CURRENT THREAT AND HOW WE CAN IMPROVE THE FUTURE OF THE AUTONOMOUS CARS

Ryo Shiraishi 195557IVSB

Tallinn University of Technology | Cyber Security Engineer

INDEX

Table of Contents

Introduction

In this paper, I would like to talk about current problems that autonomous cars are facing and its future how we can improve in order to solve the problems. Currently we are facing many problems with autonomous cars, this is because due to autonomous cars are still in development stage even though some manufacturers are making available for customers, such as Tesla. However, these manufacturers are still facing problems from uncertain car accidents. Moreover, there is one big problem with autonomous cars, since they are connected to the Internet, which it is hackable, which we are still not aware how easily it can be hacked and also how dangerous it is. Therefore, I would like to talk about these problems and how we can solve for the future cars.

Autonomous vehicles

Ideas about autonomous cars

In an autonomous car there are various kinds of sensors attached in order to sense the environment around the car. The operating system in the car will gather this data and enables the car to automatically drive itself to the set point without the human interaction on the wheel. On top of that as there is no need for the human interaction on the wheel, therefore no need of humans on the car, this enables the passenger to call their car through the smartphones or tablet to come pick you up. As the car will be coming pick the passenger up, even the disabled person who cannot walk will be able to call their car easily which will be convenient for them. As well as who cannot drive, the autonomous car will not need the interaction between human, allowing even disabled person to have their own car without any assistances.

Dangers regarding autonomous vehicles

However, even though saying with autonomous vehicles there are no need for human interactions on the wheel, there can be some kind of accidents can occur. Even the software or hardware itself may not be robust enough in order to prevent from some kind of accidents, since there can be a bug in the software or not robust enough or the hardware is not functioning correctly. These two are some example factors can lead to some kind of accidents, since the passengers on the autonomous vehicle, may not be paying attention to what is happening around them, the environment and will not be able to react quickly. Since the passengers are relying on the autonomous functionality, the possibility that they are not focusing on the driving is high, they maybe on their phone, watching a video, talking with other passengers or may not be even sitting on the driver seat. Which this will lead to no access to the steering wheel and brake, causing accident which can be life threatening. The drivers are required to pay attention even if the car is in autonomous mode. This is because if they are paying attention, they will be able to stop the car or avoid getting an accident by changing its direction quickly, since even the software can make an error through bugs.

Moreover, in sever conditional environment, for example in a sudden storm, the sensors may not be able to recognize the environment around it. Rain or snow can interfere the signal coming into the sensors and will not be able to detect. Also even if the sensors are working properly, the car can slip from wet or the bad condition road, due to not being able to detect the condition accurately and the speed may not be suitable for in that condition. In this crucial condition if the passenger who should be responsible for driving is not paying attention, this can lead to some kind of accident. On addition to this sunlight can cause some interfere on camera and causing accident. According to one of the articles, from the light coming into the cameras used for processing image for autonomous vehicle, this can cause some affect to the

functionality[1][1]. Furthermore, in case of the car do not stop or not able to change the direction even if the car is coming from the other side or due to environmental issue, the passenger who is responsible for driving must be able to react quickly like during normal driving.

Furthermore, since autonomous vehicles are connected to internet, smartphones, IoT and many more connections are possible. There are some vulnerabilities that we are unware of, such as radio signal attack and Bluetooth attack. These are available tools for hackers to be able to make a use of in order to hijack the cars and harm people. We are still unaware of how dangerous these methods of attack can be. Since even the cars have equipped with computer components and connected to the Internet of course there are some ways we can get through to gain access to the computer in the car and take over the control. Additional to this as there are many people nowadays have cars and even autonomous vehicles such as Tesla car, hackers are targeting these cars to find any vulnerabilities and make a use of in such a bad way. Since people who are driving autonomous vehicles are relying too much on self-driving method (autonomous driving), the drivers are unaware when their car can get hijacked and causing them harms. Hackers can execute easy code to that car remotely, cause harm to these people. Even if their car gets hacked and taken over the control, the passengers cannot do anything but at least could have saved their lives. This is by doing appropriate procedure, since if the passengers are aware of what is happening to the car, they will be able to act quickly. On other hand if they are not on phone or talking to other passengers on the car, their attention will not be the car, which they will not be able to act quickly. Which I think nowadays people are relying too much on technology and thinking that there are no errors in these small computers and hardware. However, this is completely wrong, people are not aware of that even still computer can make some kind of errors, therefore there are updates released by the manufacture in order to fix these errors. Since, people think computer are safe, even the autonomous cars are safe, therefore, I would like to inform people that how technology is still no completely safe to rely on it. Moreover, autonomous car technology is just evolved, which not safe to rely yet.

Further explanation about issues with autonomous vehicles

There are several issues regarding environment that will cause some dangers to the passengers on the autonomous vehicle. As I like mentioned before, weather condition can affect how sensors on the car to collect environment and light glare into camera can affect how the autonomous car to understand the condition. In this section I would like to talk more about how these can be big issues for autonomous vehicles. Unexpected weather change is one of the biggest steps for autonomous vehicles. Since autonomous cars navigate its self through by collecting many information through their cameras and sensors on the car, however if the environment instantly changes, say going into fog, heavy rain or snow, the car will not be able to collect many information. This is because as the camera and sensors are interfered, the car will not be able to process to build up how the road ahead will be like. For example street markers, lane dividers, fence, where the cars are located, signs and many more, these will be hard to be detected. Current autonomous vehicles have almost similar level of driving skills that humans are capable of, however a bit safer since autonomous vehicles can adapt to changes much quicker than humans. For example, if you think of driving in the night, rain, fog or snow, it will be harder to drive than in the clear sunny day. However, if the condition is much more sever, where you cannot see anything due to the bad

[1] https://www.patentlyapple.com/patently-apple/2018/03/apple-reveals-a-vital-safety-system-for-autonomous-vehicles-focused-on-eliminating-blinding-light-glare.html

views from rain, fog or snow, similar for autonomous vehicles this will be much harder. In a such condition like during the night, autonomous vehicles will have no struggles, this is because, use of many sensors and infrared cameras, these technologies will be able to vision the street even in the dark which cannot be done by humans. On other hand, in the severe weather condition even the view from the cameras and the sensors will be interfered. Sensors that autonomous vehicles they use are such as Light Detection and Ranging (LIDAR). This sensor uses light by bouncing it back from the sensor to the obstruction and measure the distance between the car and the obstructions. Then this information that was collected from LIDAR will combine with information being collected from camera to make a virtual map[2][2]. This allows the autonomous cars to understand how the environment around it is like, where the other cars are located, how the road is like and where to follow on the road and many more. Moreover, Velodyne's Gopalan mentions that, "If there's bright sunlight or if it's really dark at night, some of these [camera-based] features are not reliable and not available all the time," as well as "Adding a LIDAR will make two features much more reliable and much more readily available."[3][3] As I like mentioned my self earlier, environmental factor can affect camera and other sensors, whereas, LIDAR will aid the car even in any crucial conditions that camera and other sensors are while interfered. However, there are some autonomous vehicles do not use LIDAR sensor, instead they only use radar, GPS, maps, cameras and sensors, such as Tesla, "Tesla and Elon Musk have opted to eschew the use of LIDAR.". With LIDAR sensor since its functionality is to detect and map out the environment such as terrain and road, the severe weather condition may affect the sensor not being able to measure the accurate distance between actual obstructions, road conditions and terrain. Additionally, even with cameras, due to the severe weather condition if there are no good views around the car, the computer will not be able to produce precise and accurate virtual map. This leads to the autonomous cars not being able to drive safely on the road. Since these problems are arising, we must come up with new methods for the future autonomous cars. Also the car manufactures must understand how all these sensors work, since there may be some manufactures do not implement LIDAR camera due to the cost. However, this is not the point what I think, they are required to manufacture something that is totally safe for the people on the car. Therefore, even if the manufacture cost goes up, they are required to somehow implement LIDAR sensors in order to produce an autonomous car that is safe for people.

Secondly, the problem arise from the camera is that change in light condition can cause some interference for autonomous vehicles. For example, entering in and out of a tunnel, since there is a change in amount of light coming into the camera and need to adjust this light level. Also the glare of sun shine on camera will interfere the views. Cameras act as similar to our eyes, since if we turn on the light in the dark room, our eyes have reflex to adjust to be able to see from dark to bright room. For autonomous cars especially, they have to perform real-time computing to act as soon as possible if any condition changes, such as if pedestrian comes in front of the car suddenly, then the car must act accordingly to stop or prevent from hitting them. However, since the cameras' light needs to be adjusted, the interference can cause the computer not being able to detect the environment around it and can be ending up hitting a pedestrian or car in front of it. Since many people think autonomous cars are equipped with high end technologies, the cameras and sensors will not be interfered, no limitations,

[2] https://oceanservice.noaa.gov/facts/lidar.html
[3] https://www.theverge.com/2020/1/7/21055011/lidar-sensor-self-driving-mainstream-mass-market-velodyne-ces-2020

however, this is totally wrong. All these technologies have some limitations even if they are up to dated technologies. Therefore drivers are still required to focus even if they are on the autonomous car in order to handle if something goes wrong, allowing the driver to react quickly and avoid any kind of accidents.

Thirdly, the software and hardware may not be robust enough which there may be bugs can cause some errors and leading to an accident. These errors in the software or hardware causes the car not be able to make the right decisions accordingly. First example is that detection may not be accurate, such as not being able to detect the objects in front of the car leading to crash. If the hardware and software will not be able to communicate, then will be leading to not able to detect the object and crashing into an object. Secondly, another feature that is important for autonomous vehicles is to be able to identify the object, for example need to be able to identify what the road sign is showing, if the road sign is showing pedestrian cross and pedestrian is crossing, then the car must identify and stop until they finish crossing. Also need to be able to identify the traffic light, whether is it red, yellow or green therefore the car can decide on its own. If the software is not robust enough such as not enough machine learning has been done to teach AI to able to identify the road signs, objects and many other objects, then the car will not be able to make a right decision according to the object what is in around the car. Also if the car is deployed with this poor software, the autonomous cars will not be reliable and the people will not be convinced to buy since it can cause accidents. Thirdly, validation, since decisions made by autonomous vehicles are made by AI. In a such condition of where if another car which is not autonomous vehicle is turning around since the driver of that car did not see this autonomous vehicle was coming from other side of the road, the software must make validation if they have to stop or safe to keep going. However, as the software is not robust enough the AI will not be able to machine learn and make right decisions. It will keep making similar mistakes in future and the autonomous car will not be safe enough to be driven on the road publicly.[4][4]

This suggests that even if we rely control on autonomous vehicles there will be some threats of involving into accidents which may be serious or not. Since the hardware and software are not still robust enough for due to the technology and autonomous cars is just about getting evolved, we still have to be aware while riding an autonomous vehicle. Furthermore, such as with artificial intelligence in the software, there must be more training to be done in order to make better decisions in a such situation.

Cyber-attack threat

More other than software and hardware issues there are concerns with cybersecurity threats, since autonomous vehicles are connected to the internet hackers may be able to have access to the car itself by hijacking. There are no cases yet for any cyber threats for autonomous cars, however I will be taking up a few examples that may be able to be performed in near future since there are many autonomous vehicles nowadays equipped with new technologies. Since newer cars those are not even autonomous cars are equipped with radio signals, Bluetooth and even with Wi-Fi connection, which these are the main route for the hackers to hack cars.

One of the examples of way to hijack cars is by using radio signal, not even hackers but anyone can get this radio device which allows to steal the radio signal sent from key fob to

[4] https://www.autotrader.com/car-shopping/self-driving-cars-software-issues-continue-to-slow-development-of-autonomous-vehicles-266602

copy the signal. The device can be bought from online in as a small cost. This is performed by making that both the car and actual physical key is close together, however they are technically not. Since one of the attackers have this device a few hundred meters away from the key and another have near the victim's car, this is like a man-in-the-middle method attack which the device will be standing between the car and key fob. Once the owner pushes the lock button, the device will then steal that signal from the key and allowing to extract a radio signal of the entry system of the car. Once the device has read the signal eventually, allowing to be able to unlock the car's entry system. With this method, the hackers are instead of decode the radio signal code sent from the key fob, then copy it. Since before, opening the car's entry system, the system will send a signal to the key, however, the hacker's device act as a fake key, therefore, this device will retrieve this signal first. This is like an acknowledge message between the entry system and the key, in order to check if the key is located near the car. Once the signal is copied, one the device in hacker's hand will relay that signal via radio to the actual owner's key. Then the hackers will instantly relay the key's response all the way back to the car along the route that was taken to reach from car to the owner's key fob. This tricks the actual key and the car that they are near each other. According to Jun Li, who is one of the researchers, use of two devices for this attack is in order to widen the range of key fob signal coverage to make it possible even if the car and key is further apart.[5][5] In order to tackle this problem, it must be understood by every car manufactures also the consumers must understand this attack can happen to their own car. Therefore, the manufactures are able to focus what to improve and the owner will be aware and will be cautious. First of all, car manufactures must focus on software side such as coming up with a new protocol so the communication between the car and key fob cannot be intercepted by a special device currently that is being used. For example coming up with methods such as use of private and public key to exchange signal or encrypted password between the car and key fob. This method will likely to prevent from signal to be intercepted since it is encrypted and only the owner with public key can send and private key can decrypt. If the signal exchanged was accepted by car then car can unlock the car, otherwise not. Also the owner must aware since the key fob is receiving the signal from car entry system and exchanging signal so the car will know the owner is near the car. In order to prevent this signal exchange, the owner can put their car key in a special bag or purse that will block out any signals. Therefore, the signal exchange cannot be intercepted leading copy of this signal by hackers can be prevented.

Another threat is that since most of the modern cars are equipped with Bluetooth especially with autonomous cars as they may be required in order to control the car from user's phone, such as unlocking the entry system, calling your car from another place, syncing your contact on your phone to car to make a call and many more other usages are there. According to one of the articles from MIT, it is possible to take over the control of the car wirelessly using Bluetooth. The experiment conducted by the researchers, they were managed to control any functionalities in a car, such as braking system, door locks, controlling dashboard displays and many more attacks were experimented. Previously, before this Bluetooth attack was found, similar attack was performed according to other professors. They managed to take control over the computer systems of a car, by physically accessing to the diagnostics port. This diagnostics port is officially mandatory to have under the law under the dashboard and equipped with most of the modern cars, since this computer will be able to monitor data about the car, such as carbon dioxide emissions, mileage, speed and many more.[6][6] Since this port is mostly used by car manufactures and maintenance people have not or no access to

[5] https://www.wired.com/2017/04/just-pair-11-radio-gadgets-can-steal-car/
[6] https://www.makeuseof.com/tag/obd-ii-port-used/

this port, which I think this method is less possible and can be protected easily. However, with this newer method by using two devices, it is done remotely, which there is no need of having access to the car physically. First of all, in this Bluetooth attack, they targeted the car's Bluetooth system, there was a vulnerability allowing them to run code that was made to take over the control of the car. This was simply performed by using a smartphone that was already connected to the car and get a way through to authorize a new phone connection using backdoors. The researchers were able to find a few more other ways to take control of the cars, since many cars are equipped with cellular connections, via this connection they were managed to execute code to break the authentication system.[7][7] The previous method, by physically accessing to the diagnostics port will be challenging since the hackers are required to actually connect to the port, therefore the risk of being car gets hijacked was low. However, newer method that was found using Bluetooth to hijack the car is really dangerous since it can be remotely take over the control of the car. As we and the car manufactures are unaware of this vulnerability, therefore, we use this functionality without thinking of any affects. However, we must make sure how to prevent from such attack. Also the car manufactures are required to understand how this attack is made and what can they do in order to protect from such threat, such as implementation of Bluetooth intrusion detection system feature. These vulnerabilities must be covered up as soon as possible otherwise many people will start to attempt to cause harm to the innocent people and can be make use for terror attacks as well. This leads to fall in sales of autonomous vehicles as well, since people feel that they are not safe and reliable to ride. Moreover, the prevention I can think of is by turning off Wi-Fi and Bluetooth at any time while not in use, therefore, the hackers are not able to discover and attack. This allows the driver to prevent from any such attacks. Also car manufacturers are responsible to come up with some new methods in order to protect from such risks in order to prevent from happening in future and protect their customers.

Since cars' functionalities are improving especially with autonomous vehicles, there are many vulnerabilities that car manufactures are unaware of. Therefore, even if we think that autonomous cars are convenient there are many threats that we are unaware and can threaten the innocent people's lives. We and car manufactures are aware of how cars are getting convenient and safer, however must make sure there are backside which is much more dangerous. According to Scott Ikeda which was Tweeted, "#Cyberattacks on connected cars should not be taken lightly as #hackers could use them for terrorism and assassinations. #respectdata"[8][8], which I truly agree wit him. Since nowadays there are many cars are equipped with new technologies which I like discussed earlier Bluetooth is one of the tools for hackers to remotely control the car. Which if this vulnerability is not closed, people will share this method and terrorists can make use of this to harm innocent people. Also people may not be aware of these vulnerabilities have on their car, which they drive their car as usual, which this can cause accident to this driver and passengers also to other drivers. Therefore, in order to prevent from this to be happening, if there are any vulnerabilities found in the car, car manufacturers are required to inform the owners and release update for fixing the patch as soon as possible, since they may have to use their car. By informing the owner and releasing update this allows to prevent from any such accidents to the innocent people and also the car manufacture will be able to have good relation between the customer. This will lead their customers to come back to their car manufacture to buy a car from them in future.

[7] https://www.technologyreview.com/2011/03/14/196375/taking-control-of-cars-from-afar/
[8] https://www.cpomagazine.com/cyber-security/connected-cars-a-new-and-dangerous-vector-for-cyber-attacks/

Future of autonomous vehicles
How to improve hardware and software
Since I discussed about issues with current hardware and software that autonomous vehicles have in the first half, I would like to talk about how we can improve for better experience of car ride in future.

As I have talked earlier that there are some autonomous vehicles just rely on camera and sensors by not using LIDAR sensor. Since just replying on camera is not precise and accurate to vision the environment around the car since glare of sunlight into the camera or from instant light change, going in or out from the tunnel will cause interference to the camera and not being able to detect the obstructions. In order to overcome this problem, use of cameras, LIDAR sensors and other sensors will be able to help this problem. This is because if the car goes out from the tunnel as I like said before, the camera needs to adjust the lighting, which this will take some few seconds, leading not be able to collect the environment data. However, even in this short time situations can change, the car in front may stop immediately or a pedestrian will come in front. This may lead to accident. On other hand LIDAR sensor will not be affected by how much the light is coming into the sensor. This sensor will simply send out light pulse to the object and measure how far the object is located. By calculating that measurement, it will create virtual map for the autonomous car to understand how the road is like and also detects any obstructions in front of the car. This allows the autonomous cars to be able to be driven in any lighting condition, no need to worry about instantaneous change in light conditions. However, another problem with LIDAR sensor system is that there is a latency. Since newer technologies are going to be added into the car features, the central processor will be required to do more processing especially with this crucial real-time processing and creating virtual maps are involved. As well as since newer technologies and features are added price of the car will increase. Therefore, there will be cause of latency and we need to come up with newer method also may lead less sales in autonomous cars due to price increase. In order to overcome this problem Stochino, the automotive sensor architectures and sensing industry added, “the kind required for L4 and L5 — would require a radically new approach. He founded Perceptive based on a vision of an all-digital platform with relatively-low-cost but high-performance sensors — antennas and cameras — around the periphery of a car, connected with optical fibre to a central processing core.”[9][9] According to what Stochino mentions, even if we implement newer technologies to the current model, it will be a bottle neck for central processing to collect and process the data, therefore we have to come up with new model which they came up with. The bottle neck is the major problem which cause central processing unit in the car not be able to collect and produce data since all these will become like in a processing queue. However, with the new method, due to the less latency and lower cost high performance sensors equipped with the autonomous cars the cars, the car will be able to make decision quicker leading to safer driving experience and will attract new customers, since they are safe and reliable which the accident rate may be lowered. On top of how more attraction to autonomous cars, it will attract new customers to the car market as well which will benefit the car manufacturers, also they can compete with others leading to more profit coming into the business and produce up to dated safest car in future as well.

[9] https://www.extremetech.com/computing/305691-the-future-of-sensors-for-self-driving-cars-all-roads-all-conditions

Talking about software side, since with autonomous vehicles it is mostly relied on AI for safer driving experience. In order to do this will require constantly maintaining and updating in order to keep improving the software of the autonomous cars, therefore the passengers will be able to ride safely. For example, by improving the software, the camera will be able to detect objects more accurately, since these identification and object detections are done by software. As the software for detection system improves, the car will be able to accurately and precisely detect objects, this includes identifying whether the traffic light is green, yellow or red, detecting the pedestrians, road signs, weather condition and many more. Moreover according to Apple's research paper based on autonomous car software, the combination of software using neural networks and LIDAR sensor will improve the detection of smaller objects also that's in distant.[10][10] Therefore, this will lead to better detection of a pedestrian in a distant, since unlike cars, it will be harder to detect a pedestrian in distant, therefore this will lead to safer autonomous car ride and able to decrease the number of accidents. Neural network is a way for artificial intelligence to machine learn their own self. In neural networks model, there many connections between multiple nodes with layers. On one side there is an input layer where data is coming in, with autonomous vehicles that will be the image. Then this input layer will be passed down to the hidden layers where all the process will happen, in this layer the input data will be compared between the data that is already in hidden layer and compared to eventually making to output layer.[11][11] The software will learn the pattern of data on its own self and this will constantly keep happening in neural network, this is also machine learning. This is one way the autonomous cars can learn by their own self from many driving experiences. Another method that I can come up with is that the car manufacture can keep the software updated from software development department can keep training the AI. Due to the training of AI, the autonomous cars will be able to make an accurate and precise decision much quicker and predict what's going to happen, for example which route will be efficient to take and what will be likely to happen in road ahead. Then once the AI is trained, they can distribute a new software updates to the cars in order to keep the software robust and safe on the road.

Furthermore, from neural network, even in the severe condition of weather, the autonomous driving functionality will be much safer. Since the software has learned the environment condition during the severe weather condition they will be able predict what's likely to be happening in road ahead. Also by communicating between multiple sensors and cameras such as thermal camera and LIDAR camera, in the fog it will be able to detect objects in ahead of the car. Since thermal camera detects the heat from the objects, therefore if the view is not clear ahead, by detecting the heat the car will be able to understand whether there is an object ahead or not. According to FLIR, one of the companies produce thermal imaging, night vision and infrared cameras, "Thermal, or longwave infrared (LWIR), cameras can detect and classify pedestrians in darkness, through most fog conditions, and are unaffected by sun glare, delivering improved situational awareness that results in more robust, reliable, and safe ADAS and AV."[12][12] This suggests use of thermal cameras it will be much more safer to detect any objects ahead in any kind of situations especially within darkness and foggy environment. The combinations of software with neural network and technologies will be able to make autonomous cars much safer in future even in the severe weather conditions.

[10] https://www.techrepublic.com/article/apples-autonomous-car-software-uses-neural-networks-to-improve-navigation-object-detection/
[11] http://pages.cs.wisc.edu/~bolo/shipyard/neural/local.html
[12] https://www.flir.com/discover/oem/automotive/why-adas-and-autonomous-vehicles-need-thermal-infrared-cameras/

Preventing from cyber-attack threats

Since talking about cyberattack threats on autonomous cars, I would like to talk about how to prevent from these threats, from what the consumers can do and what the car manufactures can do.

One of the methods to prevent from cyber-attack is to machine learn the behavior of car when it is attacked. By neural network in the car this will be possible, since the car will learn the behavior that happened before or is stored in somewhere in the car. Therefore, once the car detects the same activity, they can notice the driver. This is the same approach to how car's software can improve in order to make the driving experience for the passengers better. Since detection of any cyber-attack on the car will be detected using software as well, machine learning will be best approach and a major step for the car manufacturers to make their cars safe and preventable from such attacks. According to Toptal Enterprise, one of the approaches in order to detect these analyze the behavior is by using Elasticseach., "illustrates how a car's user logs could flow into an Elasticsearch database, which would enable algorithmic detection of potential exploits."[13][13] Since using this analysing method, machine learning will be able to study what kind of behaviour the car can experience if it is hacked, such as unexpected brake signal sent to the central processor while there are no cars around it or engine shutdown signal sent unexpectedly. Furthermore, from my perspective, since cars are connected to the internet, they can share this threats information to other vehicles which allows other cars to prevent from a such attack in the future. Therefore, in future the autonomous cars will be communicating with other cars as well in order to share information regarding the threats that other cars have experienced. This allows all the cars to keep up to dated with new threats that are evolving in real time. Also if there is a new zero-day attack is deployed across multiple cars, this logs can be sent to the data centre where all the information about the cars, vulnerabilities, and many others. Then at the data centre it can be analysed if this is a new attack or not, if so then share this information to other cars, which allows to minimize the risk of many numbers of cars getting attacked by this new zero-day threat. Therefore, what I think of current car manufactures are required to do is, start training AI for the future development of their autonomous vehicles. Since there are currently a few markets where they have autonomous vehicles, starting training now will be able to compete in near future market where many markets are coming into autonomous vehicle. Stakeholders are willing to buy safer cars since cars are expensive to buy and have many useful features, therefore, manufactures with better software with safer driving experience will be tend to perform better in autonomous vehicle market. Which I suggest that car manufacturers have to put more focus on software development department as well along other departments.

Secondly, since new generation cellular network is evolving recent days, now the 5G is the main big step for autonomous cars. Since these cars are required to connect to the Internet in order to retrieve new data from or to data centre, communicate with other cars on the road to share traffic data to which route will be efficient and take less time. However, 5G is a big step forward for hackers to deploy massive cyber-attacks. Due to 5G providing us with newer experience of Internet usage, better experience, faster Internet connections, more things can be done that was not possible with 4G. Since autonomous cars are once of categories in IoT, hackers are able to make use of this in a wrong way, using autonomous cars as a resource for

[13] https://www.toptal.com/insights/innovation/how-machine-learning-can-enhance-cybersecurity-for-autonomous-cars

hacking device and possible to deploy DDoS attack. These cars will be turned into botnets and deploy attacks, according to one of the reports from University of California Los Angeles, "vehicular botnets can be used to perform variety of dangerous attacks - some seemingly more attractive than the congestion attack (e.g. stealing the compromised cars themselves)."[14][14] As I like mentioned earlier, even the cars can be used as a weapon, it is not surprising to hear, since there are many DDoS attacks has been done using IoT, but we are not totally aware of that it can be done using cars as well. Since in near future, there will be many autonomous cars and I think if we do not act now, to find solutions to prevent from any kind of these attacks, the future will be in a disaster, causing harms to innocent people and terrorists can make a use of this. Therefore, we as a cyber security engineer need to work to find a way to stop and prevent from such attacks like this.

Conclusion

Overall, since I have talked what are the weaknesses of current autonomous cars are having and solutions to that what we can do in order to make better driving experience as a passenger, safe from any kind of environmental, software and hardware side and cyber-attacks threats. These environmental and software and hardware issues are relatively much easier in order to make the driving experience safer since there are many solutions available and car manufacturers can come up with solutions. However, with software and hardware side, there is a need for training of AI, in order to do this, it can take a while. Since there will be many tests to be done in different conditions. For example, testing in a light weather condition as well as in a severe condition. Think of human while learning new skills, similar to this AI need to undergo many tests to be able to make the software robust enough. Through this machine learning, the AI will improve its algorithm over the time, allowing better prediction, deliver better driving experience for the passengers and safer. Otherwise, if only a few tests are done, the software will not be robust enough since the algorithm of AI is weak, if we talk from a human perspective, less knowledge. Which leads to not being able to deliver safe driving experience since not being able to predict what's going to happen in ahead of the road according to the data being collected from camera and sensors.

Moreover, with cyber-attack side, since each autonomous car is like a single computer with wheels. Therefore, there must be a mitigation from cyber-attacks by on its own self in real time and decide accordingly. To do this, AI will be in demand as well, along the software to make the car to be able to be driven safely on the road. Since cyber-security is a challenging task for car manufactures, it is not something it can be solved easily. This is due to new technologies are evolving which leads to new hacking methods are going to be developed. In order to tackle with these challenges, the car manufactures are required to be up to dated with new hacking methods that are being developed in order to make the passengers to be able ride the autonomous cars safely.

[14] https://www.ndss-symposium.org/wp-content/uploads/2017/09/01_1_3.pdf

Sources

[1] - https://www.patentlyapple.com/patently-apple/2018/03/apple-reveals-a-vital-safety-system-for-autonomous-vehicles-focused-on-eliminating-blinding-light-glare.html
[2] - https://oceanservice.noaa.gov/facts/lidar.html
[3] - https://www.theverge.com/2020/1/7/21055011/lidar-sensor-self-driving-mainstream-mass-market-velodyne-ces-2020
[5] - https://www.wired.com/2017/04/just-pair-11-radio-gadgets-can-steal-car/
[6] - https://www.makeuseof.com/tag/obd-ii-port-used/
[7] - https://www.technologyreview.com/2011/03/14/196375/taking-control-of-cars-from-afar/
[8] - https://www.cpomagazine.com/cyber-security/connected-cars-a-new-and-dangerous-vector-for-cyber-attacks/
[9] - https://www.extremetech.com/computing/305691-the-future-of-sensors-for-self-driving-cars-all-roads-all-conditions
[10] - https://www.techrepublic.com/article/apples-autonomous-car-software-uses-neural-networks-to-improve-navigation-object-detection/
[11] - http://pages.cs.wisc.edu/~bolo/shipyard/neural/local.html
[12] - https://www.flir.com/discover/oem/automotive/why-adas-and-autonomous-vehicles-need-thermal-infrared-cameras/
[13] - https://www.toptal.com/insights/innovation/how-machine-learning-can-enhance-cybersecurity-for-autonomous-cars
[14] - https://www.ndss-symposium.org/wp-content/uploads/2017/09/01_1_3.pdf