legislation over the last three years. (Peng, 2018)

- **USA**: Each US State is responsible for its own autonomous driving legislation. In 2017, 33 states had either passed legislation, issued executive orders, or announced initiatives to accommodate self-driving vehicles on public roads.

  California is without a doubt the top-ranked state in openness and preparedness for autonomous vehicles. Autonomous vehicle testing regulations were introduced in California in September 2014 and required a driver to be in the vehicle, ready to assume control at any time. In 2018, California took a step forward and allowed fully autonomous vehicles with no driver to operate on its public roads.

  According to “Fortune” magazine, more than fifty self-driving companies are testing their technologies in California with Google’s Waymo and GM leading in autonomous miles logged. Waymo accumulated 352,545 autonomous public road miles (567,366 km) in the 12 months preceding November 2017, while GM vehicles drove 131,676 miles (211,912 km) in 2017. (Peng, 2018)

  Tesla uses a totally different approach. From October 2016 are equipped with Autopilot hardware kit 2.0 which consists of 8 cameras, radar and ultrasound but no Lidar. Tesla gathers data

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

collected from on-the-road fleet to train the AI and make it learn how humans drive and react to different situations.

Arizona has also removed obstacles to the deployment of autonomous vehicles, setting up and cultivating an AV-friendly testing environment that can now rival California's. In August 2015, Arizona Governor Doug Ducey signed an executive order directing agencies to "undertake any necessary steps to support the testing and operation of self-driving vehicles on public roads within Arizona." This March, Ducey updated the executive order and gave the green light for cars without drivers to operate on public roads in Arizona. There are now over 600 self-driving cars on the state's public roads. (Peng, 2018)

Florida, Michigan, and Pennsylvania, are also leaders in the accommodation of autonomous vehicles.

- **Europe**: Northern Europe does not get as much attention as the US as far as autonomous driving is concerned, but Netherlands and Sweden are investing on automated transport systems a lot more than any other European country.

  KPMG in 2018 published a report named "Autonomous Vehicles Readiness Index" that ranks 20 countries' preparedness for an autonomous vehicle future (figure 1.3). The Netherlands took the top spot, outperforming the US (7th) and China (16th). The Netherlands heavily-used and well-maintained road network was what stood out in the survey. The country has also already built almost 30,000 electric vehicle charging points and has high-quality wireless networks for transmitting data to and from autonomous vehicles.

  The Netherlands' Council of Ministers first approved autonomous vehicle road testing in 2015 and updated its legislation to allow tests without a driver. The Dutch government is spending €90 million in an effort to adapt more than 1,000 traffic lights to enable them to communicate with autonomous vehicles. (Peng, 2018)

  In 2016 the Netherlands launched the first driverless buses "WEpods" in a central Dutch city. The electric pod was originally designed by French vehicle manufacturer and robotic specialists EasyMile. It was developed for Citymobil2, an EU-funded project looking at automated road transport systems across urban Europe. These buses can hold six people and operate on fixed lanes across the city and have already been used in Finland and Switzerland in closed environments.

  Sweden is ranked 3rd in KPMG's 2018 report. In 2015 the Swedish government first explored self-driving vehicle testing, concluding that it was possible to carry out trials at all levels of automation on Swedish roads. The Road Transportation Authority can, as of July 2017, authorize permits and supervise trials in accordance with the law.

  In December 2017 Volvo launched its "Drive Me" project in Sweden, which provided self-driving cars to a number of people in Gothenburg for use in their everyday lives. The project is aimed at collecting user feedback to improve Volvo's technology.

  In November 2017, Volvo also signed a US$300 million deal with Uber to construct and provide 24,000 self-driving-ready Volvo XC90 SUVs.

  Germany has embraced autonomous vehicles as the German parliament passed a law last May that allows companies to begin testing self-driving cars on public roadways. Drivers are allowed to remove their hands from the wheel and perform simple tasks such as using smartphones while

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

the car drives itself. However, drivers are required to always be prepared to take control in case of emergencies.

This new legislation in Germany requires a black box, a data recorder for autonomous vehicles that works much like the black boxes on planes, and it is designed to record system data and actions for review in the likely event of accidents.

The UK also is progressive when it comes to autonomous vehicle policy and regulations. Most European countries adhere to Vienna Convention on Road Traffic, but the UK is not a signatory and so is believed to have an advantage in adopting legislation to attract autonomous vehicle manufacturers and tech startups. The UK government is aiming for a wide adoption of autonomous vehicles on its roads by 2021.

In 2013, UK's Department for Transport allowed semi-autonomous cars to operate on lightly-used rural and suburban roads. In 2018, the Queen herself spoke about the importance of enacting "new laws to make the UK ready to pioneer driverless cars."

In 2018, the UK government passed a bill to draw up liability and insurance policies related to autonomous vehicles.

- **Singapore**: Singapore certainly has the opportunity to be the first Asian country to widely adopt autonomous driving. The country has the world's third highest population density, and the government is under pressure to revamp the transportation system.

  KPMG's 2018 report (figure 1.3) gives Singapore the maximum score on policy and regulations related to autonomous vehicles. In July 2015, the Singapore Land Transport Authority (LTA) authorized 6 km of test routes and doubled the distance a year later. In 2017 the LTA expanded its autonomous vehicle test area to neighboring facilities such as the National University of Singapore, Singapore Science Parks 1 and 2, Dover and Buona Vista, and thus adding 55 kilometers to the existing autonomous vehicle trial infrastructure.

  In 2017, the Government of Singapore passed legislation recognizing that motor vehicles don't require a human driver and regulating the operation of such vehicles on public roads. This set of rules exclude autonomous vehicles and their operators from existing legislation that mandates that a human driver must be responsible for the safe use of a motor vehicle moving on the road.

  Singapore's supportive environment attracted Boston-based self-driving software company NuTonomy. NuTonomy, which was acquired by Delphi for US$450 million, launched a free trial autonomous taxi service in August 2016 and hopes to launch an autonomous taxi service in the city-state by the end of 2022. (Autocar, 2016)

- **China**: China has a lot of catch-up to do to become a regulation-friendly country for autonomous driving. Although many prominent autonomous driving companies such as Baidu Apollo, JingChi.ai, and Pony.ai have their headquarters in China, the country got off to a slow start with legislation and permits.

  But things are slowly changing now, especially in big cities. Early in 2018 Shanghai issued its first self-driving licenses, that allows two automakers to test their autonomous vehicles on public roads. These tests are limited to a 5.6 km stretch of public road in the city's Jiading District. Shanghai is China's first Smart Network and Autonomous Driving Pilot City.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

In January 2018, the Beijing Municipal Traffic Commission announced that the city's first autonomous driving test track will be built in Yizhuang. Meanwhile in the same year, Hangzhou, where China's tech giant Alibaba headquarters reside, opened an autonomous driving test track, located 1.4 km from Alibaba's main campus. China's autonomous vehicle industry hub of Guangzhou recently allowed Pony.ai and JingChi.ai to test vehicles in certain districts.

In December 2017 Chongqing revealed a plan to designate a huge open road test area by 2019 that includes cities, mountains, highways, tunnels and bridges, and is enabling 5G telecommunications across the area. The local government also introduced the Chongqing Autonomous Vehicle Road Test Management Implementation Rules to regulate testing on local public roads.

Also, in December 2017 in Shenzhen the technology capital of the world, 4 buses "Smart Driving Bus System" was introduced on a dedicated 1.2 km route, although drivers were assigned to these buses for safety reasons.

- **South Korea**: South Korea's government is possibly the most aggressive in terms of investment in autonomous vehicles. Autonomous vehicles with issued licenses are allowed to operate on public roads (two sections of expressways and four sections of regular roads, spanning a combined 320 kilometers).

  In November 2017, Singapore's Ministry of Land, Infrastructure and Transport announced the opening of K-City, which is the largest town model ever built for self-driving car experimentation. K-City cost US$11 billion and presents 35 different driving conditions, including toll gates, pedestrian and train crossings, and even potholes and construction sites. K-City is dedicated in its entirety in autonomous driving testing.

  At the Winter Olympics 2018, South Korea showed its autonomous driving capabilities to the world, with Hyundai Motors deploying a self-driving car fleet while KT Corporation provided a self-driving shuttle service.

Australia: New Zealand is an early and keen adopter of autonomous driving, second only to Singapore on specific policy and legislation, according to KPMG's 2018 report (figure 1.3).

New Zealand's government encourages the testing of semi and fully autonomous vehicles and is facilitating the early adoption of autonomous driving technology. The country has no specific legal requirements for drivers to be present on autonomous vehicles while testing.

Example of New Zealand's openness in autonomous driving is that in 2018, they approved the launch of "Kitty Hawk", an autonomous passenger-carrying drone/airplane that can carry two passengers and travel with speeds up to 110 miles an hour for around 62 miles at a time.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

Overall rank	Country	Total score	Policy and legislation		Technology & innovation		Infrastructure		Consumer acceptance	
			Rank	Score	Rank	Score	Rank	Score	Rank	Score
1	The Netherlands	27.73	3	7.89	4	5.46	1	7.89	2	6.49
2	Singapore	26.08	1	8.49	8	4.26	2	6.72	1	6.63
3	United States	24.75	10	6.38	1	6.97	7	5.84	4	5.56
4	Sweden	24.73	8	6.83	2	6.44	6	6.04	6	5.41
5	United Kingdom	23.99	4	7.55	5	5.28	10	5.31	3	5.84
6	Germany	22.74	5	7.33	3	6.15	12	5.17	12	4.09
7	Canada	22.61	7	7.12	6	4.97	11	5.22	7	5.30
8	United Arab Emirates	20.89	6	7.26	14	2.71	5	6.12	8	4.79
9	New Zealand	20.75	2	7.92	12	3.26	16	4.14	5	5.43
10	South Korea	20.71	14	5.78	9	4.24	4	6.32	11	4.38
11	Japan	20.28	12	5.93	7	4.79	3	6.55	16	3.01
12	Austria	20.00	9	6.73	11	3.69	8	5.66	13	3.91
13	France	19.44	13	5.92	10	4.03	13	4.94	10	4.55
14	Australia	19.40	11	6.01	13	3.18	9	5.43	9	4.78
15	Spain	14.58	15	4.95	16	2.21	14	4.69	17	2.72
16	China	13.94	16	4.38	15	2.25	15	4.18	15	3.13
17	Brazil	7.17	20	0.93	18	0.86	19	1.89	14	3.49
18	Russia	7.09	17	2.58	20	0.52	20	1.64	18	2.35
19	Mexico	6.51	19	1.16	17	1.01	17	2.34	19	2.00
20	India	6.14	18	1.41	19	0.54	18	2.28	20	1.91

Figure 1.3: KPMG's index that evaluates a country's readiness in autonomous driving. (KPMG, 2018)

In 2019, KPMG revised the above index by adding 5 more countries. Specific index and the logic behind it can be found in https://assets.kpmg/content/dam/kpmg/xx/pdf/2019/02/2019-autonomous-vehicles-readiness-index.pdf

Another study that gives as a high-level insight into the development and deployment of rules to accommodate automated driving for 33 jurisdictions, was performed in 2018 by Baker McKenzie. This study provides an outline of the key themes arising from the intersection between the most advanced digital processing technology and mobility on a global scale. (Baker McKenzie, 2018)

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

1.4.2. Ethics:

Machines can be programmed to obey on all laws concerning driving and take into consideration details like weather or road conditions via info transmitted from various sensors throughout a car or predict mechanical failures. These will surely make driving a lot more safely than it is today, but as previously mentioned, ethical issues may arise that cannot be handled by machines. These can only be solved by AI and clever programming that sets the rules and algorithms machines can understand and follow.

On the other hand, machines run into problems when it comes to ethics. In contrast to a human being we expect machines to know the basic facts that are understood in our community. They should know how to distribute risk between drivers, cyclists, pedestrians and property and decide to follow the law and minimize damage in morally ambiguous situations.

There are a variety of situations in which a driver's common sense will override the letter of law, and rightfully so. For example, if a child runs into a street in front of a car, a human would serve over the double line to avoid hitting the child. For an AV, it is up to the developer to decide when the double line law should be broken and when it is safe to do.

AVs will not be relying on human "common sense", but on confidence level. For example, if a child runs into the street in front of a car, the AV will automatically cross over the double line if a) it determines that the object in its path is alive with a high level of confidence, and b) that there is no living obstacle it would hit if it would cross the lines. Unfortunately AVs rely solely on code execution and in software. A programmer cannot include all possible situations in his code, and that creates problems.

Also, our current legal system values life differently without AVs on the road. For example, in wrongful death lawsuits juries can determine how much a person's life might have been worth based on their education, age, job prospects, and other factors. However, an autonomous vehicle cannot determine the real value of a human life based on those criteria real-time, because it lacks that kind of data.

One of the major ethical questions is what happens in a "No-win" situation. "No-win" situations happen when a crash is inevitable, and in these cases, AVs should be able to optimize the outcome based on some goal. Deciding which goals to choose and how to order them is full with moral issues.

Clearly minimizing harm to humans is an important goal but choosing how to distribute or direct harm to humans and how to prioritize the protection of some humans over the others is difficult.

A hierarchy of protecting the most vulnerable first (pedestrians), followed by cyclists, and then cars with human passengers is the natural answer, but it may not present clear solution in all cases. For example, if an AV has to choose between crashing into a wall and killing all of its human passengers or swerving to miss the wall and killing several pedestrians, what is the right answer?

Another factor that AVs have to calculate, is economic damages. If an AV has to choose between slight fender bender itself and a car driven by a human or totaling itself avoiding the fender bender, does it have to total itself? Should it assign itself any importance? Should it damage less expensive vehicles first? Is it ethical for AVs to be programmed to avoid other vehicles made by the same manufacturer, or should these kinds of reasons, be absent from ethical programming?

Right now, studies on ethics (moralmachine.mit.edu) are taking place that are trying to come with results on what is ethical in autonomous driving and what is not and how we can implement these rules and translate them into programming language that AVs can follow and make decisions.

Artificial intelligence experts and roboticists aren’t the only ones working on the problem of autonomous vehicles. Philosophers are also paying close attention to the development of what, from their perspective, looks like a myriad of ethical quandaries on wheels.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

The field has been particularly focused over the past few years on one particular philosophical problem posed by self-driving cars: They are a real-life enactment of a moral problem known as the Trolley Problem. In this classic scenario, a trolley is going down the tracks towards five people. You can pull a lever to redirect the trolley, but there is one person stuck on the only alternative track. The scenario exposes the moral tension between actively doing versus allowing harm: Is it morally acceptable to kill one to save five, or should you allow five to die rather than actively hurt one?

Though the Trolley Problem sounds farfetched, autonomous vehicles will be unable to avoid comparable scenarios. If a car is in a situation where any action will put either the car passenger or someone else in danger—if there's a truck crash ahead and the only options are to swerve into a motorbike or off a cliff—then how should the car be programmed to respond?

Rather than preaching on this, a group of philosophers have taken a more practical approach and are building algorithms to solve the problem. Nicholas Evans, philosophy professor at Mass Lowell, is working alongside two other philosophers and an engineer to write algorithms based on various ethical theories. Their work, supported by a $556,000 grant from the National Science Foundation, will allow them to create various Trolley Problem scenarios, and show how an autonomous car would respond according to the ethical theory it follows. (Goldhill, 2018)

To do this, they are turning ethical theories into a language that can be read by computers. Utilitarian philosophers, for example, believe all lives have equal moral weight and so an algorithm based on this theory would assign the same value to passengers of the car as to pedestrians. There are others who believe that you have a perfect duty to protect yourself from harm. One might think that the driver has some extra moral value and so, in some cases, the car is allowed to protect the driver even if it costs some people their lives or puts other people at risk. As long as the car isn't programmed to intentionally harm others, some ethicists would consider it acceptable for the vehicle to swerve in defense to avoid a crash, even if this puts a pedestrian's life at risk.

Perhaps these algorithms will show that one moral theory will lead to more lives saved than another, or perhaps the results will be more complicated. It's not just about how many people die but which people die or whose lives are saved. It's possible that two scenarios will save equal numbers of lives, but not of the same people.

For example, if we take into consideration the age of the people who die in an accident then we have to have a decide as a society not just how much risk we're willing to take but who we're willing to expose to risk. If some moral theories save drivers while other protect pedestrians, then there could be a discussion about which option is best. Another matter has to do with the way we build the traffic infrastructure for example with a greater separation between pedestrians and drivers.

Hacking Ethics: More relevant to this study and also interesting for further research is how any set of values used to program self-driving cars could be hacked. For example, if a car will swerve to avoid pedestrians even if this puts the driver at risk, then someone could intentionally put themselves in the path of an autonomous vehicle to harm the driver. Then there are further questions, such as how differently-programmed cars might react with each other while they're on the road.

But while we are focused on Trolley Problem-type scenarios, we must acknowledge that simply figuring out the solution for such specific situations does not address the broader issues of whether autonomous cars are ethical. For example, when such cars are rolled out and are on the road alongside current vehicles, they will be something of an experiment in how our transit systems work. Others on the road could be deeply uncomfortable with this.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

As an example, we can use the testing of a new drug. In that kind of experiments the participants are able to make informed decisions about whether or not they want to be part of that experiment.

Autonomous cars will likely have massive unforeseen effects yet completely unknown to our society. Scientists compare the advent of autonomous driving to that of the invention of electricity. No one predict in how many ways this technology can change the way we live today, exactly like no one could predict the extent use of electricity when it was first invented and used.

The invention of standard cars, for example, gave us the rise of the suburbs and fast food drive-through restaurants. Perhaps autonomous cars will lead to people living further away. The time humans once spent driving could be replaced by leisure while in driverless cars, but this is also highly uncertain.

Meanwhile, autonomous cars' efficient driving could reduce traffic. It's a safe bet to say that we can't imagine the scale of effects. Ultimately, the effects of autonomous cars will likely be huge and unpredictable. No algorithm or philosophical theory can make driverless cars perfectly moral.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

2. Threats in autonomous driving

2.1. Autonomous Vehicles (AVs) & Connected Vehicles (CVs) – two different problems combined:

Vehicle automation is not a new technology at all. In fact, there are plenty of vehicles used every day that rely on automation to perform basic tasks, like airplanes or automated trains. The difference is that all those vehicles are not fully automated! Basic functions still rely on human input or intervention. For example, on the contrary to what everybody believes, most airplanes take offs and landings are 100% manual due to the complex nature of the task and the numerous data and different factors one has to take into consideration to perform the task. Last generation of aircrafts, like the Airbus A380, can land themselves, but they do it in a totally controlled physical environment (airports with air traffic controls) and less parameters involved (no other airplanes on the loose). When the surrounding parameters are extreme or special, then again human pilot intervention is needed.

The above described example shows how difficult it is to create a fully automated vehicle. Another important factor that is missing from these examples is that all these automated vehicles mentioned above have never deployed into a large scale, as autonomous vehicles, and that they operate in specially designed infrastructure (trains), do not encounter traffic, and when they do there are people that organize and control this traffic (air traffic controllers).

All these challenges have to be overcome before we mass produce and deploy fully automated vehicles into our society and public roads. In order to do that, it is obvious that cars have to have onboard the technology that allows them to drive themselves and also, they have to be aware about their surroundings. To do that they have to be able to send and receive data to and from infrastructure and to each other, in other words, to be connected.
For that to happen, different technologies have to be utilized and to be utilized in conjunction with the driving automation, such as communication (including protocols), information processing and AI. But that isn't enough: Infrastructure elements like data transmitters and receivers, GPS satellites, road sensors and specially designed road sings readable by automated vehicles have to be in place in order for this type of communication to be effective with the least possible interruptions.
As any other newly developed technology, connected and automated vehicles will have their flaws and security holes and will need security improvements and patches.

As a result, automated vehicle researchers and manufacturing companies have to face threats not only related to the on-board tech on a vehicle but also threats coming from the necessary vehicle to vehicle and vehicle to infrastructure communication.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

2.1. Threat Classification:

It has become obvious until now that the spectrum of threats in autonomous driving is very wide and that imposes the need to classify those threats into groups for better understanding and analysis.

The threat surface area can be divided into three main categories depending on where the attacker could focus his attack, the vehicle itself, the driver, or the underlying infrastructure (diagram 2.1).

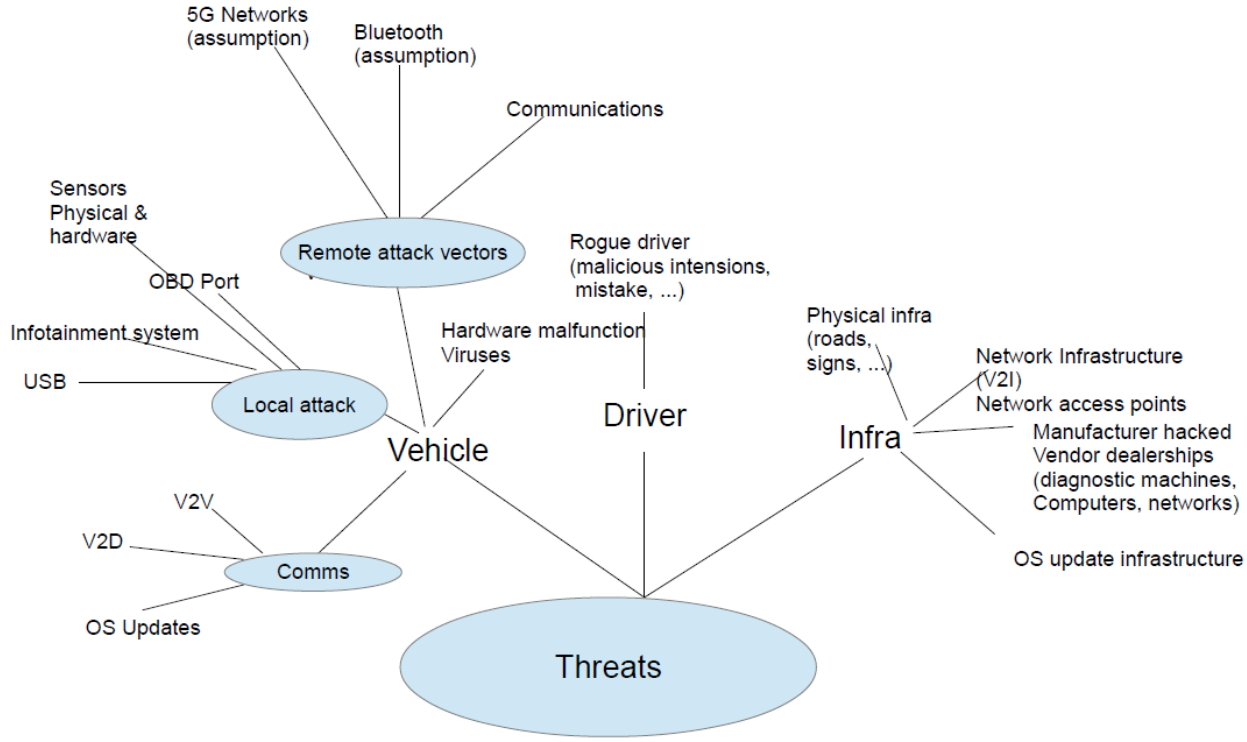


Figure 2.1: Threat Vector Classification

The vehicle attack surface area as imagined is the biggest and can be subdivided into more than one subcategories depending on the physical media (access ports, wireless network, sensors) or the communication protocol (5G+, Bluetooth, etc) used to employ an attack as seen also on the above diagram. In the same way the infrastructure threat surface area can be divided depending on the type and location of structure the attacker chooses to take advantage.

2.2. Vehicle Surface Area:

As mentioned before the widest attack surface area is the autonomous vehicle itself and is more prone to attacks due to the large number of new technologies employed for it to function properly and efficiently, to communicate with other vehicles and the infrastructure and to protect and inform the passengers using human interface displays. In addition, autonomous vehicles are easily accessible (physically or remotely) by malicious individuals compared to infrastructure.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

The threats on the vehicle itself can also be classified into two main categories depending on if the attacker has physical access to the vehicle or not, we can separate attacks to “local attacks” or “remote attacks”.

3. Local attack Vectors:

3.1. Abstract:

Local attack vectors in an autonomous vehicle can potentially be all the electronic devices, parts, physical interfaces or protocols employed by the vehicle in order to function. These include but are not limited to devices like sensors, OBD ports, USB ports, infotainment systems and in general every port that provides direct access to the vehicle’s ECU via the CANBus architecture.

3.2. Sensors and ECUs:

Our cars today make use of a vast array of sensors. Almost all functionality, from the most complex tasks to the basic ones of a modern car, rely on a type of sensor and all sensors are controlled by ECUs.

Sensors in a vehicle (autonomous or not) can be divided in three big categories. Those that are essential for basic functions of a vehicle's motor (MAP, lamda, oxygen, throttle position, knock, speed,...), sensors that have to do with the various security features of a vehicle (airbags, ESP, ABS,...), and sensors that just provide useful information to driver and passengers or make their commute easier but are not critical to its function.

A list of sensors on a modern car can be seen in the following diagram:

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

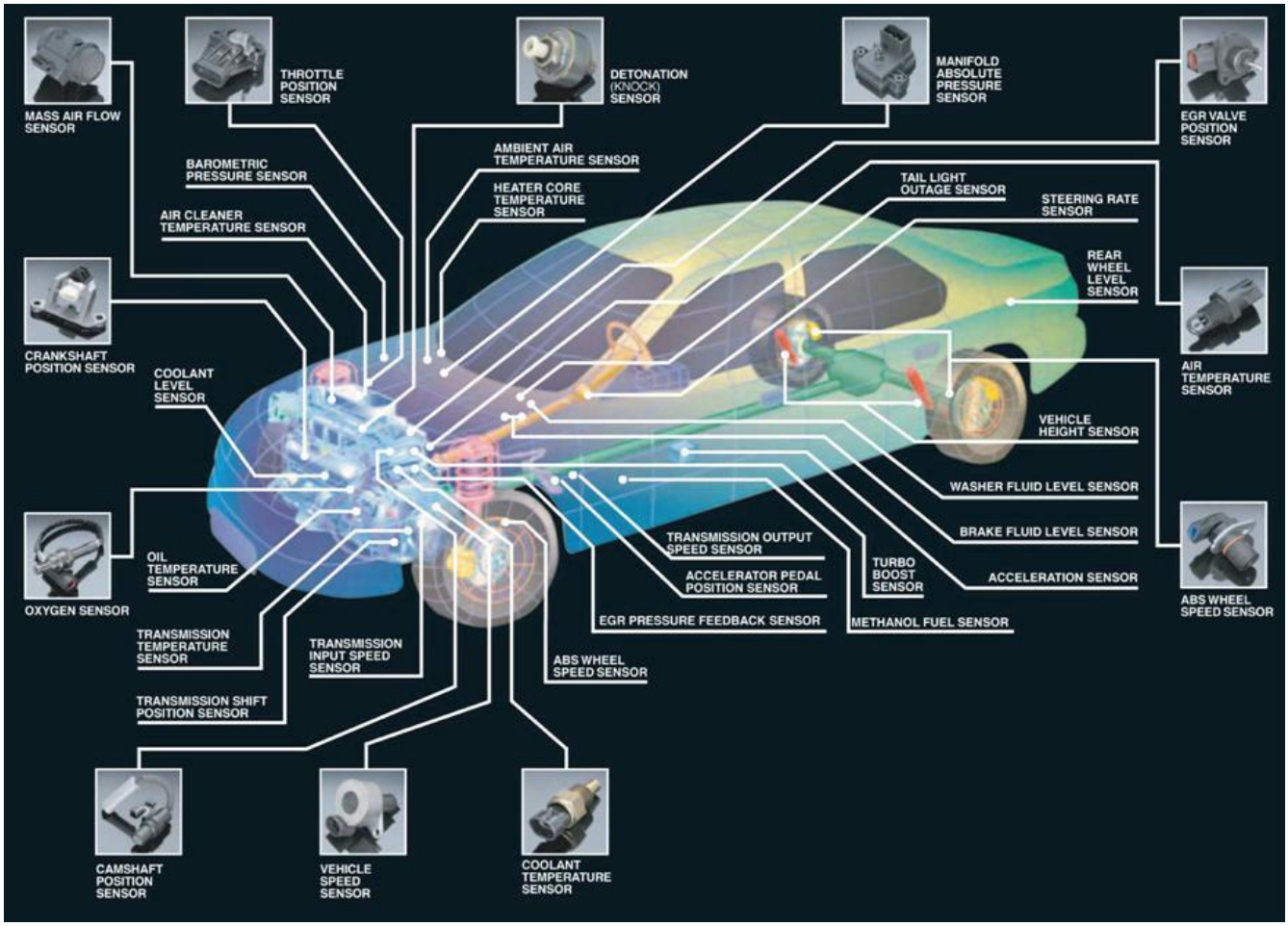


Figure 3.1: Modern car sensor diagram (©AS Autoparts blog)

Autonomous vehicles will rely heavily on sensors and other electronics in order to achieve the required level of automation. Together with the increase in the number of sensors, complexity also increases dramatically and now sensors are responsible to provide information and data for far more important tasks that affect the safety of the vehicle and the passengers on board. Automated vehicles will have to monitor, for example, all traffic and recognize other cars, pedestrians, physical obstructions etc. and the vehicle's security and lives of the passengers depend on it.

The added automation of autonomous vehicles relys in the extended use of various sensors such as LiDARs and RADARs.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

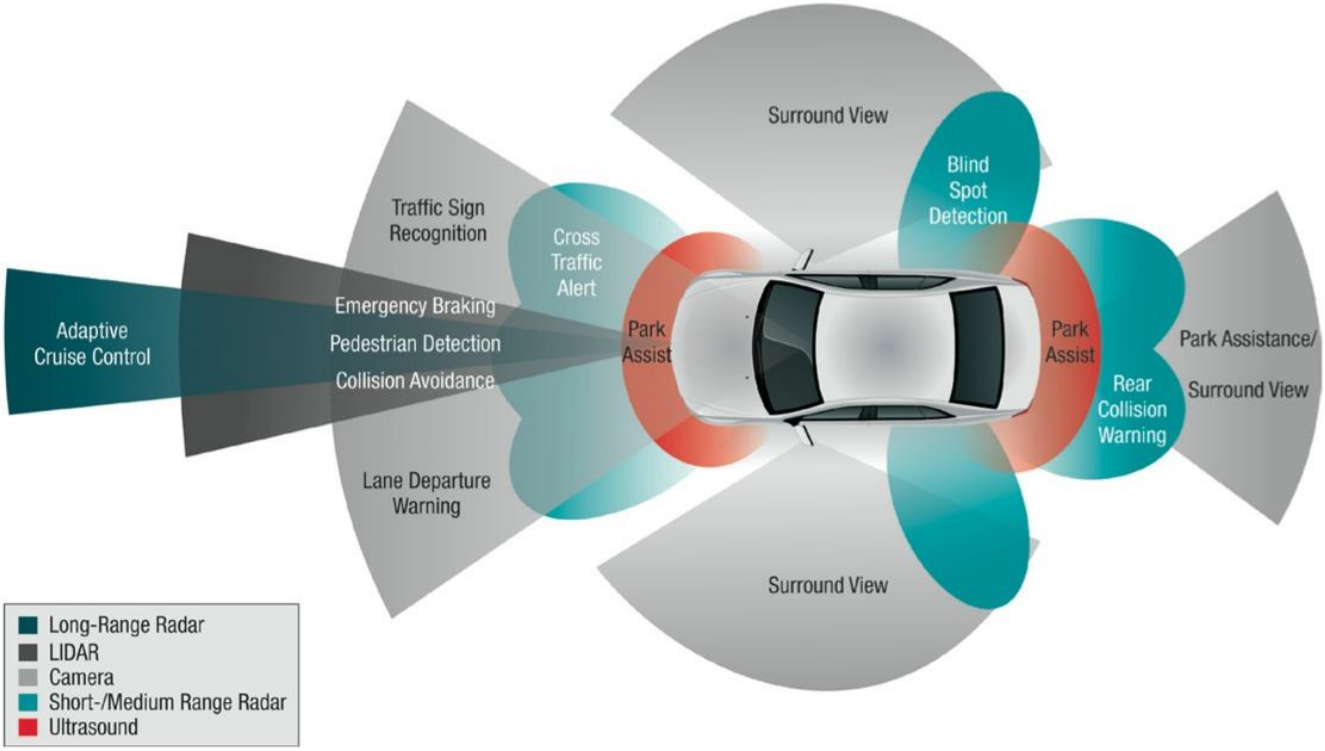


Figure 3.2: Autonomous vehicle sensors

3.3. Sensors & security:

Sensors today are widely used in the automotive industry. Many decisions our car makes (auto throttle, ESP, autobraking, the mixture of gas and oxygen in the engine, automatic headlights and screen wipers) are based on the data that sensors send to the data processing units in a car. Then the ECU after analyzing those data decides and makes changes to the operation of the vehicle.

It is obvious that autonomous vehicles function relies on sensor data, and that the integrity of these data is of critical importance. Various attempts, often successful, have been made so far to tamper with the sensors of a vehicle.

Sensors can be tampered by two ways, physically and digitally.

Although it is difficult to tamper with the engine sensors physically as someone had to have access to the vehicle's engine, anyone can mess around with a light or distance sensor and tamper the data that the sensor sends to the ECU. That way you can trick a vehicle's ECU about the distance from another vehicle or another obstacle. Another example is the easy way anyone can hack an ultrasonic sensor by just using a sound generator, or a lidar using a pulse generator and trick the car's microprocessor that an obstacle is near or use many pulse signals and immobilize the car thinking that it is surrounded by different obstacles. Also, researchers have managed to trick tire pressure sensors by using sound waves in certain frequencies and as a result by feeding it false data, make the car's ECU fail. In fact, various kind of sensors are vulnerable to analog signals resulting in problems to the vehicle's functions or even

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

immobilizing it. These attacks can be easily avoided by using low or high pass filters that can cut signals with lower or higher frequencies than the ones the sensor uses and attach those to sensors, but manufacturers have not designed those filters with security in mind. (University of Michigan, 2017)

3.3.1. Audio and Visual sensors:

The problem gets even bigger now that partially or fully automated vehicles are being developed. That's because autonomous cars will rely heavily on data fed to them by their sensors, as that is the only way to understand and map their surroundings and make decisions accordingly.

Three main types of AV sensors are going to be used extensively in autonomous vehicles:

- Image sensors / Cameras
- RADAR: Radio Detection And Ranging
- LIDAR: Light Detection And Ranging

Cameras in conjunction with radar systems provide a precise evaluation of speed and distance as well as outlines of obstacles and moving objects. Radar sensors for short range (24GHz) or long range (77GHz) are located in the front and back of a vehicle to monitor traffic and can monitor ranges from a centimeter up to a few hundred meters. Lidar systems can identify distances to objects and although they are rarely used today, they will be extensively used in autonomous vehicles industry in the coming years.

Cameras:
Even today current vehicles carry cameras. According to predictions each autonomous vehicle will have as many as 25 cameras. Video images are a suitable input parameter for highly automated driving and provide a representation of the environment outside the vehicle. Image feed is usually fed to a central processing unit for decoding and analyze, or the process can be done decentralized on the camera itself and then send the processed data to the CPU. Then the signal is being sent to a monitor for display, often enhanced with information friendly to the driver like distances or speed measurements.

Image 3.1: Camera sensor

Hacking a camera: The simplest physical way to hack a camera or a light and range sensor is to put a solid obstacle in front of it, blocking the light that passes through the sensor, and thus stop feeding data to the vehicle's systems.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

RADAR:
Several radar sensors are required for Advanced Driver Assistance Systems (A.D.A.S.) to function. Short range radar (SRR) will replace ultrasonic sensors and are placed at each corner of a vehicle and mid to large range radars that are placed in front of the vehicle for long range detection.

LIDAR:
Lidar is a new system in the automotive industry and is gaining traction. It is a laser-based system that has a laser transmitter and a highly sensitive receiver and is used to measure distances from stationary as well as moving objects and provide three dimensional images of the detected objects. In fact, lidars emit light and receive the reflected to the detected object signal. It then measures the distance by calculating the travel time of the laser beam, and dividing it with the speed of light.

Image 3.2: Lidar sensor

Like any other image or light sensor, Lidars can be tricked by simply putting an obstacle in front of them, but that can also happen by illuminating the sensor with a strong light of the same wavelength as the one the lidar uses. Then the sensor can actually erase existing obstacles in the sensed output of the lidar.
Spoofing of a Lidar has also been proven to be easy as many researchers have managed to trick it by using simple techniques and cheap equipment. As seen in below picture a Lidar uses a finite number of dots from reflected light to reconstruct a detected image.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

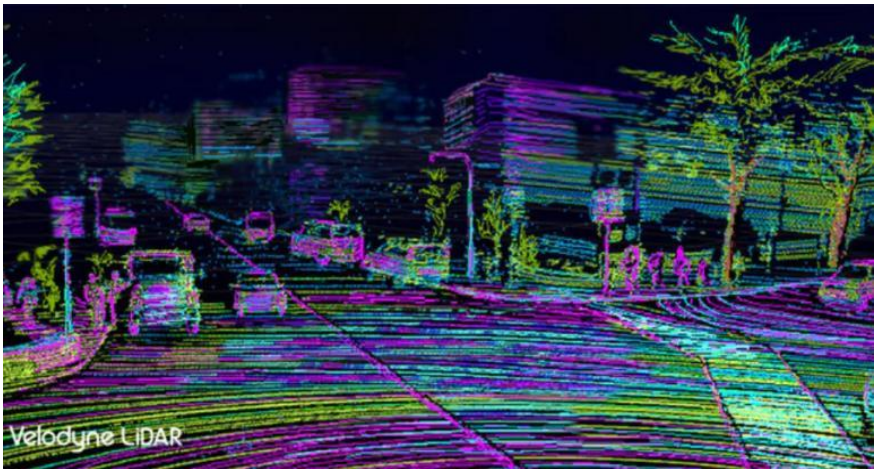


Image 3.3: Lidar view

An attacker can easily spoof a lidar just by making it respond to points of light similar to the ones of an object in front of the lidar as normally expected. Also, since the current Lidar sensors use curved glass to protect the optics inside them, someone can easily be tricked from a laser generating a point cloud at an angle can exploit refraction to change the "apparent" direction and derange the point cloud. (Chirgwin, 2017)

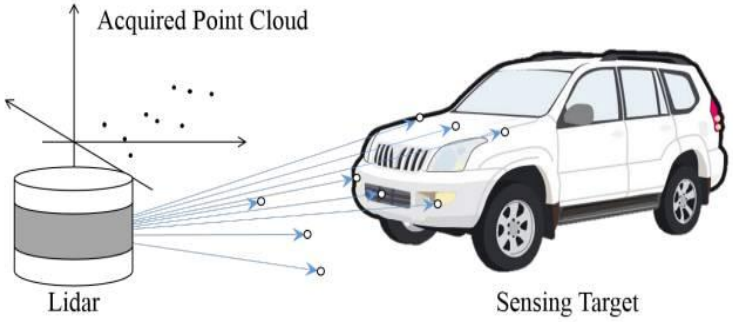


Image 3.4: Lidar function

Another attack possible on lidars has to do not with the distance but with the timing. Researchers have managed to capture a pulse emitted by a lidar and sent it back after adding a delay. This way the lidar would be impossible to react and send a warning signal to the ECU on time and the vehicle could be in serious trouble unable to react and avoid an obstacle. (Higgins, 2015)

Efforts are being made by manufacturers to improve lidar technology and safeguard lidar sensors against spoofing, by adding components that could separate real from spoofed signals. These technologies add significant cost to lidar manufacture and could also add delay to the process of the signal received by the sensor when sent to the vehicle's ECU that could have fatal consequences.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

3.3.2. Motor Sensors and ECUs:

As mentioned, modern vehicles are equipped with a large array of sensors all controlled by processing units (ECUs).

These sensors and ECUs control all functions of a vehicle from engine components and the systems responsible for the physical movement of the vehicle, to the safety features and the entertainment and convenience related components (engine management systems, automatic braking and braking assistance systems, airbags, seatbelt tensioners, door locks, gauge cluster, sound systems, infotainment systems, GPS, seat controls, communication systems and a lot more).

All these systems are interconnected, which means that an attacker could potentially exploit a vulnerability in one of the less important components and then gain access to safety and engine management systems, jeopardizing the security of the passengers.

3.4. CANBus:

3.4.1. CANBus Abstract:

Interconnected systems, ECUs and sensors communicate using the CANBus architecture.

CANBus was introduced in 1986 by Bosch and Intel and every automobile manufactured today is equipped with it. Also, CANBus is used as well in other means of transport such as trains and ships and also in a variety of industries like building automation, medical and manufacturing.
CANBus is a multi-master, message broadcast system that specifies a maximum signaling rate of 1 megabit per second. Unlike traditional networks such as ethernet, CAN sends short messages like temperature or RPM as broadcast to the entire network, instead of large blocks of data from point A to point B under the supervision of a central bus master.

Design goal of the CANBus was to create a protocol that would be noise immune, broadcast, low cost and lightweight backbone network, priority handling with limited delay for critical messages, error detection and fault confinement capabilities. An ISO 11898 (CANBus) architecture example can be seen in the following picture:

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

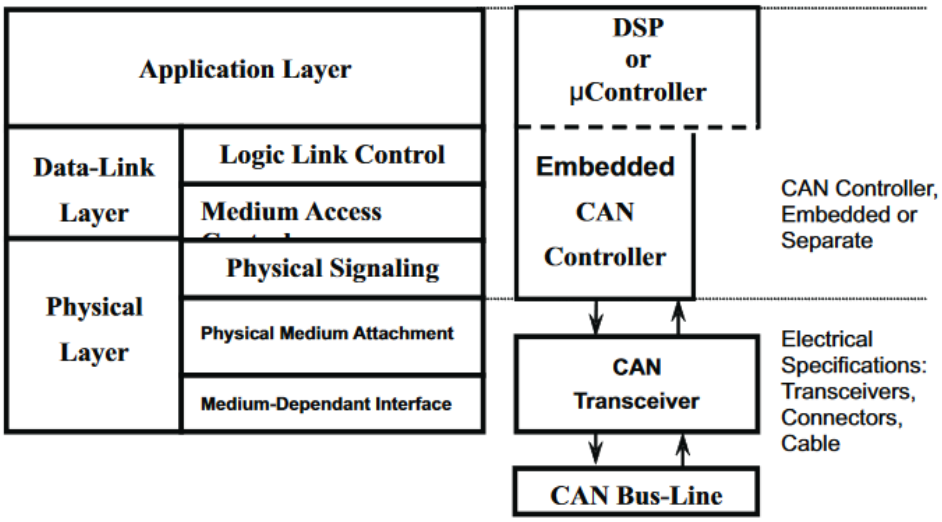


Figure 3.3: CANBus architecture

CANBus was standardized with ISO 11898 and later 11898-2 and 11898-3 in order to prevent inconsistencies between manufacturers.

- ISO 11898: Initial CAN architecture
- ISO 11898-2: High speed CAN (mostly used today)
- ISO 11898-3: Low speed or fault tolerant CAN

Each CAN node consists of 3 basic elements: a DSP or microcontroller, an embedded CAN controller, and a CAN transceiver.

- A microcontroller sends and processes complete CAN frames to and from the CAN controller and supervises the CAN controller operation.
- A CAN controller supervises the correct implementation of the CAN specifications. Syncs with the CAN signal, sends and receives data to and from the CAN transceiver, adds stuff bits, performs error handling and actualizes the error modes.
- A CAN transceiver is an interface between the CAN controller and the physical bus by translating logical signals to electrical levels.

3.4.2. The CAN communication protocol:

Standard CAN or Extended CAN:

The CAN communication protocol is a carrier-sense, multiple-access protocol with collision detection and arbitration on message priority (CSMA/CD+AMP). CSMA means that each node on a bus must wait for a prescribed period of inactivity before attempting to send a message. CD+AMP means that collisions are resolved through a bit-wise arbitration, based on a preprogrammed priority of each message in the identifier field of a message. The higher priority identifier always wins bus access. That is, the last logic high in the identifier keeps on transmitting because it is the highest priority. Since every node on a bus takes part in writing every bit "as it is being written," an arbitrating node knows if it placed the logic-high bit on the bus. (Corrigan, 2016)

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

The ISO-11898:2003 Standard, with the standard 11-bit identifier, provides for signaling rates from 125 kbps to 1 Mbps. The standard was later amended with the “extended” 29-bit identifier (extended CAN). The standard 11-bit identifier field in Figure 2 below provides for 211, or 2048 different message identifiers, whereas the extended 29bit identifier in Figure 3 provides for 229, or 537 million identifiers.

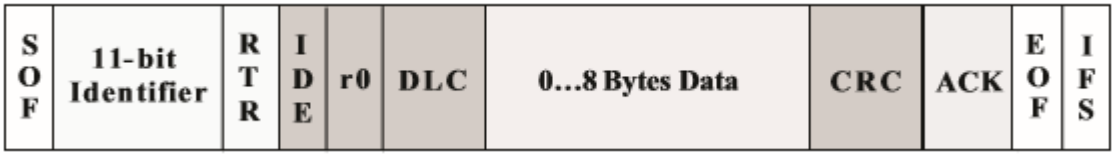


Figure 3.4:Standard CAN 11898

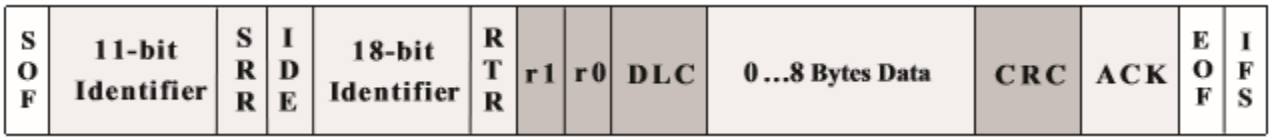


Figure 3.5: Extended CAN 11898-2

The CAN bus:

The data link and physical signaling layers of Figure 1, which are normally transparent to a system operator, are included in any controller that implements the CAN protocol, such as TI's TMS320LF2812 3.3-V DSP with integrated CAN controller. Connection to the physical medium is then implemented through a line transceiver such as TI's SN65HVD230 3.3-V CAN transceiver to form a system node as shown in Figure 4.

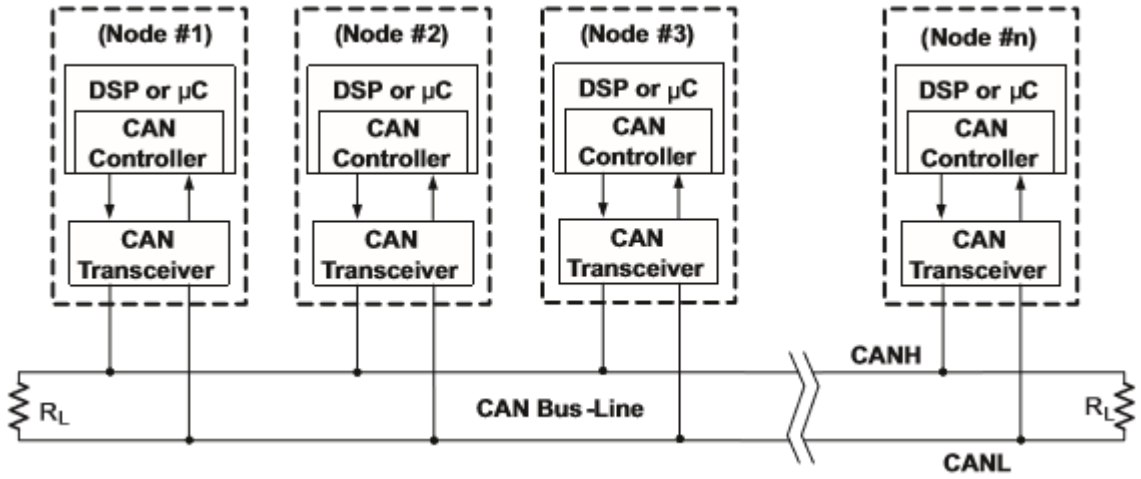


Figure 3.6: CANBus system node

Signaling is differential which is where CAN derives its robust noise immunity and fault tolerance. Balanced differential signaling reduces noise coupling and allows for high signaling rates over twisted-pair cable. Balanced means that the current flowing in each signal line is equal but opposite in direction, resulting in a field-canceling effect that is a key to low noise emissions. The use of balanced differential receivers and twisted-pair cabling enhance the common-mode rejection and high noise immunity of a CAN bus. (Corrigan, 2016)

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

The High-Speed ISO 11898 Standard specifications are given for a maximum signaling rate of 1 Mbps with a bus length of 40 m with a maximum of 30 nodes. It also recommends a maximum unterminated stub length of 0.3 m. The cable is specified to be a shielded or unshielded twisted-pair with a 120-Ω characteristic impedance (Zo). The ISO 11898 Standard defines a single line of twisted-pair cable as the network topology as shown in Figure 6, terminated at both ends with 120-Ω resistors, which match the characteristic impedance of the line to prevent signal reflections. According to ISO 11898, placing RL on a node must be avoided because the bus lines lose termination if the node is disconnected from the bus.

The terms CAN_H (CAN High) and CAN_L (CAN Low) are derived from the way in which CAN messages are physically transmitted. When the CAN bus is idle, both wires carry 2.5V. But when transmitting data, the CAN_H wire increases to 3.75V and the CAN_L wire drops to 1.25V, creating a differential between the two wires of 2.5V. This voltage differential makes the CAN bus tolerant to electrical noise and interference. (Corrigan, 2016)

The CAN standard defines a communication network that links all the nodes connected to a bus and enables them to talk with one another. There may or may not be a central control node, and nodes may be added at any time, even while the network is operating (hot-plugging).

In today's vehicles there are two types of messages going through the CAN bus network. Standard messages and diagnostic messages.

- Standard messages are the ones that are exchanged between two or more CAN ECUs for a function of the vehicle to take place. As an example, the communication between the ABS module and the central ECU and braking module, in order for a correction of the vehicle's trajectory to happen, or the radio frequency hub module with the doors locking module when the driver pushes the button to unlock the door or when the autolocking mechanism after a certain speed is reached by the vehicle.
- Diagnostic messages are the ones that are exchanged between a diagnostic device connected to the vehicle's internal network via the OBD II port and one of the ECUs for diagnostic and troubleshooting purposes.

As with any other known network like Ethernet, CANBus can be hacked by someone that has access to it, either physical or via remote access.

Several attacks (Eisenbarth, Moradi, Paar, Salmasizadeh, & Shalmani Manzuri, 2008), (Rouf, et al., 2010), (Hoppe & Kiltz, 2010), (Koscher, et al., 2010), (Miller & Valasek , 2015), (Golson, 2016) have been successful in exploiting the CANBus stream and their results were also published. The most detailed and comprehensive CANBus hacking studies have been made by Roderick Currie of SANS Institute in 2017 – Hacking the CAN Bus: Basic Manipulation of a Modern Automobile through CAN Bus Reverse Engineering (Currie, 2017) and Andrea’s Palanca of Milan polytechnic - A Stealth, Selective, Link-layer Denial-of-Service Attack Against Automotive Networks (Palanca, 2016). Both studies contain detailed explanations of the CANBus network and provide lots of examples of successful attacks to it.

In today's cars with advanced infotainment systems and a large number of ECUs controlling the active safety systems, the area of attack to the CANBus network has increased dramatically. With the advance of autonomous driving it is predicted that the area of attack will be multiplied as the number of ECUs

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

will increase and the number of sensors and CAN controllers responsible for the control of the vehicle and the processing of the data received by sensors, will dramatically increase also.

3.5. OBD II:

3.5.1. OBD II Abstract:

OBD or On-Board Diagnostics is an automotive electronic system that provides vehicle self-diagnosis and reporting capabilities for repair technicians to access subsystem information for the purpose of performance monitoring and repair. Early versions of OBD (OBD-I 1991) were very minimal and provided only a visual indicator (a blinking light) when a problem was detected, but current OBD implementations are standardized (OBD-II – SAE J1962) and provide real-time data generated by the vehicle's ECU and standard failure codes (DTCS) for all electronic subsystems of a vehicle.

OBD II standard allows for a diagnostic device to be plugged to an OBD II interface plug located underside of every vehicle's dashboard manufactured after 1996 in the US and after 2001 in the EU for gasoline cars and 2003 for diesel cars (EOBD: European OBD standard). Depending on the vehicle the OBD II port could have 16, 9, or 6 pins. (Barreto, 2017)

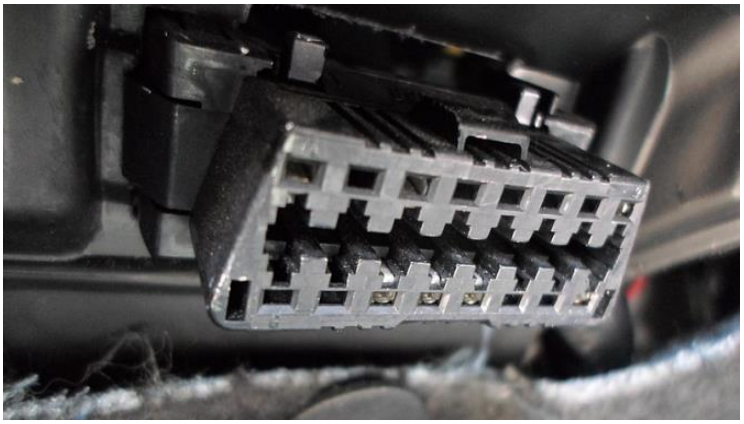
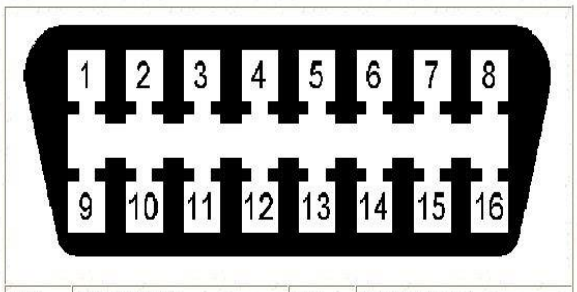


Image 3.5: OBD II port

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218



PIN	DESCRIPTION	PIN	DESCRIPTION
1	Vendor Option	9	Vendor Option
2	J1850 Bus +	10	j1850 BUS
3	Vendor Option	11	Vendor Option
4	Chassis Ground	12	Vendor Option
5	Signal Ground	13	Vendor Option
6	CAN (J-2234) High	14	CAN (J-2234) Low
7	ISO 9141-2 K-Line	15	ISO 9141-2 Low
8	Vendor Option	16	Battery Power

OBD-II Connector and Pinout

Figure 3.7: OBD-II connector pinout

The OBD standard specifies the pinout of the port and also the signaling protocol, the messaging format and a list of standardized DTCs. Because of the OBD standard, every OBD II diagnostic device can connect and receive data from every vehicle that uses the it. (E, 2013)

Data and information that can be retrieved from a vehicle via OBD port are:

- Powertrain (engine & transmission: DTC codes start from Pxxxx)
- Body (DTC codes start from Bxxxx)
- Chassis (DTC codes start from Cxxxx)
- Network (DTC codes start from Nxxxx)

DTC (Diagnostic Trouble Codes):

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

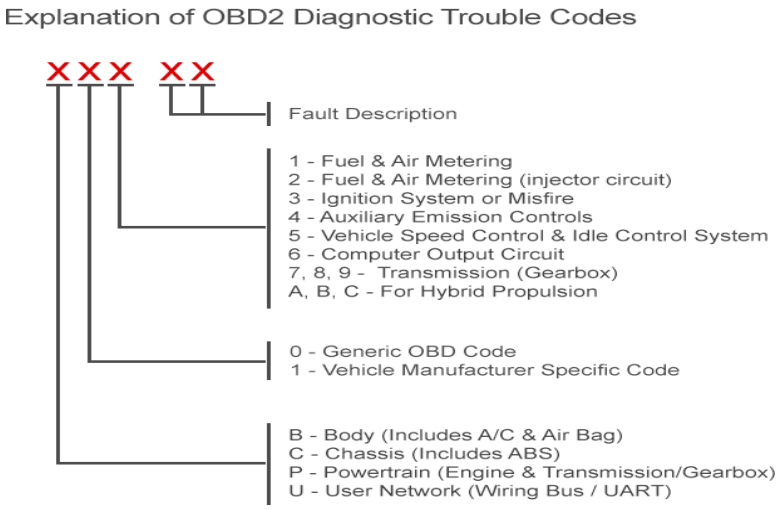


Figure 3.8: Diagnostic Trouble Codes

In addition, we can get info about VIN (Vehicle Identification Number), calibration identification number, ignition counter and emissions control systems counter.

Services: There are 10 diagnostic services (or modes) in the latest OBD-II standard (SAE J1979):

- 01: Show current data
- 02: Show freeze frame data
- 03: Show stored Diagnostic Trouble Codes
- 04: Clear Diagnostic Trouble Codes and stored values
- 05: Test results, oxygen sensor monitoring (non CAN only)
- 06: Test results, other components/systems monitoring (test results, oxygen sensor monitoring for CAN)
- 07: Show pending Diagnostic Trouble Codes (detected during current or last driving cycle)
- 08: Control operation of on-board component/system
- 09: Request vehicle information
- 0A: Permanent Diagnostic Trouble Codes (DTCs or Cleared DTCs)

PIDs (SAE Standard J1979): PID= XX (HEX)

PIDs are codes used to request data from a vehicle using an OBD-II diagnostic tool. For each PID, a certain reply is expected and a specific form, and these are catalogued for reference (i.e. PID=0D) returns the vehicle's speed to km/h. (zhaoshentech, 2018)

Except for diagnostics and troubleshooting, OBD-II is also used in modern cars for ECU adjusting and reprogramming, scanning tools, data loggers, supplementary vehicle information and vehicle telematics. Depending on the device used to access the OBD-II port, a user can also access more advanced diagnostic options, set manufacturer or vehicle specific ECU parameters, access and control other ECUs like airbags control, ABS, real time monitoring or graphing of engine parameters to facilitate diagnosis or tuning. Also, along with the use of GPS, OBD allows for fleets of vehicles to be tracked and report information about fuel consumption, speed limit tracking, as well as remote diagnosis of malfunctions.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

Image 3.6: OBD-II Diagnostic module

3.5.2. OBD-II and threats:

During our short description and analysis of the OBD-II standard, it has become clear that OBD can access all electronic devices and ECUs of a vehicle and change values or report information. It is obvious that any malicious individual that has access to OBD either via the OBD port (physical access), or for example the GPS module (GPS spoofing or jamming) or the wireless communication module (remote access), can tamper with a vehicle's functions. This problem becomes even more apparent in autonomous vehicles where all functions will be controlled by processing units. Also, in an autonomous vehicle a central processing unit will be needed to collect and process data from all ECUs and make driving decisions or predict a failure and take actions to prevent a failure, or for example immobilize the vehicle. Malicious intended access to such systems via the OBD could be proven to be fatal for passengers.

Several studies have been conducted to expose and address weaknesses of the OBD standard. Unfortunately, OBD and its creators, when developed several years ago, had no security concerns when designing it or implementing it.

For example, OBD-II does not require any kind of authentication of authorization for any device that connects to the OBD port. Attacks that are based on physical access to the port are controversial. That is because on one hand an attacker should have physical access to the inside of a vehicle, but on the other hand if such access is granted, then all vehicle functions can be controlled by the attacker, as he will have access to the CAN bus stream.

Some of the most known studies on vulnerabilities on the OBD-II are:

- The most detailed research so far concerning OBD has been conducted by Argus Cyber security team, when they managed to hack into more than one dongles that plug into the OBD port without facing any serious difficulties of any kind and then inject malicious packets into the CANBus. In fact they found security holes into one of the industry's most used dongles, Bosch Drivelog OBD-II which is a smart device that connects via Bluetooth and track fuel consumption and send alerts when service of the vehicle is needed. To do that, a PIN is required to be entered from the Bluetooth device and sent to the dongle. Researchers brute-forced the PIN entry gaining

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

access to the device. They also found security holes in the message filter of the dongle that allowed them to inject malicious messages into the CANBus network.
It is worth mentioning that both vulnerabilities have been patched by Bosch, using two factor authentication between the application and the dongle and updating the firmware preventing the malicious code to be injected into the data stream. (Kovelman, 2017)

- Another OBD-II connected device the "Zubie", that contains a cellular modem and automatically collects data about fuel consumption, engine status, and GPS location. Researchers managed to connect to the device's diagnostic port a standard UAT port and gained access to all device's files. They decompiled the Python executable program that runs on the device and were able to see what the device was doing at any given time. "Zubie" didn't use any kind of encryption or authentication during firmware updates. That omission allowed the attackers by using a rogue cell site and DNS false records to inject a trojan firmware, that gave them access to every vehicle's function, from unlocking the doors to shutting down the engine. (Argus Cyber Security, n.d.)

- Digital Bond Labs security researcher Cory Thuen discovered that he could exploit Progressive's Snapshot driver tracking tool in order to hack into the onboard networks of certain automobiles. Snapshot is a tool manufactured by Progressive auto insurance that plugs into the OBD-II port. Its purpose is to monitor driving behavior in order to offer cheaper insurance rates to safer drivers. By reverse engineering the dongle and plugged it into his Toyota Tundra, determined that Snapshot does not authenticate itself nor applies any encryption to its traffic data neither contains digital validation signatures, or offer a secure boot function. Snapshot devices communicate with Progressive over the cellular network in plain text. This means that an attacker could pretty easily set up a fake cell tower and perform a man-in-the-middle attack. (Brian Donohue, 2015)

3.6. Progress – Countermeasures:

As it has been proven, an attacker can take full remote control of a vehicle taking advantage of security holes in devices that connect to the OBD port or if they have physical access to it. In order to prevent these attacks several proposals and actions have been made. Autonomous vehicles can be safe from malicious attackers using the OBD port by implementing changes like:

- Physical access prevention & software dongles: The need to secure the OBD port has lead to the creation of devices intended to secure physically the port itself. Examples of these devices are from companies like Runsafe security, Argus security (these provide physical and software protection) or Autocyb (provides only physical protection).

RunSafe uses binary stirring to increase security by leveraging randomization (binary stirring) or novel control flow integrity (CFI). The overlay is an example of a defensive technology called run-time application self-protection (RASP). They can "shrink" an application or the OS attack surfaces by up to 90%. The framework for neutralizing these attacks centers on transforming code loaded in-memory to add hardening and to appear different via randomization. Like a snowflake, identical embedded devices provide the appearance of having unique sets of software files in kernel, user, variable, and thread space. Thus, a malware attack lacks the uniformity needed to scale to other devices, eliminating an entire

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

class of cyberattacks by shrinking the attack surface. What is unique and innovative about RunSafe's approach to randomization and security is their three-pronged solution. First, they randomize every in-memory binary: functions and libraries. Second, they randomize the ordering of blocks to eliminate attacks where software functions can be called out-of-order to insert malicious code. These are known as Return/Jump Oriented Programming (ROP/JOP) attacks. Third, they randomize memory set aside for input variables as they are sourced into the code stack. (RunSafe Security, 2019)

Argus technology identifies attacks using its patent-pending deep packet inspection algorithms that scans all traffic in a vehicle's network, identifies abnormal transmissions and enables real-time response to threats. Argus aftermarket solution is designed to provide a comprehensive overview of cyber attacks and irregularities, allowing car makers to identify unauthorized attempts to change an ECU's behavior.

- Another approach is to add and use authentication in OBD by implementing an authentication gateway between the OBD-II part and the other networks, that will be designed to control access and privileges. This will allow only transmission of PIDs data queries to all unauthorized users and full CAN bus access to authenticated users.

3.7. Infotainment Systems:

Our vehicles in the last decade have been transformed into media consuming devices since manufacturers have added electronic devices such as touch screens, GPS, USB ports and SD cards for media reading, Bluetooth & wireless connections etc. This trend will surely continue in autonomous vehicles. Driver and passengers will have a lot of spare time (especially in long commutes) since their attention will not be needed anymore. It is also certain that functions will be added to the infotainment systems making them more and more complex.
Today as an infotainment system we describe the collection of hardware and software in a vehicle that provides audio and video entertainment, and also include devices such as navigation systems, video players, game consoles, and also provide USB, Bluetooth and WIFI connectivity. Future infotainment systems will surely add to these systems, as these systems will also be necessary for the functionality and safety of the vehicle. Personal assistants (like those in our phones) will be embedded in our vehicles, as an interface between the passenger and the vehicle, communicating destinations and other information.

The security of these systems will be of big importance, as any other system that can potentially control the vehicle. Potential local threat surfaces (wireless and remote threats will be covered in a different chapter of this paper) in infotainment systems are:

- Touch screens and other inputs: used to control the infotainment system functions
- USB ports, SD cards: used to transfer files to and from the system for playback purposes or edit.
- Bluetooth
- WIFI
- GPS
- Cellular interface

3.8. USB & SD Cards:

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

Current infotainment systems on vehicles are very prone to hacking. They are usually embedded systems based on ARM CPUs and Linux OS with full access to Bash command line shell and all linux based utilities. These systems, as reported from various attack attempts by researchers, (Rus, 2017) seem to be created in a hurry and not with security in mind, but ease of implementation and convenience, using outdated programming principles and technology stacks by today's standards. It is obvious that viruses or worms that can affect linux OS can also work on infotainment systems, giving access to systems functions or even more dangerous, allowing attackers to go further into the CAN bus.

By injecting malicious code via a USB stick to the infotainment system, researchers have managed to gain access to:

- Contacts, call logs, SMS and other info stored in smartphones are stored to unit's memory when paired with a smartphone and are being kept even after the phone was disconnected.
- GPS location and location history has been accessed using the same method, and also managed to infect any USB plugged into the USB port, spreading potentially the virus to other vehicles.
- Virus or malware can be controlled by SMS and read info saved on the connected smartphone such as call logs, user's phone directory or even passwords and banking authentication PINs, and even block incoming and outgoing calls.

3.9. Infotainment via WIFI:

- Audi & VW infotainment systems: In early 2018 researchers at "Computest" managed to almost gain access to the CANBus by exploiting the WIFI module in Audi & VW cars. They willingly stopped their efforts before gaining access to the vehicle's most critical systems although this was feasible for legal reasons. In both cases (Audi & VW) a port scan into the WIFI adapter or the cellular connection respectively revealed some sort of telnet service that was running in the background. The exact exploit was never revealed by the researchers to the public, but only to the VW group, that according to them they patched t it. Unfortunately, the exploit does not exist only in vehicles produced after the incident, and all older cars are susceptible to it. (Dunn, 2018)

- Pioneer “avic” infotainment: Another example is the hack of the Pioneer “avic” infotainment system that has been hacked by using a USB stick containing a special image that boots the device into test mode and overwriting the internal SD card with the image. The hack has been developed to allow map files of the navigation system to be updated but lead to the replacement of the entire image of the system with custom firmware entirely created by the community adding or replacing original functionalities to the system. As anyone can imagine, this kind of freedom can also be exploited by malicious individuals and used as an entry point to vehicle's basic functions and controls. (Day, 2016)

- Attack on the application layer (MirrorLink): Another study prove that it is possible to gain access to an infotainment system by exploiting a security gap in MirrorLink protocol. MirrorLink is a protocol that enables the connection of a smartphone to a vehicle's infotainment system and control some of its functions, make phone calls, stream content from the phone to the vehicle's screens or even display on the screen applications that run on the phone. Similar protocols have developed in the last few years with the same functionality like Android Auto, Apple CarPlay or GENIVI. (Mazloom, Rezaeirad, Hunter, & McCoy)

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

Researchers managed to enable MirrorLink that was by default disabled by the manufacturer, simply by changing a single value of a configuration file using a publicly available firmware update signed by the manufacturer. The attackers after bypassing the signed certificates, using a smartphone, they could gain access and extract data stored on infotainment system's memory chips, obtain application data, kernel and configuration files from these chips. They proved that by using a smartphone, an attacker can send malicious messages on the vehicle's internal CANBus with serious or fatal consequences.

3.10. Countermeasures:

Considering the above examples, it is obvious that an in-vehicle infotainment (IVI) system is a wide attack surface that can be used by attackers to gain access to a vehicle's CANBus flow. It is also obvious that sometimes the process was generally easy for someone with the necessary technical skills, and that IVIs and protocols used by them are designed without taking into consideration the security aspect, hypothesizing that attackers would have difficulty gaining physical access to a vehicle. Unfortunately, that is not the case.

- Develop infotainment applications based on safe and secure operating systems such as linux distros or manufacture proprietary instead of old and unsecure like WinCE (MirrorLink).
- Safeguard communication protocols that are used in autonomous vehicles infotainment systems and develop secure pairing methods between mobile devices and IVIs.
- Run processes at a lower privileged level that does not grant the application access to the CAN controller.
- Run applications on a virtual and isolated model similar to Android OS or iOS.
- Ensure that Bluetooth and WIFI is in not discoverable mode by default or be fully deactivated when possible.
- Create the infrastructure necessary to provide fast patches and firmware updates to infotainment systems. Also, manufacturers need to find ways to sign and secure patches from unauthorized access.
- Separate non-critical system components from critical ones and isolate the latter ones in their own network. Non-critical systems should have read-only rights to the CAN network.
- Secure and tighten authentication methods (two factor authentication).

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

Local Attack Vectors			
Part	Available attacks	Severity	Difficulty
Image sensors	Physical obstraction	Medium	Easy
RADAR	Physical obstraction Jamming	Medium	Easy
LIDAR	Physical obstraction Spoofing Time Spoofing	Medium to High	Easy
Motor sensors	via CANBus & OBD	High	Medium
ECUs	via CANBus & OBD	High	Medium
CANBus	Physical & Remote	High	Medium
OBD II	Physical & Remote OBD Dongles Cellular Networks Bluetooth Software hacks	High	Medium
Infotainment systems	USB & SD WIFI Bluetooth GPS Cellular Networks Software hacks	Medium to High	Medium
USB & SD	Physical access Software hacks Viruses	Medium	Medium
WIFI	Remote access to CANBus	Medium to High	Medium

Table 3.1: Local Attack Vectors Matrix

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

4. REMOTE ATTACKS:

4.1. Abstract:

Essential to the success of autonomous driving and the fulfillment of its promises for ease of use and security via the minimization of accidents, is the implementation of various communication technologies into the vehicles. Autonomous vehicles must be able to communicate with other vehicles, with the driver and the passengers, and also with the manufacturer and the authorities such as traffic control stations, GPS satellites and emergency public facilities like the police, fire stations and hospitals. Depending on the location of the other end of the communication party, the distance from the vehicle, and if the party is stationary or mobile, we can categorize wireless communications in autonomous driving in:

- Vehicle 2 Vehicle (V2V): is the wireless transmission of data between motor vehicles. Its main purpose is the avoidance of collisions between vehicles and the reduce of traffic jams in overpopulated metropolitan areas.
- Vehicle 2 Driver (V2D): is the data transfer between the vehicle and its driver via optical and sound interfaces.
- Vehicle 2 Infrastructure (V2I): is the wireless transmission of data between motor vehicles and the underlying motorway infrastructure like RFID readers and cameras, traffic lights, lane markers, streetlights, signage and parking meters.
- Vehicle 2 Everything (V2E or V2X): is the communication between an autonomous vehicle and everything else and contains V2V, V2I and V2D.
- Vehicle 2 Pedestrian: is the communication between an autonomous vehicle and pedestrians via applications that warn the pedestrians or vice versa.
- Vehicle 2 Network: is the communication between an autonomous vehicle and application servers supporting V2N applications, while the parties communicate with each other using Evolved Packet Switching (EPS). V2X services are required for different applications and operation scenarios.

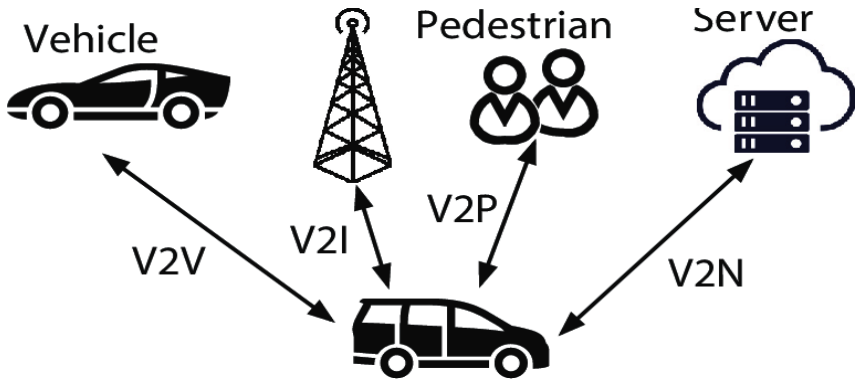


Figure 4.1: Vehicular communication modes

Also, depending on the type of communication, different protocols are used that fit the profile and the needs of each category such as 5G+, Bluetooth or WIFI.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

4.2. V2V & V2I architecture:

Like every wireless and bidirectional transmission of data, AVs must have the following three components:

- Vehicle On-Board Unit or Equipment (OBU or OBE): An OBU is comprised by a radio transceiver (DSRC or WAVE), a GPS system, a processing unit that computes the data from sensors and transceivers, and then presents them to a human machine interface for the driver to understand. An OBU is responsible for the communication between a vehicle and RSUs and other nearby vehicles. They transmit status messages in set intervals, in order to provide GPS location data to other vehicles and facilitate safety applications between them. OBUs also gather and store vehicle data together with GPS positioning information and transmit those to nearby RSUs.
- Roadside Unit or Equipment (RSU or RSE): RSUs are located at infrastructure nodes like intersections, interchanges and other locations and provide an interface to nearby vehicles. An RSU is composed by a radio transceiver (DSRC or WAVE), a processing unit, a V2I communications interface and it also has a GPS unit attached. The RSU via the communications interface receives and sends data from and to vehicles respectively in order to avoid collisions and prevent accidents and traffic jams by prioritizing messages. Message prioritization works by giving high priority to messages that have to do with safety and low priority to messages that are about various other vehicle applications or entertainment related messages. (Gáspár, Zsolt, & Aradi, 2014)
- Safe Communication Channel: As every other critical communication interaction between nodes, security is essential when it comes to V2V and V2I communications. The importance of data transmitted between vehicles and smart infrastructure nodes demands that a secure, without interferences, comms channel is used. Also important is the timing in delivering vehicle information to other vehicles and infrastructure. In order to avoid collisions or inform about road conditions, accidents and traffic jams, data must be delivered in a timely manner. But most importantly, the communication protocol and media must be carefully chosen to provide security. Protocols designed and intended for home and office use like IEEE 802.11a, may drive down implementation costs, but do not provide characteristics like high data rate delivery with low latency in hundreds of nodes/vehicles which are constantly on the move. The information provided above dictates that a secure, fast and adaptable communication channel is essential to the successful implementaion of autonomous driving V2V and V2I networks.

4.3. Mobile Ad Hoc Networks (MANETs):

Autonomous vehicles, which are always on the move, will form Mobile Ad Hoc Networks (MANETs) to talk to each other.

Generally, there are two distinct approaches for enabling wireless mobile units to communicate with each other: infrastructure-based and ad hoc.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

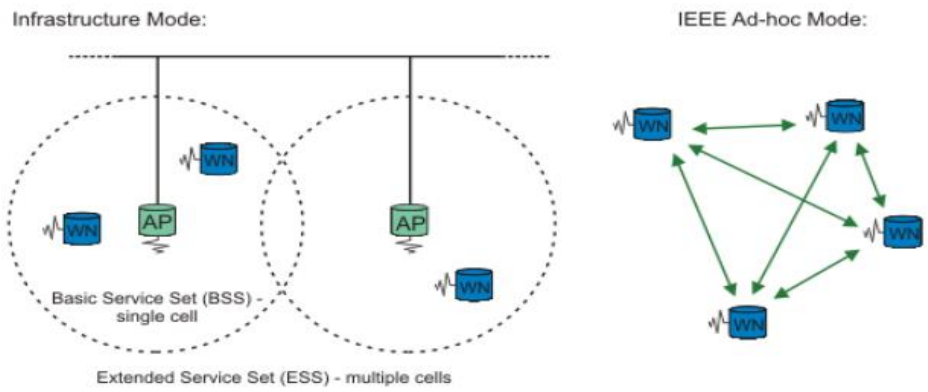


Figure 4.2: Infrastructure-based and Ad Hoc networks example

Wireless mobile networks have been based on cellular network designs and relied on good infrastructure support, in which mobile devices communicate with access points (or base stations) connected to the fixed network infrastructure. Typical example of this kind of wireless networks is the GSM network that our mobile phones use today.

In recent years the widespread availability of wireless communication and handheld devices has initiated the research for self-organizing networks that do not require a pre-established infrastructure. These ad hoc networks consist of autonomous nodes that work in conjunction in order to pass information. Usually these nodes play the roles of end systems and routers at the same time. Ad hoc networks can be subdivided into two categories: static and mobile. In static ad hoc networks the position of a node may not change once it has become part of the network.

In mobile ad hoc networks, systems may move in random directions. A Mobile Ad Hoc Network is commonly called a MANET. Mobile Ad Hoc Networks creates the basis for connectivity between vehicles which is called Vehicular Ad Hoc Network. It is a variation of MANETs, with the emphasis being now the node is the vehicle. A MANET is some way like an autonomous system in which mobile hosts connected by wireless links are free to move randomly and often act as routers at the same time.

A MANET is a collection of wireless mobile nodes that dynamically form a network to exchange information without using any pre-existing fixed network infrastructure or a centralized administration. MANET nodes are equipped with wireless transmitters and receivers using antennas, which may be omni-directional (broadcast), highly -directional (point-to-point), possibly steerable, or some combination thereof. At a given point in time depending on the nodes' positions and their transmitter and receiver coverage patterns, transmission power levels and co-channel interference levels, a wireless connectivity in the form of a random, multi-hop graph or ad hoc network formulates between the nodes. This ad hoc topology may change with time as the nodes move or adjust their transmission and reception parameters. (Gáspár, Zsolt, & Aradi, 2014)

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

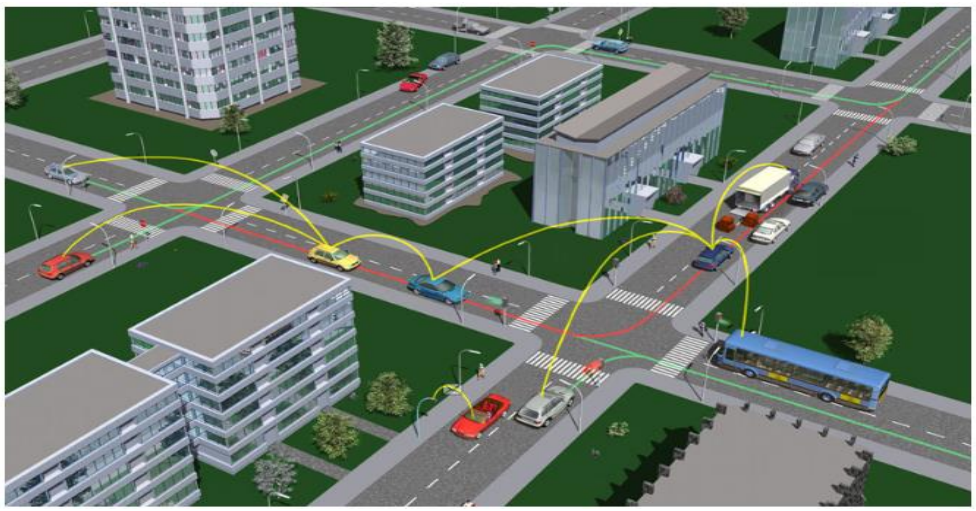


Figure 4.3: Vehicular Ad Hoc Network, VANET

In such an environment, it may be necessary for one mobile host to use the aid of other hosts in forwarding a packet to its destination, due to the limited range of each mobile host's wireless transmissions.

MANETs are a very important part of communication technology that supports truly pervasive computing, because in many contexts information exchange between mobile units cannot rely on any fixed network infrastructure, but on rapid configuration of wireless connection. Next generation of mobile communications will include both infrastructure wireless networks and infrastructure less Mobile Ad Hoc Networks (MANETs).

In VANETs, just like MANETs, it is very important to develop an efficient, reliable and secure routing protocol. The main challenge of any routing protocol is to find an optimal way of communication between nodes (vehicles). Most known VANET routing protocols are the Ad-hoc On Demand Vector Routing (AODV) (C. E. Perkins & E. M . Royer) which uses a demand-driven route establishment procedure. And the Dynamic Source Routing (D. B. Johnson & D. A. Maltz, 1996) which is also classified as reactive in nature. Routes are stored in cache and it is expected that source will have complete knowledge of hop-by-hop route to the destination.

Main objectives of a VANET is:

- Road Traffic Safety: Reducing the number of fatalities/injuries on the roads by alerting the drivers about dangers in advance.
- Comfort and Quality of Road Travel: Provide comfort applications for drivers and passengers like advanced traveler information systems, electronic payment systems, variable message signs and electronic toll collection, etc.

Some of the key characteristics of a VANET model are as follows:

- Dynamic Topology: VANET environment has a constantly changing topology due to high mobility of the vehicles. The connection between two vehicles travelling with average suburban speed limits in opposite directions lasts for a very short time. This connection time goes much lesser as the speed of the vehicles increases in a freeway/highway environment.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

- Frequent Disconnections: The link connection between the vehicles in VANET has frequent disconnections because of the high movement of the nodes and frequent change in the environment.
- Mobility Modeling: In order to implement VANET efficiently and realistically, an accurate mobility model is required for this highly dynamic environment of VANET.
- Predictable Mobility Patterns: In VANET environment most of the vehicles move on pre-defined roads and highways. This allows the use of predictable mobility patterns in network design. (Sabih-ur Rehman, M. Arif Khan, Tanveer Zia, & Lihong Zheng, 2013)

4.4. Standards and communication Protocols in Autonomous driving (V2V & V2I):

Three categories of standards are implemented in vehicular networks.

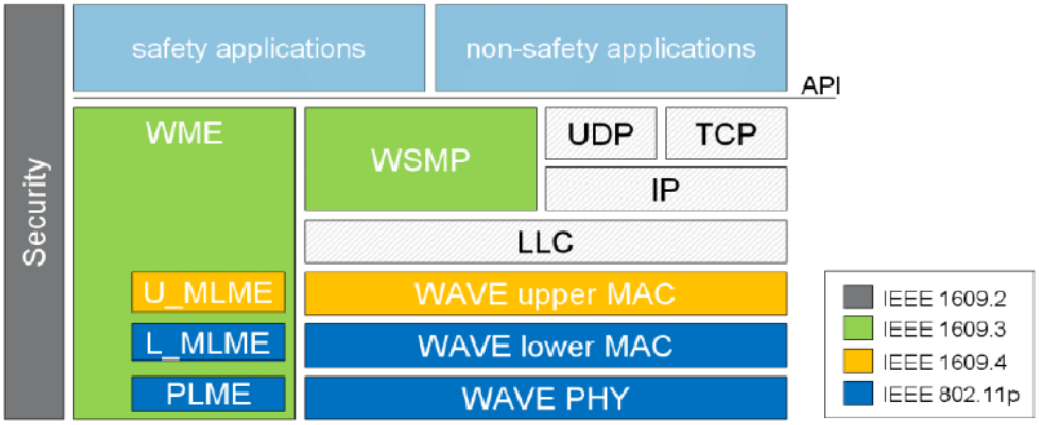


Figure 4.4: V2V standards and communication stacks

4.4.1. IEEE 802.11p (WAVE):

WAVE or Wireless Access in Vehicular Environment which is currently under development derives from DSRC (Dedicated Short Range Communications). DSRC operates in the 5.9GHz band with a bandwidth of 75MHz and a range of 1km and can only be used by for vehicle-to-vehicle and vehicle-to-infrastructure communications. Private services are also permitted in order to spread the deployment costs and to encourage the quick development and adoption of DSRC technologies and applications. Although DSRC spectrum is allocated in the US, the same spectrum is saved in the EU for vehicle communications for compatibility reasons.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

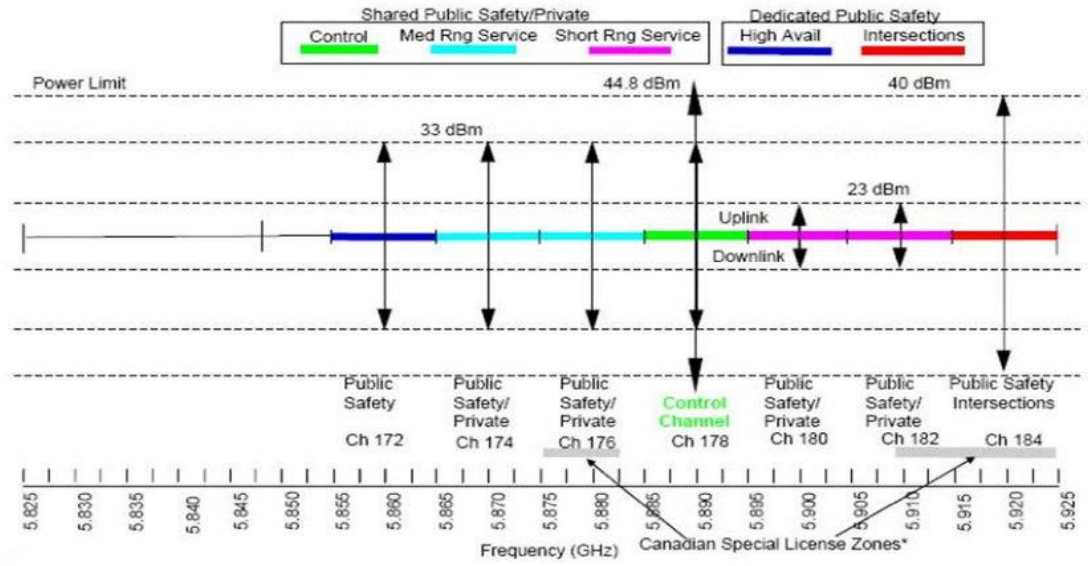


Figure 4.5: DSRC-spectrum-band-and-channels-in-the-US

4.4.2. IEEE 1609:

IEEE 1609 defines the architecture, the communication model, the management structure, the security mechanisms and the physical access for high speed (<27 Mb/s), short range (<1000m) and low latency wireless communications in vehicular networks.

The IEEE 1609 family of standards define the three basic components of a V2V or V2I communication systems which we described earlier: Vehicle On-Board Unit or Equipment (OBU or OBE), Roadside Unit or Equipment (RSU or RSE), and Communication channel between OBU & RSU.

4.4.3. SAE J2735:

SAE J2735 is the DSRC message set dictionary that defines message set, its data frames and data elements specifically for use by applications intended to utilize the (DSRC/WAVE) communications systems. (SAE)

SAE J2735 dictionary contains:

- 15 messages
- 72 data frames
- 146 data elements
- 11 external data entries

The most important message type is the basic safety message, also called “heartbeat” message because it is constantly being exchanged with nearby vehicles. This way, vehicles in the same vehicular network, receive and send information about:

- Temporary ID
- Time

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

- Latitude
- Longitude
- Elevation
- Positional Accuracy
- Speed and Transmission
- Heading
- Acceleration
- Steering Wheel Angle
- Brake System Status
- Vehicle Size

Except from "heartbeat" other DSRC messages are:

- A la carte message -- composed entirely of message elements determined by the sender, allowing for flexible data exchange.
- Emergency vehicle alert message -- used for broadcasting warnings to surrounding vehicles that an emergency vehicle is operating in the vicinity.
- Generic transfer message -- provides a basic means to exchange data across the vehicle-to-roadside interface.
- Probe vehicle data message -- contains status information about the vehicle to enable applications that examine traveling conditions on road segments.
- Common safety request message -- used when a vehicle participating in the exchange of the basic safety message can make specific requests to other vehicles for additional information required by safety applications.

Up until now we have described standards that are used in both V2V and V2I communications. V2I communications will probably utilize interfaces with other wireless technologies different to MANETs for efficient vehicle-to-infrastructure communication. V2I communication is essential to autonomous vehicles function since the data transmitted between vehicle and road infrastructure prevents, via data processing and using algorithms, high risk situations and AV impacts with other vehicles or stationary objects and structures.

4.5. Mobile networks (GSM, UMTS, 5G+, Bluetooth, WIFI):

Mobile networks such as the ones our mobile phones use, can also be utilized in autonomous driving. GSM (2G) was the first widespread mobile network but was originally designed only for voice

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

telephony. Since then with various revisions (phases) and extensions like GPRS and EDGE, GSM was capable of transferring data between mobile devices but with very slow rates by today's standards. UMTS (also known as 3GPP) was the third generation of broadband cellular network and is based on W-CDMA radio technology offering higher bandwidth from GSM and transfer speeds that reached to 7.2Mbps. The need for higher speeds and the transmission of large video files or video conferencing on mobile devices lead to 4G or LTE which is widely used today and maxes out at 100Mbps. (Vora, 2015)

5G is the latest generation of cellular mobile communication networks and succeeds 4G. It is designed based on needs like high performance data rates, reduced latency, energy saving, cost reduction and massive device connectivity. Although specifications are not final at the time of writing of this essay, based on the design characteristics, it is clear that 5G is ideal for vehicle communication either with other vehicles or the infrastructure. The second phase of 5G specifications will be completed and submitted to the International Telecommunication Union in April 2020, but design is aiming at speeds of up to 20Gbps, and early deployments show latency reduced of about 15% to 50%. (Vora, 2015)

5G networks achieve these higher data rates by using higher frequency radio waves, in the millimeter wave band around 28 and 39GHz while previous cellular networks used frequencies in the microwave band between 700MHz and 3GHz. A second lower frequency range in the microwave band, below 6GHz, will be used by some providers, but this will not have the high speeds of the new frequencies. Because of the more plentiful bandwidth at these frequencies, 5G networks will use wider frequency channels to communicate with the wireless device, up to 400MHz compared with 20MHz in 4G LTE, which can transmit more data (bits) per second. OFDM (orthogonal frequency division multiplexing) modulation is used, in which multiple carrier waves are transmitted in the frequency channel, so multiple bits of information are being transferred simultaneously, in parallel (Massive MIMO).

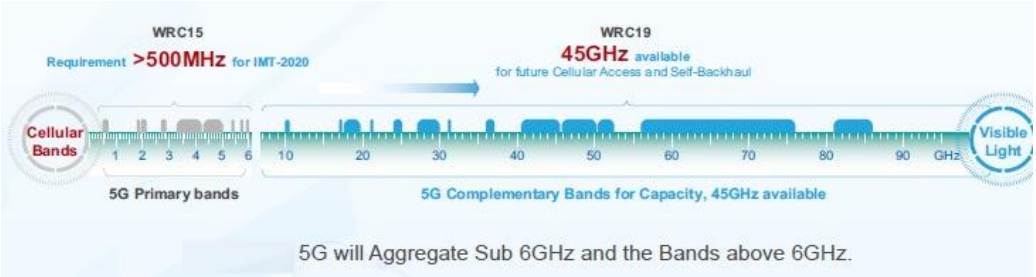


Figure 4.6: 5G Spectrum

Because waves of this size are absorbed by gases in the atmosphere and have shorter range than microwaves, the cells on a 5G network will have to be smaller (the size of a city block) than those of 4G/LTE networks which could reach the size of many kilometers depending on the number of subscribers connected to the cell. Also, millimeter wave antennas are smaller in size and there won't be the need to have them installed on towers, but on telephone poles or buildings. These design specifications limit the application of 5G networks on populated areas and big cities, since the cost of network infrastructure is prohibiting the application on a larger scale for the time being.

Data rates of 5G make the technology ideal for autonomous driving, since autonomous vehicles need to receive, send and process huge amounts of data coming from other vehicles or the infrastructure.

4.5.1. Bluetooth:

Another wireless data transmission technology that can be utilized for small distance communication between vehicles and/or infrastructure is Bluetooth.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

Bluetooth technology is a wireless communications technology that is simple, secure, and can be found almost everywhere. It was developed to replace cables between devices and are widely used today even in the automotive industry on devices like Hands Free headsets, Bluetooth enabled speakers, or health monitoring devices that monitor vital signs of the driver and the passengers. The development of Bluetooth is coordinated by the Car Working Group, started in 2000 and continues to develop via different revisions and added features.

Bluetooth devices when paired, create small ad-hoc networks (piconets) which are created ad hoc every time two or more Bluetooth devices are in proximity. Each device can communicate with up to seven other devices in the same piconet and each device can also be connected to unlimited piconets simultaneously. This means that Bluetooth as a technology can really be used in vehicular networks as the number of connections possible are limitless.

The range of Bluetooth devices depends on the class of the radio used. For example, we have:

- Class 3 radios – that have a range of up to 1 meter or 3 feet
- Class 2 radios – most commonly found in mobile devices – have a range of 10 meters or 33 feet
- Class 1 radios – used primarily in industrial use cases – have a range of 100 meters or 300 feet

Bluetooth technology operates in the open and unlicensed industrial, scientific and medical (ISM) band at 2.4 to 2.485 GHz, using a spread spectrum, frequency hopping, full-duplex signal at a nominal rate of 1600 hops/sec. The 2.4 GHz ISM band is available and unlicensed in most countries. The most commonly used radio is Class 2 and uses 2.5 mW of power. Bluetooth technology is designed to have very low power consumption. This is reinforced in the specification by allowing radios to be powered down when inactive.

Bluetooth technology's adaptive frequency hopping (AFH) capability was designed to reduce interference between wireless technologies (such as WLAN) sharing the 2.4 GHz spectrum. AFH works within the spectrum to take advantage of the available frequency. This is done by the technology detecting other devices in the spectrum and avoiding the frequencies they are using. This adaptive hopping among 79 frequencies at 1 MHz intervals gives a high degree of interference immunity and also allows for more efficient transmission within the spectrum. For users of Bluetooth technology this hopping provides greater performance even when other technologies are being used along with Bluetooth technology. The AFH technology is shown in the following diagram. (Dimitrakopoulos & Bravos, 2017)

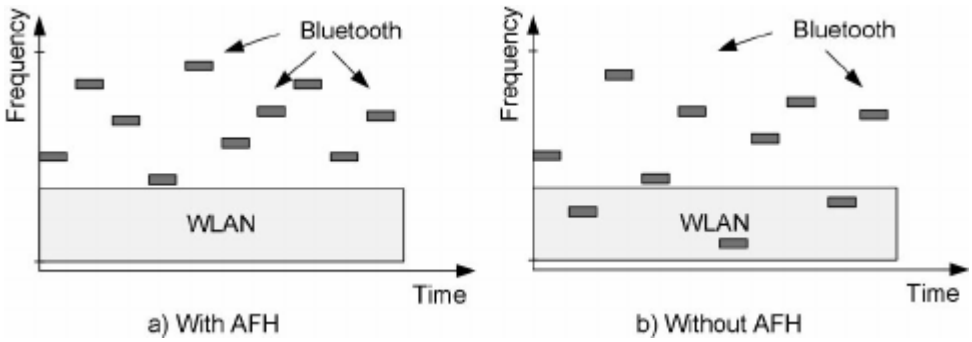


Figure 4.7: Bluetooth with and without AFH

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

The major revisions of Bluetooth can be found in the following diagram along with their major changes in each release.

Year Introduced	Bluetooth Version	Feature
2004	2.0	Enhanced Data Rate
2007	2.1	Secure Simple Pairing
2009	3.0	High Speed with 802.11 Wi-Fi Radio
2010	4.0	Low-energy protocol
2013	4.1	Indirect IoT device connection
2014	4.2	IPv6 protocol for direct internet connection
2016	5.0	4x range, 2x speed, 8x message capacity + IoT

Table 4.1: Bluetooth major releases

The most recent iteration of Bluetooth is 5.1 presented in January 2019 and the major areas of improvement over previous versions are:

- Angle of Arrival (AoA) and Angle of Departure (AoD): this feature offers the capability to identify the direction of a transmitting Bluetooth device from a receiving antenna, which means that Bluetooth 5.1 devices can pinpoint their precise location.
- GATT Caching: Whenever a client device connects, it performs "service discovery" to see what the server device supports. This takes time and energy. Bluetooth 5.1 performs more aggressive caching, and clients can skip the service discovery stage when nothing has changed. These "GATT caching enhancements" mean the connection happens faster and less energy is spent.
- Advertising Channel Index & Periodic Advertising Sync Transfer: Bluetooth devices can advertise (available to connect to nearby devices) cycling through channels 37,38 and 39 in order. With 5.1 version the device can advertise its readiness by selecting channels at random. his reduces the odds that two Bluetooth devices will interfere with each other and "talk over" each other on the same channels when advertising their readiness to connect, and it'll be helpful in places with a lot of Bluetooth devices. Also, Periodic Advertising Sync Transfer saves power when two Bluetooth devices are connected. (Hoffman, 2019)

Latest advances in the Bluetooth protocol, make it ideal for various different automotive usages and not only for connecting devices as it happens today. Bluetooth devices and therefore Bluetooth enabled cars can pinpoint with great precision their location, discover nearby other vehicles and transfer data between them or the infrastructure. The same goes also for Bluetooth enabled infrastructure parts like traffic lights that can now warn vehicles about traffic flow and pedestrians.

Even today, several manufacturers offer Bluetooth capable traffic control devices. These are capable for privileging the public transport at the intersections or measuring the traffic and pedestrian flows with the help of the electronic devices installed with Bluetooth radio (such as smartphones, tablets, navigation units etc.) These systems detect anonymous Bluetooth signals transmitted by visible Bluetooth devices located inside vehicles and carried by pedestrians. This data is then used to calculate traffic journey times and movements. It reads the unique MAC address of Bluetooth devices that are passing the system.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

By matching the MAC addresses of Bluetooth devices at two different locations, not only the accurate journey time is measured, privacy concerns typically associated with probe systems are minimized.

4.5.2. WIFI:

WIFI or WLAN can be used in vehicular networks as mentioned earlier (802.11p WAVE). WIFI is based on the IEEE 802.11 standards and is a trademark of WIFI Alliance. WIFI today is used by hundreds of different devices from computers and smartphones to refrigerators and air conditions. WIFI access points have a typical range of 20m indoors and a greater range outdoors. Hotspot coverage can be as small as a single room with walls that block radio waves, or as large as many square kilometers achieved by using multiple overlapping access points.
Different versions of WIFI exist, with different ranges, radio bands and speeds. WIFI most commonly uses the 2.4 gigahertz (12cm) UHF and 5.8 gigahertz (5cm) SHF ISM radio bands; these bands are subdivided into multiple channels. Each channel can be time-shared by multiple networks. These wavelengths work best for line-of-sight. Many common materials absorb or reflect them, which further restricts range, but can tend to help minimize interference between different networks in crowded environments. At close range, some versions of WIFI, running on suitable hardware, can achieve speeds of over 1 Gbit/s.

	802.11 (Legacy)	802.11b (Legacy)	802.11a (Legacy)	802.11g (Legacy)	802.11n (HT)	802.11ac (VHT)	802.11ax (HE)
Year Ratified	1997	1999	1999	2003	2009	2014	2019 (Expected)
Operating Band	2.4 GHz/IR	2.4 GHz	5 GHz	2.4 GHz	2.4/5 GHz	5 GHz	2.4/5 GHz
Channel BW	20 MHz	20 MHz	20 MHz	20 MHz	20/40 MHz	20/40/80/160 MHz	20/40/80/160 MHz
Peak PHY Rate	2 Mbps	11 Mbps	54 Mbps	54 Mbps	600 Mbps	6.8 Gbps	10 Gbps
Link Spectral Efficiency	0.1 bps/Hz	0.55 bps/Hz	2.7 bps/Hz	2.7 bps/Hz	15 bps/Hz	42.5 bps/Hz	62.5 bps/Hz
Max # SU Streams	1	1	1	1	4	8	8
Max # MU Streams	NA	NA	NA	NA	NA	4 (DL only)	8 (UL & DL)
Modulation	DSSS, FHSS	DSSS, CCK	OFDM	OFDM	OFDM	OFDM	OFDM, OFDMA
Max Constellation / Code Rate	DQPSK	CCK	64-QAM, 3/4	64-QAM, 3/4	64-QAM, 5/6	256-QAM, 5/6	1024-QAM, 5/6
Max # OFDM tones	NA	NA	64	64	128	512	2048
Subcarrier Spacing	NA	NA	312.5 kHz	312.5 kHz	312.5 kHz	312.5 kHz	78.125 kHz

Table 4.2: IEEE 802.11 Standards

The general WIFI that is based on 802.11 standards and is used on most WIFI enabled devices though cannot be used in vehicular networks since it is not secure enough for critical operations and can only be used for infotainment applications. As previously described only the IEEE 802.11p WAVE (DSRC) which is special developed with vehicular networks in mind, is capable for safe and reliable communications in V2X applications.

4.5.3. Cellular V2X (C-V2X):

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

A specially designed IEEE standard also exists that describes the technology to meet the requirements of V2X communications. C-V2X was developed within the 3GPP (3rd Generation Partnership Project) to to replace the US promoted Dedicated short-range communications (DSRC) and the Europe originated Cooperative Intelligent Transport Systems (C-ITS) As such standards are decisive steps towards the target autonomous driving and clues to market influence, especially as the National Highway Traffic Safety Administration (NHTSA) plans to propose the compulsory introduction of vehicle-to-everything technology off 2020 for all US vehicles.

Cellular-V2X (C-V2X) as initially defined as LTE V2X in 3GPP Release 14 is designed to operate in several modes. (5GAA, n.d.)

- Device-to-device is Vehicle-to-Vehicle (V2V), Vehicle-to-(Roadway) Infrastructure (V2I) and Vehicle-to-Pedestrian (V2P) direct communication without necessarily relying on network involvement for scheduling.
- Device-to-cell tower is another communications link which enables network resources and scheduling and utilizes existing operator infrastructure. Device-to-cell tower communications constitute at least part of the V2I proposition and are important to end-to-end solutions.
- Device-to-network is the V2N solution using traditional cellular links to enable cloud services to be part and parcel of the end-to-end solution.

In the device-to-device mode (V2V, V2I, V2P) operation, C-V2X does not necessarily require any network infrastructure. It can operate without a SIM, without network assistance and uses GNSS (Global Navigation Satellite Systems) as its primary source of time synchronization.
C-V2X also supports V2N applications utilizing existing cellular networks where other voices and data communications occur. V2N would deliver network assistance and commercial services requiring the involvement of a Mobile Network Operator (MNO). Provides enhanced communication range and reliability in dedicated ITS 5.9 GHz spectrum that's independent of a cellular network, as well as network communications (V2N) in traditional mobile broadband licensed spectrum. (5GAA, n.d.)

When compared with 802.11p-based technologies, Direct C-V2X provides increased communication range (~2X), better non-line-of-sight (NLOS) performance, enhanced reliability, and cost efficiency without relying on cellular network assistance or coverage for enhanced safety services.

C-V2X has many advantages compared to other V2V solutions (Qualcomm, 2018):

- Direct safety communication independent of cellular network: Low latency Vehicle to Vehicle (V2V), Vehicle to Infrastructure (V2I), and Vehicle to Person (V2P) operating in ITS bands (e.g. 5.9 GHz)
- Network communications for complementary services: Vehicle to Network (V2N) operates in a mobile operator's licensed spectrum
- C-V2X complements other ADAS sensor technologies: compatible with radars, lidars, cameras and ultrasonic sensors
- Enhanced range and reliability
- More cost efficient than other technologies
- Up to 500km/h relative speed support
- Forward compatible evolution path to 5G

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

C-2VX has evolved over the years and is now implemented into 5G networks. 5G NR (New Radio) will be utilized which uses a new OFDM (Orthogonal frequency-division multiplexing) based wireless standard and is now supported by most electronic device and vehicle manufacturers. 5G NR is developed by Qualcomm, completed the standardization process in December 2017 and incorporates a lot of new technologies like Scalable OFDM numerology with 2^n scaling of subcarrier spacing, Flexible self-contained slot structure, Advanced ME-LDPC and CA-Polar channel coding, Massive MIMO and Mobile mmWave.

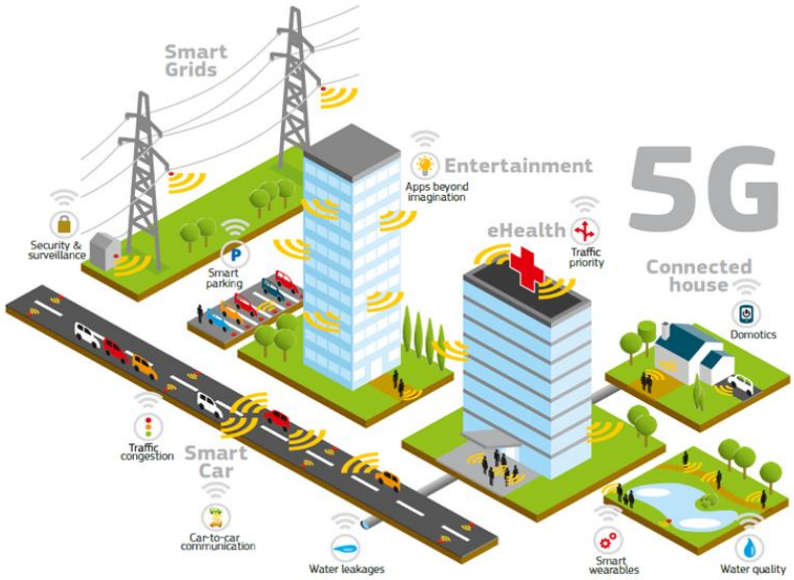


Figure 4.8: 5G NR utilization and use cases (source: National Instruments)

5G NR provides the following advantages when compared to traditional DSRC (WAVE) solutions (Qualcomm, 2018):

- Broad ecosystem support
- a unified connectivity fabric to expand into new industries
- C-V2X has a clear and forward compatible evolution path to 5G NR
- 5G NR C-V2X provides lower latency, ultra-reliable communication and high data rate for autonomous driving

The most logical communications solution for autonomous vehicles would be a combination of all the technologies described. Cellular 5G+ networks could be used for longer range connectivity between vehicles and infrastructure nodes and DSRC based communication for short range and peer to peer messaging between vehicles on the network. LTE-V2X and 5G+ networks can also be used connectivity between cars.

4.6. SECURITY CONCERNS ON REMOTE COMMUNICATIONS FOR AVs:

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

Various technologies, standards and protocols are going to be used in autonomous driving and vehicular networks for communication purposes between the vehicles and their surroundings. Complexity and reliability are the key factors that manufacturers have to face. Combining many new technologies makes for an extremely complex design and creates the need for standardization. Manufacturers need to agree on standards and use the same protocols of communication throughout the entire fleet of vehicles, infrastructure devices and applications. Also, the significance of data exchanged between nodes on a network, like security information, dictates that all parts of the autonomous driving environment should be reliable and secure. Downtime of any part of the autonomous driving architecture could have catastrophic results costing lives and vast amounts of money.

Protecting the entire AV environment is crucial from malicious attacks and from malfunctions. It is evident that the more different technologies used, the more the attack surface widens, since every technology's security flaws are combined and added to the list of problems that have to be addressed. We will explore each technology, standard or protocol's security gaps separately exposing the size of the problem and the difficulty to predict and address them. We will also present known attacks and security gaps that have already been reported and addressed.

Malfunctions: As any other complex systems that relies on new technologies, there is an increased risk of system malfunction, temporary or permanent, that could lead to disastrous results. V2V, V2I, or V2X systems are now practically at their infant stages, undergoing testing, and it is planned to be in production by major automotive makers not earlier than 2021. Technologies are new and immature at the present time.

A lot of articles and conversations have been made about the first lethal accident involving an autonomous vehicle that took place on March 2018 and involved an Uber self-driving car and a woman trying to cross the road carrying a bicycle. The woman was killed after the impact while the car was doing 38mph and failed to break in time. Some experts claimed that the car's lidar and radar sensors should have picked the human 6 seconds before the impact taking into consideration the weather conditions, and others blame the car's emergency braking system that was reportedly deactivated to help ensure less erratic testing.

After the accident, Uber had halted their tastings for 9 months and were resumed on December 2018, after extensive testing on their vehicles and training for drivers, and also changed the testing procedure by making compulsory that a second passenger will always be assigned to each vehicle monitoring the car's systems.

Firstly, we are going to focus on general types of attacks and concerns about autonomous driving.

Hacking: Being an IT dependent system, a V2V, V2I or V2X communication system is vulnerable to attacks made by hackers. A hacker could alter the information received by one or more of the processing units on board an autonomous vehicle, provide false data, and drive the vehicle to a predefined or preferable by the hacker location, or perform an action controlled remotely. Depending on the technology that the attacker could choose to exploit, various techniques and methods are being used and some of them will be presented later in this thesis.

Plethora of protocols: Because V2X communication is not yet standardized, there are various different protocols or technology used by the automotive manufacturers. These differences could lead to fatal

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

results, as autonomous vehicles could not be able to recognise signals sent from a vehicle from a different manufacturer.

Cost: Right now, the cost to produce and implement such systems in current vehicles is anything but cheap and the computing power requirements are also big for the current technology offerings. Manufacturers need to simplify and excell obstacles of current tech in order for V2X to be viable and successful.

Privacy Concerns: A very big concern when it comes to autonomous vehicles is privacy. There are a lot of drivers and researchers that are worried about the information received and processed by the sensors and the processing units on board an autonomous vehicle. These range from real time data such as current speed and location, to non-real time data such as previous destinations, data about the habits and most frequent places a driver prefers. This data can always be used by malicious individuals in order to harm the driver and the passengers. There are also concerns that this data can be used by or sold from the vehicle's manufacturer to companies that gather data and use them for commercial purposes.

Additional security concerns must be raised by the constant changing topology of the wireless networks that are created between autonomous vehicles or the infrastructure nodes, the absence of certification authority, and the lack of a centralized point of management.

Wireless & Ad Hoc networks: Anyone within range with a wireless network interface controller can attempt to access a network. Autonomous vehicles communication networks are susceptible to all kind of attacks that typical wireless networks are. In addition to those common vulnerabilities, ad hoc networks have also security gaps and problems due to their constantly changing topology.

Some of the most common security threats for wireless networks are mentioned below:

- Man-in-the-Middle (MiM): It is the most common type of attack on a wireless network and allows an attacker to intercept data packages that are exchanged between nodes. One of the most common tactics used in MiM attacks is eavesdropping. Attackers will intercept messages between two users who believe they are talking directly to one another. Connections that do not have mutual authentication protocols at both ends particularly vulnerable to these sorts of attacks since authentication protocols are specifically designed to ward off these types of attacks.

- DoS Attacks: WLANs are inherently vulnerable to DoS. Phony messages sent to disconnect users, consume AP resources, and keep channels busy. Current DSRC technology is limited due to the range of frequency used, and as consequence the amount of vehicles connected to a certain network cannot be large. A malicious individual could feed the the V2V, V2I or V2X communication system with a plethora of signals and lead to a situation that these signals, that are important for the vehicle's operation, don't reach through leading to a disaster.

- Active Interfering & Impersonation: Basically, typical access points created by malicious individuals that can infiltrate into the vehicular network and could impersonate a vehicle or an infrastructure node on a network. This way they could allow the adversary to delete messages, to inject erroneous messages, to modify messages violating availability, integrity, authentication, and non-repudiation. Ad hoc networks do not have a centralized piece of machinery such as a name server, which could lead to a single point of failure and thus, make the network that much more vulnerable.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

- Sniffing: Packet analyzers are programs that can be used in wireless networks to intercept packets and provide the intruder info about their contents. This way crucial information about the function of a vehicle or a message exchanged by a vehicle and another node can be read and exploited.

- Masquerading: In this kind of attack, the attacker actively pretends to be another vehicle by using false identities and can be motivated by malicious or rational objectives. Then he can diffuse wrong information in the network to affect the behavior of other drivers.

- Byzantine fault: In a byzantine fault, a component such as a vehicle or an infrastructure node can inconsistently appear both failed and functioning to failure-detection systems, presenting different symptoms to different observers. The compromised nodes may seemingly operate correctly, but, at the same time, they may make use of the flaws and inconsistencies in the routing protocol to undetectably distort the routing fabric of the network. In addition such malicious nodes can also create new routing messages and advertise non-existent links, provide incorrect link state information and flood other nodes with routing traffic, thus inflicting byzantine failures on the system. Such failures are severe, because they may come from seemingly trusted nodes. Even if the compromised nodes were noticed and prevented from performing incorrect actions, the erroneous information generated by the byzantine failures might have already been propagated through the network.

- Ad hoc networks problems: As mentioned, ad hoc networks may consist of hundreds or even thousands of nodes and are sporadic in nature, have a dynamically changing topology, and lack a a certification authority and a centralized monitoring or management point. Standard security solutions would not be good enough since they are essentially for statically configured systems. This gives rise to the need for security solutions that adapt to the dynamically changing topology and movement of nodes in and out of the network.

Bluetooth attacks: Bluetooth protocol which is used in automotive products today such as handsfree devices, speakers or as a communication protocol between mobile devices and vehicles, is succeptible to typical wireless network flaws as it creates an ad hoc network (piconet) between connected nodes. Bluetooth also can be exploited using specific to this protocol methods such as BlueJacking, BlueSnarfing, BlueBugging, BlueBump, BlueDump, BluePrinting, Blueover, BlueBorne, Fuzzing, Off-Line PIN Recovery, Brute-Force, Reflection/Relay, Backdoor etc. (Lonzetta , Cope, Campbell , Mohd, & Hayajneh , 2018)

Gaining access to Bluetooth interface of an autonomous vehicle would not be enough. A hacker’s goal will be to gain access to CANBus via the Bluetooth protocol and Bluetooth connection. Given the fact that more and more Bluetooth enabled devices are being connected to cars, makes Bluetooth security even more important.

Gaps in the Bluetooth protocol have enabled researchers in the recent past to gain access to a car's engine management software. Specifically, Israeli firm Argus Cyber Security in 2017 (Hassan, 2017) reported that it had been able to remotely take control of a car via Bluetooth and stop the car's engine remotely. A leak in the authentication process that affected the Bluetooth pairing and authentication process allowed them to brute-force the secret PIN of the pairing process. That hack was not adequate though, since they also hacked Bosch's Drivelog Connect ODB-II dongle to allow them to get to the CANBus and inject malicious messages into it.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

Another recent (2018) hack has been performed by Privacy4Cars (privacy4cars, 2018), an application developer for smartphones designed to help erase personally identifiable information (PII) from modern vehicles. The hack was named "CarsBlues" and exploits the infotainment systems of several makes via the Bluetooth protocol and can be performed in a few minutes using inexpensive and readily available hardware and software and does not require significant technical knowledge. Upon discovery, Amico, a vehicle privacy and cybersecurity advocate, immediately notified the Automotive Information Sharing and Analysis Center (Auto-ISAC), the organization established by the automotive industry to share and analyze intelligence about emerging cybersecurity risks among its members. Amico recently noticed that at least two manufacturers have made systematic updates to their new 2019 models, making those new models immune to CarsBlues.

Autonomous vehicles will surely be a part of the IoT in the coming future. Bluetooth devices that are connected to these cars will have access to a large amount of information about our lives, behaviors, and will allow advertisers to send us targeted ads, and track our driving habits. So, even though Bluetooth hacks alone are not able to provoke car accidents, they can surely invade our privacy and share private information to the highest bidder. Also, despite the fact that known Bluetooth attacks have been patched by car manufacturers or new versions of the Bluetooth protocol, it is almost certain that new attacks and ways of having access to devices that connect to our cars will come to surface in the future.

5G+ and C2-VX:

5G and its next iterations will be probably utilized in autonomous driving and future "smart" cities that enable autonomous driving. That's thanks in large part to cellular vehicle-to-everything (C-V2X) communications, an additional feature of 5G that is designed to deliver direct communications between cars and other smart objects in a town's infrastructure. C-V2X could enable a traffic light to send alerts to vehicles about pedestrians or allow cars to warn other nearby vehicles that there's ice on the road, for example — all without the need for a nearby cell tower as explained in previous chapter of this thesis.

Consequently, the security of the new 5G protocol is very important. 5G as every other new technology, has its flaws and will need improvements and patching. Several studies and articles have already been posted concerning 5G's security. Some of the most recent ones are described below:

- Authentication & Key Agreement (AKA) vulnerabilities: AKA, which is associated with the 3GPP, ensures that a device and a 5G network can authenticate each other while maintaining a confidential data exchange and keeping the user's identity and location private. Researchers in the Information Security Group with the aid of the security protocol verification tool Tamarin, they systematically examined the 5G AKA protocol, taking the specified security aims into account. They concluded that the 5G AKA protocol, although it is very much improved from previous implementations in 3G and 4G, it is insufficient to achieve all the critical security aims of the 5G and that it does not adequately protect privacy from active attackers but admit remedying that problem would not be straightforward. (Basin, et al., 2018)

- Torpedo (Tracking via Paging mEssage DistributiOn): Torpedo as exposed by researchers in University of Iowa and Purdue University (Hussain, Echeverria, Chowdhury, Li, & Bertino, 2019), exploits a weakness in the paging protocol that carriers use to notify a phone before a call or text message comes through. The researchers found that several phone calls placed and cancelled in a short period can trigger a paging message without alerting the target device to an incoming call, which an attacker can use to track a victim's location. Knowing the victim's

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

paging occasion also lets an attacker hijack the paging channel and inject or deny paging messages, by spoofing messages like Amber alerts or blocking messages altogether.

- Piercer & IMSI-Cracking: These attacks are based on Torpedo. Piercer allows an attacker to determine an international mobile subscriber identity (IMSI) on the 4G network and IMSI-Cracking can brute force an IMSI number in both 4G and 5G networks, where IMSI numbers are encrypted. These attacks puts even the newest 5G-capable devices at risk from stingrays, which law enforcement use to identify someone's real-time location and log all the phones within its range. Autonomous vehicles which will implement 5G networks to communicate with the authorities and for vehicle-to-vehicle communications, will probably be also succeptible to similar attacks. (Hussain, Echeverria, Chowdhury, Li, & Bertino, 2019)

- DDoS attacks could be more severe: 5G's high speed bandwidth together with increased number of IoT devices that use it, set the stage for more severe DDoS attacks that could exploit more and more devices increasing the available security gaps and attack vector.

4.7. Remote Attacks Recommendations:

Factoring the attacks that could be made to autonomous vehicles using wireless transmission of data for V2V, V2I and V2X communications presented above, we could propose the following mitigations.

- **In-vehicle Firewalls & Antivirus**: Autonomous and connected vehicles are handling and transferring data such as every other connected to the internet device, much like computers and smartphones. We also connect to our car's devices via different interfaces like the OBD port and USB, WIFI and Bluetooth. Exactly like computers, connected cars can also be targets from viruses and other exploits. This means that there is a need for antivirus software and firewalls to be implemented in them, protecting from malicious execution of code or blocking data transfers to and from unknown sources. Antivirus and firewall in-vehicle solutions would be able to monitor code executed on vehicle's OS and hardware ECUs, compare it to the manufacturer's original software and block access to any unauthorized requests. Antivirus solutions can be implemented from the factory or purchased from third party vendors.

- **IPS/IDS**: Vehicle networks, as every other network can be infiltrated by malicious individuals. Vehicular networks (VANETs) also pose new threats due to the type of communication systems which are utilized in these vehicles that are very reliant to external information exchange. Known attacks such as black hole, DDoS or wormhole and greyhole, are also possible, making IDPS systems necessary. Autonomous vehicles are exchanging critical information such as Cooperative Awareness Messages (CAMs), warning and notification messages, control data between each other and also the infrastructure. Also, autonomous vehicles are always on the move and are not connected to a physical protection system, and attackers do not need physical access to the vehicle. IDPS systems are already available for semi-autonomous vehicles and self-driving cars and offer protection. IDPS devices can monitor packets (packet inspection) of exchanged messages, detect malicious packets, block traffic or reset connections. IDS detect malicious activities using signature-based detection compared to a vast and continuously growing database of known threats.

Traditional IDPS devices installed on computer networks offer 98% reliability rates, but that is not enough for VANETs. Although 98% seems adequate for computer applications, it is catastrophic for an

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

autonomous vehicle where lives are on stake. Unacceptable in this situation are also false positive detections, so it is important that security updates on IDPS devices are continuous and provide protection from new attacks.

- **Security updates & patches**: Modern semi-autonomous vehicles and even more, future full autonomous ones, will rely heavily on software-based systems with millions of lines of code, introducing the risk of software related problems and recalls. The solution to this problem is updates and patches. Updates can now be delivered over-the-air (OTA) without the need for a driver to take his car to a service bay. Updates are not limited to navigation or infotainment systems as they are on current non-autonomous vehicles, but will also be able to address security issues, read vehicle's diagnostics and even provide new features and capabilities. It is important to understand that updates could also target all on-board CPUs of a vehicle and will be able to provide functions like improved driving performance, efficiency, or distribute useful consumer functions and applications. Antivirus software updates and definitions can also be delivered wirelessly addressing newly discovered threats and thus securing the vehicle from promptly from malicious attacks.

Updates and patches should be mutually authenticated by the car and the distributor to ensure that they are correctly intended for the vehicle and that it has not been tampered with, before distributed to a set of ECUs in the vehicle. Updates and patches should also be categorized and offer the owner the decision to apply them or not, and when. Security critical updates should inform the owner about their importance not allowing the user to bypass them.
Much like our computers and smartphones, vehicles that are for some reason inactive for a long period of time, could have to install multiple updates before going into operational mode again. Consumers must realize the importance of updates, since security patching could potentially save their lives and the lives of other drivers and pedestrians.

4.8. General recommendations for autonomous vehicles security:

- **Security by design**: All components that an autonomous vehicle uses are newly designed and constantly change as the technology and standards are still in development and have not been finalized yet. That is a good opportunity for manufacturers to implement security features in their designs. This should include hardware and software solutions used in autonomous vehicles. Manufacturers can choose secure protocols and operating systems, secure authentication methods or patch current ones before making the technology available to the public. The same thing can be done in the hardware design by implementing security features and defining security objectives, attack surfaces and system vulnerabilities before autonomous vehicles enter mass production. Also designs should allow law enforcement agencies to determine the liabilities and the parties at fault in the unfortunate situation of an accident by incorporating monitoring and logging capabilities to their systems design. Systems should also be easy to upgrade and patched as opposed to current in-vehicle tech that is mostly overlooked by vehicle manufacturers when support and updates are usually non-existent. Another important factor is the need for manufacturers to setup the necessary underlying infrastructure to support and maintain autonomous vehicles in a secure manner before the vehicles become available. Dealerships and factories should have the necessary equipment designed on the same secure principles and be able to provide maintenance and upgrades to customers.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

- **Systems Redundancy**: For applications such crucial as autonomous driving, communication devices essential to vehicle's main security functions, should be redundant. Benefits of redundancy are evident throughout the industrial world when the applications are vital or have significant financial risks. Computer infrastructure for example is always redundant in high risk environments where networks lines, data crunching systems or file servers are all redundant. Also redundancy is present in airplanes, where all navigation systems are up to 5 times redundant. In autonomous driving, redundancy could allow the vehicle to fall back to these systems when an anomaly in use or a malfunction is detected, allowing the vehicle to continue functioning uninterrupted, without risking the lives of those on board or the surrounding vehicles and pedestrians. It is evident that not all systems on an AV can be redundant, but only those that are necessary for a vehicle to function and allow the vehicle to come to a complete stop without risks, like communications systems or ECUs that control braking and steering, sensors and control devices and electrics . Although this measure would result in greater manufacturing costs for the automotive industry, it could also be the deciding factor between life and death or serious damage to the vehicle and the infrastructure. Redundancy will also build confidence in consumers in autonomous driving, allowing the technology to be implemented faster and overcome the fears of complexity. Manufacturers of electric and electronic devices, such as Bosch, are already creating redundant systems for braking and steering (Servoelectric power steering, iBooster ESP) which include double components like power supply, electronic circuits, control units and sub-machines, and in case one fails, control is automatically transferred to the remaining functioning component.

- **Exhaustive testing**: It is evident that autonomous driving, as a concept, is extremely complex and requires the cooperation of multiple new untested or at early stages of testing, in the real world technologies. Monitoring systems, communication receivers and transmitters, data crunching CPUs and other components have to work in conjunction. AI systems and big databases also help them make ethical decisions in very short timeframes. The importance of these technologies working as they were designed to do makes testing really important because the cost in human lives and the economic impact could be huge if they don't. Testing must be exhaustive at a component level for every piece of technology that is implemented in an autonomous vehicle, and also at a vehicle level. Component and vehicle manufacturers have already completed millions of hours of testing in lab environments and in several cases in real world scenarios. In early 2019, autonomous vehicle testing is allowed in various countries and cities around the world (US, UK, Australia, Switzerland, Netherlands, France, China, Canada, Germany), and in closed labs and circuits. More specific, 74 cities around the globe permit autonomous vehicle testing and this number is expected to increase significantly in the coming years. AV manufacturers measure the amount of testing in progress by miles driven without an accident. Statistically, there is a limit of 275 million miles to be driven without an accident for an autonomous vehicle to be considered as safe as a human driver, but in 2019 all testing hours in total are equal to 3% of that limit (RAND Corporation statistical analysis). The vast majority of testing still needs to be done.

Along with on road testing, several other tests need to completed for the autonomous vehicle technology to be considered reliable and exude trust and confidence. AI systems need to be trained using vast amounts of data gathered. The same principle applies for training algorithms and deep learning systems used in autonomous driving. Massive data sets are being recorder together with how humans react to different driving scenarios, that are then being fed into neural networks. While this allows design engineers to reasonably tackle the problem of algorithm design, it also makes a test engineer's job much harder. Algorithms are now a black box and more testing is required because they don't have a

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

fundamental understanding of the code that can be used to generate test scenarios. Rather, they need to test against almost every conceivable scenario to ensure the algorithm's function properly.

Another cause for concern is the lack of testing and security standards for autonomous vehicles. The technology and components used to provide autonomous driving are not yet standardized making testing difficult. New and different types of sensors are used, and also key design decisions still need to be made for the number of sensors used or if the processing of the data received from the on-board sensors will be centralized, decentralized on the sensors themselves or if a hybrid model of processing will be used. Testing methods and infrastructure must be flexible in order to be able to adopt changes, since testing systems now cannot keep up with the changes in the technology used. Rapid changes render classic testing procedures obsolete really fast and thus test engineers will have to be prepared to adapt procedures and documentation as the standards continue to evolve.

- **UI warnings and logic**: Another critical feature that can be implemented in autonomous vehicles is the ability to warn the passengers when something is wrong, or a mechanical and electrical component of the vehicle has malfunctioned or is about to malfunction. This type of warnings should be able to warn and request for immediate action the passengers on-board if the vehicle is unable to operate as it was designed to do. Warnings should be delivered fast and use optical, sonic or touch/vibration alarms since passengers on an autonomous vehicle may be involved in various activities during their commute, and they may not have their attention on the road or they may be destructed.

- **Malfunction prediction**: Autonomous vehicles should be able to predict critical system failures. Data from their on-board sensors could be processed and compared with those of a normally functioning vehicle, in order to predict malfunctions. Also, data gathered from AI systems and neural networks could be used in vehicles from the same manufacturer or that use the same components and after performing a heuristic analysis, could point out abnormal operation warning the passengers even before the actual failure occurs and advise for service or command the vehicle's full halt.

- **Statistical behavior analysis for hacking attempts**: Another attack vector that can be predicted and prevented is hacking and virus threats. Behavior and statistical analysis of the data gathered from sensors and autonomy systems on-board an autonomous vehicle can be used and compared with “known good” operational data. If those do not match, warnings could be issued for hacking attempts and delivered to the passengers or the manufacturer. This procedure could also trigger the use of fallback systems of a vehicle, avoiding deeper infiltration or total failure.

- **Simplification of tech when possible**: All previous analysis has shown that the technology required for autonomous driving to be possible and effective, is extremely complex, but also is in its infantry stages. This means that a lot of different components are used borrowing techniques and features that were not initially designed for use in autonomous vehicles. Examples of these technologies are CANBus and 5G networks. Also, different components are used like WIFI, Bluetooth and 5G communication modules. Autonomous vehicle security and cost of production could benefit from a simplification of those devices. At present time, hardware like sensors or processors on-board an autonomous vehicle, are big in size and require a lot of space, making vehicles wider and taller than standard cars, sacrificing the comfort of the passengers and making the cost to produce extremely high. As technology becomes widely available and progresses, these devices could be reduced in size and the cost could come eventually come down.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

- **On the fly services/check**: Communication devices on-board an autonomous vehicle allows the exchange of information between vehicles and infrastructure but could also be used by manufacturers to check the status of a vehicle remotely and proceed on repairs for software or configuration-based problems and faults. Manufacturers should have the ability to connect even to a moving vehicle remotely following authentication procedures and diagnose problems or do preventative checks and changes, or even upgrades to the vehicle's software without interrupting their operation or making necessary for the owner to visit a dealership. They could also guide the owner to do simple repairs and alter configuration settings to their vehicles using on-board screens and infotainment systems.

- **Standardization**: As we have previously described in this thesis, manufacturers use different technologies and protocols when it comes to the implementation of an autonomous vehicle. This lack of standardization creates many problems. Vehicle makers are now able to create close ecosystems and propriety software solutions that do not allow interoperability. If this trend continues, software developers would have to come up with different versions of software compatible with each manufacturer platform. This does allow for quick software solutions and adaptations, and developers will not have the time to optimize and secure their code.

  On the other hand, standardization which is managed by an independent governing body and not a single company, will provide a common stable base and allow everyone to participate in the development of the autonomous driving ecosystem. These systems need to bring together the best and more secure technologies from different independent companies and research organizations and at the same time they will provide interoperability between different vendor solutions. Such a standard is OMG's (Object Management Group) DDS (Data Distribution Service) for real time systems, that acts as a common language between all devices, applications and systems. DDS is especially important for autonomous vehicles as it can hasten innovation and drastically lower the risk of integrating all these disparate systems and offers next generation standards, based security, control at the data level, and a proven track record in multi-billion dollar missions and safety critical systems worldwide.

5. Infrastructure Attacks:

5.1. Infrastructure Abstract:

Autonomous driving has a lot of potential and can change the future of transportation and safety. But to be effective and fulfill its promises and goals a lot of things need to change. People tend to focus on autonomous vehicles and forfeit critical parts of the autonomous driving puzzle. One of these parts is the underlying infrastructure which enables autonomous driving. By infrastructure we mean the shared environment in which vehicles function and contains roads, traffic lights, signs, sensors, communication receivers and transmitters, and every other device that aids vehicle's uninterrupted and safe operation. Parts of the infrastructure can also be considered GPS satellites that aid navigation and manufacturers support systems and dealerships which offer updates and service.

Major investments in transportation infrastructure are already happening in many countries around the world today and countries with long standing infrastructure need to replace or upgrade aging roads and

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

bridges providing a perfect platform to investigate investment in resilient infrastructure that is capable of adapting to changing environments, and leveraging technology, creating a truly connected "smart city". Some of the more apparent changes that need to be made on transportation infrastructure are:

- Sensors: Sensors need to be placed in strategically chosen locations like crossroads or traffic lights by using pre-cast pavement slabs. Sensors will sync with autonomous cars and can measure vehicle vibrations to predict a car's next move, communicate directly with vehicles on the road, and alert drivers of upcoming accidents and alternate routes.

- Streetlights: Streetlights can utilize already developed IoT technology to communicate with vehicles about upcoming traffic patterns and provide information and manage congestion. Systems like that, are being tested today in cities like Las Vegas. As a vehicle approaches a stop light, vehicle sensors talk to the sensors on the lights telling the vehicle how much longer it will be until the light turns green, and when the car can accelerate. Simpler but also effectively, in the Netherlands roads incorporate weight sensors that inform a traffic light that a car approaches and according to traffic allow the vehicle to pass or stop.

- Self parking: Autonomous vehicles will also decrease the time spent during the daily rush hour, specifically with parking. Currently, parking in cities can be a nightmare. Garages are constantly full and drop-off locations on busy streets are less than ideal. With autonomous vehicles, though, special zones will allow cars to pick up and drop off their passengers without interrupting traffic flow. Parking garages designed for autonomous travel will also be built outside cities rather than in busy downtown districts.

- Radio transmitters: Specially designed data transmitters and receivers will be placed in strategically picked positions that share information about road conditions, accidents, weather or traffic congestions and will enable autonomous vehicles to adopt their driving style or reroute to avoid bad weather and traffic jams.

Manufacturers facilities and infrastructure, service points and dealerships must also change and adapt to the new requirements that autonomous driving dictates. Auto makers should either in-house or via third party vendors the equipment necessary to provide updates and fixes to a large fleet of vehicles on a timely manner. They should also be able to monitor vehicles and log their operational data and provide assistance and support to vehicle owners. Dealerships and service points should also be able to update vehicles and service them by having the equipment and spare parts. Lastly, they should train their stuff to be familiar and support the new technologies that autonomous vehicles have on-board.

Much like autonomous vehicles, infrastructure can also be exploited by malicious individuals trying to gain access to a fleet of cars. The difference is that by tampering with infrastructure components someone can impact a large number of vehicles or have access to a large database of data and information. This danger dictates that infrastructure security is even more important than that of a single vehicle, since a possible successful attack attempt could result in a great loss of lives and could have bigger financial impact.

5.2. Infrastructure threats:

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

- **Physical obstructions and hacking**: The simplest way of interfering with infrastructure elements like signs and traffic signals is physical obstruction. Someone with malicious intentions can easily alter, block or even remove signs and traffic lights. This kind of tampering could be more dangerous in areas where GPS signal is weak and thus the vehicle has no other way to get info about the road besides signs and traffic signaling. Physical tampering is easy but can be prevented by securing traffic signals and signs from physical access either positioning them far from reach or blocking access by securing them physically.
  Hacking is also possible as smart signs; traffic signals and sensors can be treated as IoT devices and can be exploited since they have access to the infrastructure and vehicular network. A malicious individual could gain access to traffic signaling and create havoc putting in danger vehicles and passengers. Unprotected sensors could also be tampered to provide false information to vehicles about traffic jams, weather conditions or accidents on the road.

- **Manufacturer hacking**: As mentioned in the introduction to this chapter, autonomous driving infrastructure hacking is a lot more dangerous and can result to greater losses in human lives, vehicles or infrastructure components. Also, manufacturers in the new era of autonomous driving will have to provide new over-the-air services to vehicle's owners in order for the vehicles to operate normally offering software updates and adding features. To do that, manufacturers, will have the ability to connect to our vehicles remotely without the need for the owner to drive his vehicle to service centers. It is evident that someone who can have physical or remote access to the manufacturer's infrastructure and over-the-air mechanisms, will have the ability to take control of all the entire fleet of cars of the specific brand. That infiltration would allow a malicious individual to take control of the vehicle either by sending control commands or by injecting malicious code to the vehicle's software exploiting the update function.

Securing manufacturer's infrastructure from physical or digital access is therefore of critical importance. This means that buildings and antennas, part of the over-the-air access, should be guarded and secured allowing access only to authorized personnel. The same level of security should also be applied to all systems responsible for the software updates and remote access of the vehicles. These systems should have strong and secure authentication mechanisms either from the vehicle side or the infrastructure side. Administrators should be authenticated using multiple steps, transmissions should be always encrypted and updates should be signed by the manufacturer. Vehicles should also be able to authenticate malicious attempts using their on-board IDPS systems and report them to authorities or the manufacturer itself, so that an manufacturer could be able to stop any unauthorized attempt with great speed and limit the attack to as less vehicles as possible. Network protection devices like firewalls, IPS and IDS, should also be implemented in every vehicle maker infrastructure network disabling access to those systems to any outside the network resource and creating demilitarized zones. In general, the latest technology in network security would be needed for a manufacturer to be as possible protected from external access to their systems.

- **Vendors, dealerships infrastructure**: As any other vehicle, autonomous cars will need scheduled (service intervals, updates, recalls) and unscheduled (mechanical or electronic systems failure) visits to the manufacturer dealerships and fleet of authorized service points. Even today, any car manufactured 25 years ago and after and which is using the CANBus architecture, can be diagnosed for failures and errors by just connecting it to diagnostic devices. The same procedure can facilitate the software update to later versions and patching for security

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

gaps. Same technique is most likely that will be used by manufacturers in autonomous vehicles, and since more functions of the car will be controlled by software, updates and patches will be more frequent and could have the ability to alter basic functionalities of the vehicle like driving style, security features, communication system or even AI algorithms controlling the vehicle's behavior to accidents and more. It is then evident that someone who has access to diagnostic-update devices could easily make use of the technology and plant malicious code disguised as update, or alter lines of code taking control of the vehicle.

Authorization, update package signing and encryption could also be the solution to this problem. Access to infrastructure devices that can perform vehicle diagnostics and updates to the software should be limited only to authorized personnel and strong authorization procedures and mechanisms should be in place protecting them from unauthorized possession and use. Availability of these devices should also be limited to a small group of dealers and service point that do have the expertise and training to use them. Each car should be protected with a unique code or by using secure authentication methods like public and private key pairs and biometrics. Every piece of code, intended for the vehicle, should be encrypted. By employing modern encryption methods and algorithms like Triple DES or AES, RSA or Blowfish and Twofish vehicle makers can bulletproof their software when critical updates are being pushed to the vehicle making malicious code injection difficult.

As we know every kind of software protection method or authorization mechanism is not 100% immune to hacking attempts, but by using multiple protection and authorization tools, manufacturers can limit the number of individuals capable of performing these kinds of attacks.

- **Infrastructure availability**: Autonomous driving is very depended on various systems on and off board the vehicle, in order to be operational and reach its objectives for safety and speed and secure transportation. Autonomous vehicles receive geographical data from GPS satellites, traffic or possible accident and weather information from ground networks. Also, as described, vehicles receive updates and security patches from the manufacturers network. Autonomous vehicles can operate without these systems, but their functionality becomes very limited and, in some instances, dangerous.

For example, AVs can drive through a city without using GPS guidance but by recognising street signs and traffic lights, but what happens when traffic signs are not available or tampered, or when they are driving in areas with no satellite access? The same of kind of problems arise when information from ground networks and supporting services is not available. Traffic cannot be predicted and information regarding accidents or road blocking events cannot reach the vehicle and allow it to take actions and avoid them. Also, extremely dangerous would be a situation where a vehicle's manufacturer network is down and over-the-air updating function is offline. Critical updates could not reach the vehicle making it dangerous for use.

According to our opinion, the key solution to these problems is redundancy, VANETs and human intervention. Redundancy would allow the vehicle to resort to different systems when the defaults are not available and human intervention will be needed in the extreme situation that none of the redundant systems are online.
Maps, road signs or speed limits can be also saved in the vehicle’s memory updated in preconfigured time intervals, in order for them to be up to date and reliable for the vehicle to resort to when needed. Information can also be received by local networks using 5G, Bluetooth or other communication methods.
VANETs which are created between in proximity vehicles can also provide a solution. Information can be retrieved by close by vehicles that share their data when requested. Vehicles in a VANET could hold

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

information from previous destinations in their memory or from a previous VANET that they were connected.
As a last resort, a human passenger could take over disabling automation. When a vehicle gets in a situation when critical to its operation information can be retrieved from infrastructure or close VANETs, it could inform the passengers on board to take over by optical or sonic signals. They should be able to take the vehicle to a complete stop or continuing their drive until their destination or up until the services are restored. This alternative unfortunately in the long run will not be reliable enough since it requires that the passengers have a driving experience and are trained.

- **Early implementation and mixed driving environments**: Transition to a fully autonomous future is something that cannot implemented over a night, but it will need many years to be adopted until the entire fleet of cars gets replaced, the infrastructure will be updated and available all over the planet. Finally, users will need to be trained to use these vehicles, be willing and persuaded to leave their non-autonomous vehicles, and trust in the new, safer and time saving technology. Adoption of autonomous driving will be slow, costly and for many years autonomous and non-autonomous or semi-autonomous vehicles will coexist creating confusion and problems. The trickiest problem has to do with how humans might adjust their behavior to autonomous cars. For some drivers and pedestrians, simply recognizing an autonomous vehicle on the road can produce some undesirable behaviors, whether it's more aggressive or more timid driving. Experts say that autonomous vehicles should be more aggressive in their driving style, because at the moment they operate overly cautious which does not engender trust to human drivers. Autonomous vehicles need to alter their driving style via IA and act much like an experienced human driving. When this happens, it will be a matter of time before they are accepted and become part of our everyday life.

6. Driver Attack Surface:

6.1. Driver Attack Abstract:

Until now, we have seen that autonomous vehicles and autonomous driving in general, can be exploited using security flaws in physical components that of a vehicle (sensors, OBD port, infrastructure components, etc.) or the software necessary for vehicle's operation (CANBus, communication protocols, etc.). One factor that has yet been discussed, is the human one, and more specifically the kind and amount of intervention a human passenger/driver should have over the process of driving and the vehicle as a physical object itself. Ethical questions also arise regarding human intervention. One of them is when and if the passenger should have the option to disable automation and under what circumstances and in what degree.

If human intervention is possible, that would allow malicious individuals or groups to create problems while using the vehicle. At the same time this situation would also be the last resort for a vehicle that malfunctions to save those on-board or other near-by vehicles and/or pedestrians. If an individual with malicious intents that is on-board the vehicle, would be allowed to take full or partial control of the vehicle, or even make simple corrections to its course and manual entries, then the vehicle could be involved in an accident damaging other near-by cars or infrastructure elements like buildings and signage. A situation like this, could also result in accidents where other near-by vehicles would not know how to react to a possible erratic behavior of the autonomous car, as a result of the manual inputs

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

given by the malicious driver. Specific behavior is expected from all vehicles in an area for autonomous driving as a concept to be effective an accident free.

Another example of non-desired human intervention would be when a human passenger/driver is involved that is under the influence of alcohol or drugs. Manual override in a situation like this should also not be allowed under any circumstance, because results could be also fatal.

Human intervention should also not be permitted when passengers are unable for any reason to drive, like elderly people or human with sense impairments (visual or sonic) or physical body disabilities.

Autonomous vehicles, although their operation is automated and do not need manual inputs from passengers, it would still be a good idea for human passengers to have training sessions on basic vehicle operation and manual handling systems. It would also be really helpful, at least in the early stages of autonomous driving implementation, if passengers could take all the necessary theoretical exams, as drivers do today to drive conventional automobiles. This kind of training would allow for humans on-board a vehicle to understand basic mechanical failures and read road signs, helping them interact with the car and their surroundings if needed. Passengers with disabilities should not be allowed to disable automation on a vehicle at any time and under any circumstance.

6.2. Driver Recommendations:

As previously mentioned, a lot of ethical questions arise when talking about human intervention in autonomous driving. Rules have to be in place governing when it is allowed or not for a passenger/driver to be able to override automation on an autonomous vehicle, and manually enter inputs altering its course. Under what circumstances or what kind of failures an automated vehicle should pass control to a human passenger, should also be standardized and driving exams have to be redesigned entirely in order to facilitate new technologies and basic AV functions.

Another critical factor is the ability of a passenger to drive and make critical decisions at any given time. Technology already exists and allows for alcohol and drug use tests to be performed on-board non-automated vehicles, that disable engine's start when the driver exceeds certain alcohol use thresholds. The same technology can be implemented in autonomous vehicles, deciding if a passenger is capable or not, to control the car if there is a need to.

Researchers also suggest a solution for people with disabilities. The vehicle should ask basic questions upon boarding phase to the passengers checking driving abilities or if any of them has physical disabilities, so it could partially transfer handling to the passengers, if needed, according to their answers.

7. Conclusion – Findings:

Since the inception of automobiles capable of human transportation in 1769 by Nicolas-Joseph Cugnot, a lot has changed, but the principles of car design remain the same. Automobiles were created to shorten big distances and bring people and cultures together by minimizing the effort required to do just that. Many changes have been made to the original design ideas over the decades and centuries that followed, but the basic idea remained the same.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

During the evolution of car industry, automakers had the chance to incorporate, available in each era technology, into vehicles making them more efficient, comfortable, safer and recently even more enjoyable. From steam powered vehicles we moved to internal combustion engines and now electric powered vehicles. From simple mechanical contraptions, cars have evolved to fully electrical, carrying electronic devices such as communication devices, GPS receivers and infotainment systems.
Massive adoption of automobiles, also lead to various problems. Traffic became part of our everyday lives and the cost in human lives is getting bigger and bigger every day. A viable solution to these problems is autonomous driving. What we have seen in various comics and sci fi movies is today finally technologically possible.

Autonomous driving promises to provide solutions to many problems. It could make our commute faster, more enjoyable, but most importantly, safer. It could also help on transportation equity, as elder passengers or with a disability to drive, will be able to take advantage of the new technology. Last but not least, autonomous driving will help reduce our carbon dioxide footprint, as autonomous vehicles will be shared amongst users and always available. These promises are based on the use of various different already existing technologies that have been modified according to needs, or newly devised to address specific design goals of autonomous driving.

In order for autonomous driving to be successful and effective, various technologies have to operate efficiently and in cooperation. Data from various optical sensors (lidars, radars and cameras) and antenna receivers (WIFI, Bluetooth, GPS, …) on-board an autonomous vehicle, are fed into powerful processing units that analyze that data and create an internal image of the surroundings. Based on that map, they plot a path and send commands to the vehicle's control mechanisms, like steering wheel and brakes, to follow that path and avoid obstacles, follow road rules and signage, and to interact with other close-by vehicles. These decisions are also guided by rules, predictive modelling and special object discrimination and object avoiding algorithms that are loaded into on-board processing units.
Autonomous vehicles can also be "connected". This means that by using communication devices and suitable data transferring protocols, they can interact with other vehicles or parts of the "smart" infrastructure like traffic lights and crossroads. They can also download updated information for traffic congestions and take advantage of vast databases, AI, and deep learning techniques that can predict accidents by analyzing similar recorder events and driving conditions.

As already mentioned, ethical questions could also arise from the use of autonomous driving technology and the actions a vehicle should decides to take during a critical or fatal situation. An autonomous vehicle should make decisions based on the programming algorithms used. Researchers are now creating the algorithms a vehicle should rely on its decision making based on human interaction. Databases are being created that are based on how a human would interact in critical situations and will include every possible scenario imaginable. It is still under discussion weather it will be for the better or worse if those algorithms and decision-making progress will exclude human emotion in its process.

Unfortunately, as it already happens with non-autonomous vehicles, there will be malicious individuals that will try to infiltrate autonomous driving vehicles or parts of the autonomous driving infrastructure and gain access to them, fulfilling their malicious intentions. By gaining access, they could take control of an individual or a fleet of vehicles. The use of a large number of different technologies and communication protocols in autonomous driving design, increases their attack surface significantly. As already discussed in this thesis, the attack surface of an autonomous vehicle and the underlying infrastructure, is the sum of the vulnerabilities of each technology used, as long as no extra measures have been taken when incorporating them to the design.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

Based on the kind of access a malicious individual or team has on an autonomous vehicle, physical or remotely, threats can be divided into local or remote attack vectors.
At this stage of evolution in autonomous driving, the easiest way to obstruct the functions of an autonomous vehicle is to physically mess with its on-board exterior technology or parts of the infrastructure. Anyone could cover the optical sensors that an autonomous vehicle uses to interact with each surrounding environment leading to limited vehicle functionality or complete disability. Also easy it could be for someone to tamper with road signage in areas that the vehicle solely relies on them to "read" information about the route rules, for example in underground parking lots or in general when GPS signal is not available or in roads that are not mapped. This kind of tampering could only be prevented by ethical reservations an individual should have or by educating the people of the results of such an action could have.

Local attack vectors are usually targeted on a single vehicle penetration and are mostly based on exploiting the CANBus architecture. CANBus has been a part of automotive technology for the last few decades, and successful attacks have been reported exploiting it until now. Access to the CANBus stream can be gained via various subcomponents of a vehicle including but not limited to sensors, OBD port and interfaces of an infotainment system. Infiltrating the CANBus stream would allow for complete access to vehicle's controls and electronic aids that use the CANBus protocol, and could result in total loss vehicle's control. This indicates that securing access to the vehicle's CANBus gateways is of critical importance. As explained, this can be accomplished physically by adding security mechanisms between the various interfaces, or digitally by employing more advanced methods of authentication and encryption when someone tries to gain administrator access to electronic devices on-board a vehicle.

On the other hand, a remote attack could target more than one vehicle at the same time. Current autonomous driving technology, that is still in its infant stages, uses a lot of known communication protocols, like WIFI, Bluetooth, vanets, and 5G, to accomplish vehicle to vehicle (V2V), vehicle to the underlying infrastructure (V2I) and vehicle to everything else (V2X or V2E) communication. Each kind of communication uses different protocols created especially for autonomous driving use or already designed for other not so critical applications. Each of these data transmission technologies has its advantages, but also its flaws. Individuals with malicious intentions could exploit these flaws and gain access to a single vehicle, an entire fleet of vehicles, or the underlying supporting infrastructure. Unfortunately, as shown and described in detail in this paper, known and widely used protocols have flaws and design security gaps that should be addressed before deploying them for use with such critical applications, as is autonomous driving. Patching and creating new revisions of these protocols is the most secure way of defending autonomous vehicles from possible attacks. On the other hand, newly designed technologies. Like 5G and 5G+ or C-V2X, are especially designed for automotive applications, but are still in early stages of development and would probably need a lot of new patches and revisions until they are considered safe and secure. Also, final decisions, guidelines, and standards for autonomous driving, are still to be created and agreed by various manufacturers and organizations. Which technologies will eventually be used in autonomous driving, is something that is still to be decided, and these decisions must be made with security as the first priority in mind.

In general, known effective techniques and mechanisms can be used to avoid and overcome security issues in autonomous driving. Over-the-air updates and patches, that use secure authentication mechanisms, should prevent mass penetration in autonomous vehicles. Extensive testing of the various components and penetration testing, in controlled or in real life scenarios, could also allow manufacturers to identify problems and security flaws, and address them before mass production.
Network protection and intruder identification devices, such as firewalls and IDPS, have already been tested and are being mass produced by security companies. These devices although they are situated on-board a vehicle, work exactly as the ones we today use in our home or professional networks. They

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

prevent access from intruders, to and from the vehicles, using custom generated rules. They also have the ability to protect a vehicle using pattern and behavioral analysis, identifying suspicious behavior within the vehicle itself or a car network. In production at the moment, are also antivirus client from various software companies that protect access to vehicles interfaces, analyze packets going through a vehicle network, and take action or inform the owner of the vehicle or the manufacturer, for suspicious packets and threats.

Another big weapon in fighting the war between individuals with malicious intent and autonomous vehicle owners and manufacturers is the concept of redundancy. This logic can be implemented, not only on the mechanical parts of a vehicle, but also in electronic devices and communication receivers and transmitters. Redundancy is a key to a problem-free operation. When a malfunction or tampered part of a vehicle is identified, then the on-board logic controllers should be able to fall back to redundant solutions without affecting any of its functions. The use of redundancy can be transparent to passengers and should be able to safeguard the vehicle's operation until it reaches a service point or comes to a full stop.

It is almost certain that new threats and attack vectors will be identified and exploited in the future, until autonomous vehicles go into mass production and become part of our everyday lives. The more they gain infiltration to our society and way of living, the more interest they will attract from malevolent individuals or groups. Until then, researchers and car manufacturers, need to make the right decisions designing secure and most importantly easy to update software and hardware mechanisms. That is the proposed way to in order for them to be able to address security issues rapidly and to contain attacks to a minimum number of vehicles affected. They should also manufacture vehicles that can easily be upgraded to newer standards as the industry evolves, and at the same minimizing the production costs.

Some say that autonomous driving mass infiltration is even decades ahead of us, and others we are just a few years till autonomous vehicles become the new norm. Either way, the whole endeavor of autonomous driving is extremely difficult and it will surely need optimizations and a lot of time before it reaches its full potential. The adoption period will be very big and problematic, until all vehicles on the road today give their place to new and autonomous ones. Society will also need time to get used to the idea of autonomous driving and overcome worries and prejudice. At the end though, autonomous driving technology will surely transform the way we live from the first moment autonomous vehicles will become available to the public, as the first vehicles did in the late 18^{th} and early 19^{th} century. They will make our daily commute faster, environmental friendlier, and more enjoyable. They will also bring equity to transportation for those who are unable to drive and fulfilling their design objectives. Most importantly though, autonomous driving will make our future commutes safer when teething problems are addressed.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

Glossary:

OBD (On Board Diagnostics): is a connection interface and diagnostic system for troubleshooting automotive problems and provides error codes for most functions of a vehicle.
ECU (Electronic Control Unit): Is any embedded electronic processor that controls one or more of a vehicle's subsystems.
LiDAR (Light Detection And Ranging): is a sensor that creates a map of a vehicle surroundings by emitting and then receiving the emitted light.
Radar (Radio Detection And Ranging): is a detection system that uses radio waves to determine range, angle and velocity of objects. It does so by emitting and receiving radio frequency signals.
ESP (Electronic Stability Program): is a technology that improves a vehicle's stability and braking by detecting and controlling loss of friction of each tyre of a vehicle.
ABS (Anti-Lock Braking System): is an electronic system that prevents the locking of tyres of a vehicle when braking in extreme conditions.
USB (Universal Serial Bus): is a computer interface responsible for transferring data.
MAP sensor (Manifold Absolute Pressure sensor): is a sensor, part of modern internal combustion engine, that measures the manifold pressure.
Lambda sensor: is a sensor, part of modern combustion engine, that measures the proportion of oxygen in the gas.
Knock sensor: is a sensor, part of modern combustion engine, that detects vibrations coming from knocks in internal combustion engines.
A.D.A.S. (Advanced Driver Assistance Systems): Electronic systems that aids driving in modern vehicles. Such systems for example are ABS, cruise control or lane departure warning systems and automatic braking assistants.
PID (Parameter IDs): ID codes used in OBD diagnostic to identify problems on vehicles.
WIFI: A family of wireless technologies based on the IEEE 802.11 standard and used in wireless local area networks.
Bluetooth: An industry standard for wireless data transfer usually used in communication and recently in IoT devices.
CFI (Central Fuel Injection): System that manages the fuel injection mixture into modern internal combustion engines.
SMS (Short Messaging Service): Service that facilitates the exchange of short text messages between cellular devices.
MirrorLink: Is a communication standard that facilitates the interaction between a smartphone or similar electronic device with a vehicle's infotainment system.
AVIC: Series of vehicle infotainment systems produced by pioneer electronics.
Apple CarPlay: Is Apple's standard that enables the connection and interaction between an iOS device and an infotainment system on a vehicle. Device's data can be displayed on the vehicle's screen and the device can be controlled by the touchscreen.
Android Auto: Is Google's solution for connecting and controlling Android devices to infotainment systems on board modern vehicles.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

GENIVI Alliance: Non-profit automotive industry alliance that develops standard approaches for integrating operating systems and middleware present in the centralized and connected vehicle cockpit.
WinCE: Microsoft's OS for small computers and embedded systems that resembles Windows for laptops and desktops.
iOS: Apple's operating system installed in mobile devices, phones and tablets produced by Apple.
ARM: Company that produces processors based on RISC architecture and usually embedded in mobile devices and other applications when consumption power is critical.
Linux: Open source operating system based on Unix.
RFID (Radio Frequency Identification): Technology that uses electromagnetic field to identify and track tags attached to objects.
GPS (Global Positioning System): Satellite based system that enables the track of geological position of moving or static objects over the globe.
EPS (Evolved Packet Switch): Evolved packet system is the central network portion of the UMTS LTE mobile communication system. The packet system primarily transfers packet data between edge networks and the radio access network. (definition from UMTS Long Term Evolution by Lawrence Harte)
GSM (Global System for Mobile communications): European cellular network communications system used in mobiles phones across Europe developed in 1982 and used until today going through various evolutions steps.
4G: The fourth generation of broadband cellular network technology that provides high speed data transfers and voice telephony.
5G: The fifth and newest implementation of broadband cellular network technology. 5G is expected to replace 4G networks in the following years starting from 2019.
DSRC: An open-source protocol for wireless communication, similar in some respects to WiFi.
OBU (On Board Unit): Communication device mounted on vehicles. It allows DSRC communications with other **OBU**s or RSUs. (igi-global.com)
RSU (Road Side Unit): Device attached to infrastructure and enable the communication with vehicles.
MANET (Mobile Ad Hoc Network): Wireless network without centralized control units but based on mobile nodes that carry also network structure information and acts as a router.
VANET (Vehicle Ad Hoc Network): Vehicular networks based on MANET technology. Vehicles are the nodes of a VANET.
UMTS (Universal Mobile Telecommunications System): third generation mobile cellular system based on the GSM standard.
OFDM (Orthogonal Frequency-Division Multiplexing): A form of signal waveform or modulation that provides some significant advantages for data links that is used for many of the latest wide bandwidth and high data rate wireless systems including Wi-Fi, cellular telecommunications and many more
MIMO (Multiple-input and multiple-output): A method for multiplying the capacity of a radio link using multiple transmission and receiving antennas to exploit multipath propagation. (Wikipedia)
AFH (Adaptive Frequency Hoping): Technology used by Bluetooth and can reduce the effects of interference between Bluetooth-enabled and other types of devices. Device that use AFH change frequency channels in coordination many times a second.
5G-NR (5G New Radio): An LTE evolution technology for wireless cellular communication that uses OFDM and can carry data on several parallel data streams or channels.
DoS (Denial of Service): A cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled. (source: Wikipedia)
DDoS (Distributed Denial of Service): Same as DoS but the incoming traffic flooding the target of an attack comes not from one but different sources usually spanning in various locations around the planet.
IPS (Intrusion Prevention System): A network security/threat prevention technology that examines network traffic flows to detect and prevent vulnerability exploits.
IDS (Intrusion Detection System): A system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered.
OTA (Over The Air): Refers to various methods of distributing new software, configuration settings, and even updating encryption keys to devices like cellphones. Updates are sent simultaneously to many devices from one source.
IDPS (Intrusion Detection & Prevention System): Network security devices that offer features from both Intrusion detection and intrusion prevention systems. These systems examine traffic packets, identify malicious activity and alert the users.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

References:

5GAA. (n.d.). *Exploring the technology: C-V2X*. Retrieved from 5gaa.org: http://5gaa.org/5g-technology/c-v2x/

Argus Cyber Security. (n.d.). *A remote attack on an aftermarket telematics service*. Retrieved from https://argus-sec.com/: https://argus-sec.com/remote-attack-aftermarket-telematics-service/

Autocar. (2016, August 02). *Delphi Automotive tests autonomous taxi service in Singapore*. Retrieved from autocar.co.uk: https://www.autocar.co.uk/car-news/industry/delphi-automotive-tests-autonomous-taxi-service-singapore

Baker McKenzie. (2018, March 05). *Baker McKenzie Launches Global Driverless Vehicle Survey 2018.* Retrieved from www.bakermckenzie.com: https://www.bakermckenzie.com/-/media/files/insight/publications/2018/03/global-driverless-vehicle-survey-2018/mm_global_driverlessvehiclesurvey2018_mar2018.pdf?la=en

Barreto, V. (2017, August 18). *What is OBD II? History of On-Board Diagnostics*. Retrieved from www.geotab.com: https://www.geotab.com/blog/obd-ii/

Barsotti, F. (n.d.). LVMM - The Localized Vehicular Multicast Middleware:a Framework for Ad HocInter-VehiclesMulticast Communications. *2005*. Università degli studi di Pisa.

Basin, D., Dreier, J., Hirschi, L., Radomirović, S., Sasse, R., & Stettler, V. (2018, October 18). A Formal Analysis of 5G Authentication.

Boffey, D. (2019, May 03). *Amsterdam to ban petrol and diesel cars and motorbikes by 2030* . Retrieved from www.theguardian.com: https://www.theguardian.com/world/2019/may/03/amsterdam-ban-petrol-diesel-cars-bikes-2030

Brian Donohue. (2015, January 27). *Progressive Snapshot Exposes Drivers to Car Hacking*. Retrieved from https://www.kaspersky.com.au: https://www.kaspersky.com.au/blog/progressive-snapshot-car-hacking/7284/

C. E. Perkins, & E. M . Royer. (n.d.). Ad-hoc On-Demand Distance Vector Routing. Second IEEE Workshop on Mobile Computing Systems and Applications.

Chattopadhyay, A., & Lam, K.-Y. (2018, October 01). Autonomous Vehicle: Security by Design. School of Computer Science and Engineering, Nanyang Technological University, Singapore.

Chirgwin, R. (2017, June 27). *Researchers blind autonomous cars by tricking LIDAR*. Retrieved from theregister.co.uk: https://www.theregister.co.uk/2017/06/27/lidar_spoofed_bad_news_for_self_driving_cars/

Corrigan, S. (2016, May). *Introductionto the ControllerAreaNetwork(CAN).* Retrieved from www.ti.com: http://www.ti.com/lit/an/sloa101b/sloa101b.pdf

Currie, R. (2017, May 18). *Hacking the CAN Bus: Basic Manipulation of a Modern Automobile Through CAN Bus Reverse Engineering.* Retrieved from www.sans.org: https://www.sans.org/reading-room/whitepapers/threats/paper/37825

D. B. Johnson, & D. A. Maltz. (1996). Dynamic Source Routing in Ad Hoc Wireless Networks. Mobile Comput ing.

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

Day, L. (2016, December 13). *Pioneer AVIC Infotainment Units Hacked to Load Custom ROMs*. Retrieved from https://hackaday.com: https://hackaday.com/2016/12/13/pioneer-avic-infotainment-units-hacked-to-load-custom-roms/

DEEMSOFT. (n.d.). *Autonomus Vehicles*. Retrieved from https://deemsoft.com/deemsoft-autonomous.php

Dimitrakopoulos, G., & Bravos, G. (2017). *Current Technologies in Vehicular Communications.* Springer.

Dunn, J. E. (2018, May 02). *Volkswagen and Audi car infotainment systems hacked remotely*. Retrieved from https://nakedsecurity.sophos.com: https://nakedsecurity.sophos.com/2018/05/02/volkswagen-and-audi-car-infotainment-systems-hacked-remotely/

E, A. (. (2013, January 29). *Complete List of OBD Codes: Generic OBD2 (OBDII) & Manufacturer*. Retrieved from www.totalcardiagnostics.com: http://www.totalcardiagnostics.com/support/Knowledgebase/Article/View/21/0/complete-list-of-obd-codes-generic-obd2-obdii--manufacturer

Eisenbarth, T., Moradi, A., Paar, C., Salmasizadeh, M., & Shalmani Manzuri, M. (2008). On the Power Analysis in the Real World: A Complete Break of the KeeLoq Code Hopping Scheme.

Escypt gmbh. (2016). *Automotive Intrusion Detection and Prevention System (IDPS).* Retrieved from ESCRYPT: https://www.concarexpo.com/fileadmin/Redaktion/Dokumente/Praesentationen_ConCarForum_2017/24_escrypt_GmbH_-_Jan_Holle.pdf

Gardiner, B. (2018, July 23). *How yesterday's cars might mix with tomorrow's autonomous traffic*. Retrieved from https://www.hagerty.com: https://www.hagerty.com/articles-videos/articles/2018/07/23/how-yesterdays-cars-might-mix-with-tomorrows-autonomous-vehicles

Gáspár, P. D., Zsolt, S. D., & Aradi, S. (2014). Highly Automated Vehicle Systems. BME MOGI.

German Federal Ministry of Transport and Digital Infrastructure - Ethics Commission. (2017). Automated and Connected Driving. (p. 36). German Federal Ministry of Transport and Digital Infrastructure.

Goldhill, O. (2018, February 11). *Philosophers are building ethical algorithms to help control self-driving cars*. Retrieved from qz.com: https://qz.com/1204395/self-driving-cars-trolley-problem-philosophers-are-building-ethical-algorithms-to-solve-the-problem/

Golson, J. (2016, September 19). *Car hackers demonstrate wireless attack on Tesla Model S.* Retrieved from www.theverge.com: https://www.theverge.com/2016/9/19/12985120/tesla-model-s-hack-vulnerability-keen-labs

Hassan, J. (2017). *Cars with Vulnerable WIFI Dongle can be Hacked via Bluetooth*. Retrieved from www.hackread.com: https://www.hackread.com/cars-with-vulnerable-wifi-dongle-can-be-hacked/

Higgins, S. (2015, September 09). *How to hack an Automotive LiDAR for $60*. Retrieved from www.spar3d.com: https://www.spar3d.com/blogs/the-other-dimension/vol13no39-how-to-hack-a-lidar-sensor-for-60/

Hoffman, C. (2019, January 31). *Bluetooth 5.1: What's New and Why It Matters*. Retrieved from https://www.howtogeek.com: https://www.howtogeek.com/403606/bluetooth-5.1-whats-new-and-why-it-matters/

Holmes, F. (2018, November 12). *Over-the-air updates moving from 'nice to have' to 'vital'*. Retrieved from https://www.automotiveworld.com: https://www.automotiveworld.com/articles/over-the-air-updates-moving-from-nice-to-have-to-vital/

Hoppe, T., & Kiltz, S. (2010). Security threats to automotive CAN networks - Practical examples and selected short-term countermeasures.

Hussain, S. R., Echeverria, M., Chowdhury, O., Li, N., & Bertino, E. (2019). Privacy Attacks to the

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

4G and 5G Cellular Paging Protocols Using Side Channel Information. Purdue Univeristy & University of Iowa.
International, S. (2010). DSRC Implementation Guide: A guide to users of SAE J2735 message sets over DSRC. SAE International.
Jillian Goldberg. (2018, February 11). *Automotive Cyber Security Essentials and IDS IPS Technology for Vehicles*. Retrieved from https://blog.guardknox.com: https://blog.guardknox.com/automotive-cyber-security-essentials-ips-ids-technology
Jones, M. (2018, October 10). *10 Public Wi-Fi Security Threats You Need to Know.* Retrieved from www.safervpn.com: https://www.safervpn.com/blog/10-public-wi-fi-security-threats/
Kalra, N., & Paddock, S. M. (2016). *Driving to Safety: How many miles of driving would it take to demonstrate autonomous vehicle reliability?* Retrieved from www.rand.org: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1400/RR1478/RAND_RR1478.pdf
Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., . . . Savage, S. (2010). Experimental Security Analysis of a Modern Automobile.
Kovelman, A. (2017). *A Remote Attack on the Bosch Drivelog Connector Dongle*. Retrieved from https://argus-sec.com: https://argus-sec.com/remote-attack-bosch-drivelog-connector-dongle/
KPMG. (2018). *Autonomous Vehicles Readiness Index.* KPMG International Cooperative .
Leigh, B. (2017, March 07). *Standards vs. Standardization: How to Drive Innovation in Self-Driving Cars*. Retrieved from www.rti.com: https://www.rti.com/blog/2017/03/07/standards-vs-standardization-how-to-drive-innovation-in-self-driving-cars
Lonzetta , A. M., Cope, P., Campbell , J., Mohd, B. J., & Hayajneh , T. (2018, July 19). Security Vulnerabilities in Bluetooth Technology as Used in IoT. Journal of Sensor and Actuator Networks.
Mazloom, S., Rezaeirad, M., Hunter, A., & McCoy, D. (n.d.). *A Security Analysis of an In Vehicle Infotainment and App Platform.* Retrieved from http://damonmccoy.com: http://damonmccoy.com/papers/ivi-woot.pdf
McLaren, S. (2019, January). *Infrastructure is the missing piece to an autonomous future*. Retrieved from https://betanews.com: https://betanews.com/2018/12/20/infrastructure-is-the-missing-piece-to-an-autonomous-future/
MERTL, S. (2018, May 16). *How cars have become rolling computers*. Retrieved from The Global Mail: https://www.theglobeandmail.com/globe-drive/how-cars-have-become-rolling-computers/article29008154/
Michelle , G. X., & Mao, S. (2017, September). *AN OVERVIEW OF 3GPP CELLULAR VEHICLE-TO-EVERYTHING STANDARDS*. Retrieved from https://www.researchgate.net: https://www.researchgate.net/publication/321088744_An_Overview_of_3GPP_Cellular_Vehicle-to-Everything_Standards
Miller, C., & Valasek , C. (2015). A Survey of Remote Automotive Attack Surfaces.
NHTSA. (2019). *Automated Vehicles for Safety*. Retrieved from United States Department of Transportation : https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety
Noor, K. (2019, May 13). *Bluetooth, ad hoc and Piconet*. Retrieved from https://medium.com: https://medium.com/@kashifnoor/bluetooth-ad-hoc-and-piconet-f7d5b9b027a9
Palanca, A. (2016). *www.politesi.polimi.it.* Retrieved from A Stealth, Selective, Link-layer Denial-of-ServiceAttack Against Automotive Networks: https://www.politesi.polimi.it/bitstream/10589/126393/1/tesi_palanca.pdf
Peng, T. (2018, March 15). *Global Survey of Autonomous Vehicle Regulations*. Retrieved from https://medium.com: https://medium.com/syncedreview/global-survey-of-autonomous-vehicle-regulations-6b8608f205f9
Phillips, J. (2018, August 09). *Testing the Unknown: The Real Problem with Autonomous Vehicles*. Retrieved from www.electronicdesign.com:

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218

https://www.electronicdesign.com/automotive/testing-unknown-real-problem-autonomous-vehicles
privacy4cars. (2018, November 16). *CarsBlues Vehicle Hack Exploits Vehicle Infotainment Systems Allowing Access to Call Logs, Text Messages and More*. Retrieved from www.privacy4cars.com: https://www.privacy4cars.com/can-my-car-be-hacked/default.aspx
QAD CEBOS. (n.d.). *www.cebos.com/blog/milestones-automotive-manufacturing/*. Retrieved from QAD CEBOS: https://www.cebos.com/blog/milestones-automotive-manufacturing/
Qualcomm. (2018). *5G NR based C-V2X.* Retrieved from www.qualcomm.com: https://www.qualcomm.com/media/documents/files/5g-nr-based-c-v2x-presentation.pdf
Qualcomm. (2018). *Connecting vehicles to everything with C-V2X.* Retrieved from www.qualcomm.com: https://www.qualcomm.com/invention/5g/cellular-v2x
Rouf, I., Miller, R., Mustafa, H., Taylor, T., Oh, S., Xu, W., . . . Seskarb, I. (2010). Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study.
RunSafe Security. (2019, February 04). *Binary Randomized Security*. Retrieved from https://runsafesecurity.com: https://runsafesecurity.com/blog/binary-randomized-security/
Rus, T. (2017, December 22). *Car hacking: a real risk we're ignoring when in fact, we shouldn't*. Retrieved from drivemag.com: https://drivemag.com/news/car-hacking-a-real-risk-we-re-ignoring-when-in-fact-we-shouldn-t
Sabih-ur Rehman, M. Arif Khan, Tanveer Zia, & Lihong Zheng. (2013, January). Vehicular ad-Hoc networks (VANETs)—An overview and challenges.
SAE. (2018, 12 11). *SAE International Releases Updated Visual Chart for Its "Levels of Driving Automation" Standard for Self-Driving Vehicles*. Retrieved from Sociaty of Automotive Engineers: https://www.sae.org/news/press-room/2018/12/sae-international-releases-updated-visual-chart-for-its-%E2%80%9Clevels-of-driving-automation%E2%80%9D-standard-for-self-driving-vehicles
SAE. (n.d.). DSRC Implementation Guide: A guide to users of SAE J2735 message sets over DSRC. SAE International.
The Industrial Internet of ThingsVolume G5: Connectivity Framework. (2018). Industrial Internet Consortium. Retrieved from www.iiconsortium.org: https://www.iiconsortium.org/IICF.htm
University of Michigan. (2017, March 14). *Sonic cyber attack shows security holes in ubiquitous sensors*. Retrieved from Michigan News: https://news.umich.edu/sonic-cyber-attack-shows-security-holes-in-ubiquitous-sensors-2/
US National Highway Traffic Safety Administration. (2017, September). *Automated Driving Systems 2.0 - A Vision for Safety.* Retrieved from NHTSA: https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf
Vora, M. L. (2015). EVOLUTION OF MOBILE GENERATION TECHNOLOGY:1G TO 5G AND REVIEW OF UPCOMING WIRELESSTECHNOLOGY 5G. International Journal of Modern Trends in Engineering and Research.
zhaoshentech. (2018, September 17). *IoT4Car*. Retrieved from www.hackster.io: https://www.hackster.io/frankzhao/iot4car-1b07f1

Institutional Repository - Library & Information Centre - University of Thessaly
02/05/2024 21:11:56 EEST - 18.226.214.218