Threats and Attacks to Modern Vehicles

Philipsen, Simon Grønfeldt; Andersen, Birger; Singh, Bhupjit

Published in:
2021 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS)

Link to article, DOI:
[10.1109/IoTaIS53735.2021.9628576](https://doi.org/10.1109/IoTaIS53735.2021.9628576)

Publication date:
2021

Document Version
Peer reviewed version

[Link back to DTU Orbit](#)

Citation (APA):
Philipsen, S. G., Andersen, B., & Singh, B. (2021). Threats and Attacks to Modern Vehicles. In *2021 IEEE International Conference on Internet of Things and Intelligence Systems (IoTaIS)* (pp. 22-27). IEEE. <https://doi.org/10.1109/IoTaIS53735.2021.9628576>

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Threats and Attacks to Modern Vehicles

Simon Grønfeldt Philipsen
DTU Engineering Technology
Technical University of Denmark
Ballerup, Denmark
S163595@student.dtu.dk

Birger Andersen
DTU Engineering Technology
Technical University of Denmark
Ballerup, Denmark
birad@dtu.dk

Bhupjit Singh
DTU Engineering Technology
Technical University of Denmark
Ballerup, Denmark
bhsi@dtu.dk

Abstract—As modern vehicles are complex IoT devices with intelligence capable to connect to an external infrastructure and use Vehicle-to-Everything (V2X) communication, there is a need to secure the communication to avoid being a target for cyber-attacks. Also, the organs of the car (sensors, communication, and control) each could have a vulnerability, that leads to accidents or potential deaths. Manufactures of cars have a huge responsibility to secure the safety of their costumers and should not skip the important security research, instead making sure to implement important security measures, which makes your car less likely to be attacked.

This paper covers the relevant attacks and threats to modern vehicles and presents a security analysis with potential countermeasures. We discuss the future of modern and autonomous vehicles and conclude that more countermeasures must be taken to create a future and safe concept.

Index Terms—Modern vehicles, autonomous car, security attacks, security countermeasures.

I. INTRODUCTION

The future of Internet-of-Vehicles technology and self-driving is flourishing. These new cars are packed with technology, which makes driving a lot easier and safer, using sensors, entertainment systems, GPS and autopilot. There are different levels of autonomous driving vehicles. The definition of which level and what the differences are between them can be found in [5]. The levels of automation described in this article are from level 3 to level 5. So, are these cars safe to use? Could a potential attacker control the car and make it crash? To find the answers, one will have dig deeper into which threats that these cars, will face in the future.

Several companies are investing in this field and are competing to release the latest and safest autonomous cars. Cyber-attacks are a significant threat, both to industry and to consumers, security measures in these cars will have to keep up with new threats and new methods of attacks that are being developed as rapid as the Internet-of-Vehicles development. So, if the companies tries to cut corners with their technologies without the thought for security, it can end up with consumers losing trust in these companies [6].

Modern-day vehicles are not just mechanical parts moving around spending gasoline. Nowadays, there are millions of lines of code involved in building the software and hardware for modern autonomous cars. In fact, there are more lines of code in modern autonomous cars, than in a Boeing 757 aircraft, according to [12]. More than 100 million lines of code are put into an autonomous car, and all these lines of code have to be checked for bugs, errors, and fail safes in order to be safely released to the public consumer.

Multiple white-hat hacker groups are testing these cars and their flaws, some even successful, proving the companies

who makes these cars, that the design of either hardware or software can be compromised and abused for either harming other people or collecting data of people's location. Tencent Keen Security Lab is one of the teams who are working with these companies to make them safer. In their blog [13] they showcase an example of how bad it can go, when the autopilot function has been compromised within a Tesla S model.

Another team also found a way to compromise a jeep, which can be remote controlled to such an extent, that they have full control over every function of the car. Abusing the entertainment system in the car, gives them access to every system, including the engine. The test person in the car, have no control over the car anymore, which could lead to a potentially dangerous situation [14].

II. UNDERSTANDING THE CAR

Before we can begin to understand how to protect our cars from attacks, we first must understand how most modern automated vehicles are functioning, and which parts of the car does what. Most systems running in automated cars today, can be divided into 3 different set of organs: Control, Communication and Sensing. Each have a role to play, and all have to be able to communicate with each other in such a way, that the features of the car are all functional. In Figure 1 we can see the 3 layers and their respective functions.

In the bottom of the pyramid, we have sensing, which covers all the sensors, cameras and GPS [1]. If those are compromised, the car will already lose the automated functions such as, autopilot, if such feature exists in the car.

The next layer is communication. This part of the car holds in-vehicle communication also called "CAN bus" (Control Area Network), OBD (On-Board Diagnostics) ports and other telematics. This part of the car could be vulnerable of manipulation in messages between vehicles, V2V (Vehicle to Vehicle) and V2X (Vehicle to Everything). This part also

Fig. 1. The Autonomous Vehicular Sensing-Communication-Control (Au-toVSCC) framework

holds, software updates and version control [1]. The in-vehicle network is also affected of data coming from the sensing layer, which could potentially be compromised and would send incorrect data.

Threats to both the sensing and communication layers can affect the topmost tier functions in the car, the control layer, which affects functions of the car, such as vehicle speed and steering control, brakes and much more. It also covers all psychical tampering with the car, entry points such as: USB, OBD, electrical charging port and other ways of getting into the in-vehicle network. If compromised, it would be a serious breach, would weaken trust between consumers and the company providing the car.

III. ATTACKS AND COUNTERMEASURES

In this section we are considering attacks and countermeasures layer-wise.

A. Attacks on Sensing Layer

Modern autonomous vehicles use different sensing technologies sensors like: GPS, MMW (MilliMeter Wave) radar, LiDAR (Light Detection and Ranging) sensor, ultrasonic sensor, and camera sensor. this section will briefly describe attacks on sensing layer.

1) *GPS Jamming and Spoofing Attacks*: GPS jamming happens when a cyber-criminal blocks GPS signals. Selling or using GPS jamming equipment that can block communications is illegal in most of world. However, jamming is also possible by means of legal low-cost SDR (Software Defined Radio) [30].

While jamming might seem to be the biggest threat here, GPS spoofing is harder to detect. A spoofing attack is a situation in which a person or program is successfully identified as another by falsifying data, to gain an illegitimate advantage. GPS spoofing allows hackers to interfere with navigation systems without operators realizing it. The fake GPS feeds cause drivers to go off course without any coercion.

GPS spoofing happens when someone uses a radio transmitter (SDR) to send a counterfeit GPS signal to a receiver antenna to counter a legitimate GPS satellite signal. Most navigation systems are designed to use the strongest GPS signal, and the fake signal overrides the weaker but legitimate satellite signal. GPS signal spoofing can be easily achieved using a simulator that gives a fake satellite signal [16], however more advanced spoofing techniques might give problems in the future and will be in dire need of research. According to [15], advanced spoofing techniques, now makes cars vulnerable to GPS signal spoofing.

2) *MMW Attacks*: MMW radar uses many different frequencies, but the 76.5 GHz band is exclusively for automotive radar systems worldwide. MMW radar jamming, and spoofing attacks were demonstrated in Defcon24 in 2016 [17]. The demonstration showed that it was possible to jam and spoof the radar, which caused blinding and malfunction of the Tesla, which could potentially lead to crashes and impair the safety of self-driving cars.

3) *LiDAR Sensor Attacks*: In the article "Remote Attacks on Automated Vehicles Sensors", it was demonstrated the effectiveness of relay attacks and spoofing attacks on LiDAR. A cheap transceiver was able to inject fake objects that are successfully detected and tracked by the ibeo LUX 3, which is the current model tested. These attacks show that more countermeasures are needed in order protect these automated cars from reacting to fake cars, placed by attackers [18].

4) *Ultrasonic Sensor Attacks*: In the report "Can You Trust Autonomous Vehicles", they tested Tesla, Audi, Volkswagen, and Ford using ultrasonic sensor attacks, jamming and spoofing attacks. They showed that all tested vehicles were able to be jammed and spoofed by transmitting ultrasonic pulses with similar patterns [17].

5) *Camera Sensor Attacks*: In the article "Remote Attacks on Automated Vehicles Sensors", they tested a camera sensor (MobilEye C2-270) by blinding the camera with laser and LED matrix. The attacks confused the auto controls. For the MobilEye C2-270, a simple laser pointer was sufficient to blind the camera and prevent detection of vehicle ahead [18].

B. Countermeasures for Sensing Layer

Countermeasures depend on the sensor type.

1) *Spoofing Countermeasures*: In the article "GNSS Spoofing and Detection", it was found that combining strategies can provide a reasonably secure countermeasure that could be commercially deployed [15], using different techniques such as Advanced Signal-Processing-Based Techniques for a Single-Antenna Receiver, Encryption-Based Defenses, Defenses Based on Drift Monitoring and Signal-Geometry-Based Defenses. Many of the spoofing detection strategies have weaknesses that might be exploited by a sophisticated spoofer. In some cases, the strength of one strategy might offset the weakness of another. Thus, the simultaneous use of two or three complementary strategies might provide a very powerful means to detect spoofing. However, in the article is also written "A number of these defenses will remain vulnerable to a determined spoofer with a very large budget". This means that the current tested hardware devices, available to the market, are still in danger of spoofing attacks.

2) *MMW Radar Countermeasures*: The radar is normally used to detect cars and objects, through different weather conditions such as, snow, rain and fog. In [19], is proposed a data fusion algorithm to combat these attacks, making it significantly harder to inject and jam, and easier to detect incoming attacks. Furthermore, in [20] is agreed that moving the frequency from 76.5 GHz band to over 100 GHz, could increase the accuracy of the radar.

3) *LiDAR Countermeasures*: It is possible to relay and spoof on the ibeo LUX 3. According to [21], it is possible to use different types of wavelengths to counter potential attacks. By combining multiple wavelength LiDAR makes it

significant harder for the attacker to attack both signals at the same time. The budget for the attacker is also increased, therefore less likely to happen. Another way of adding more security, would be to use V2V communication. The way that V2V communication works is by sharing measurements, so that the vehicle, which is being attacked, can compare other vehicles data to detect inconsistencies. However, this method, also opens up potential threats of other vehicles sending false measurements.

4) *Camera Countermeasures*: There is countermeasures that exists [18], which can protect the camera of being tampered with. However, there is a significant increase in both price, and space. if someone really want to attack your camera with a laser, they can do so, if spending enough resources. So manufactures would have to decide how well they want to protect their consumers, for a certain cost. Most of the countermeasures require the camera to be modified. This not only increases the cost, but also the dimensions of the device, which can be problematic for the cost-driven and space-restricted automotive environment.

C. Attacks on Communication Layer

Figure 2 illustrates the many ways that attackers can maliciously interfere with vehicular communication. To combat these threats, all forms of communication within the in-vehicle network must meet underlying common security requirements.

In-vehicle communication is using CAN bus [2], enabling communication via CAN frames broadcasted to all the nodes connected to the CAN bus. Every ECU (Electronic Control Unit) receives the frames transmitted on the CAN bus and can decide whether to take corresponding actions after identifying the frame ID. Terms like 'nodes' or ECUs are parts of the body, interconnected via the CAN bus. Information sensed by one part can be shared with another. In an automotive CAN bus system, ECUs can, e.g., be the engine control unit, airbags, audio system, etc. A modern car may have up to 70 ECUs.

To enhance in-vehicle network security, it is valuable to study the principle of in-vehicle network attacks. A series of experimental studies on how to attack in-vehicle networks have been accomplished [2]. In this section we will go through different attacks and countermeasures to in-vehicle

network attacks.

1) *Frame Sniffing*: Frame sniffing is the starting point of all attacks made to the in-vehicle communication. CAN frames are broadcasted to all nodes, hence a compromised node, can intercept all frames transmitted via the CAN bus, by accessing an in-vehicle network via available interfaces (e.g., the OBD port, telematics system). After analyzing historically recorded frames, the details of the CAN frames can be known. In [22], Koscher et al. build a custom program called CarShark, which was build to intercept frames and data send by the can system. He realized that the range of valid CAN frames is small, which enables attackers to discover many different functions and weaknesses on selected ECU's. The method is also called "Fuzzing".

2) *Frame Falsifying*: By knowing the most of the valid CAN frames, attackers can now design their attack and send fake frames via the CAN bus. These fake frames contain false data that can mislead corresponding legitimate ECU's. Attackers can falsify the fuel level, change the speedometer reading and display failure information on the instrument panel cluster by falsifying frame data. The incorrect information may fool the driver, or even worse, cause dangerous behaviors [22].

3) *Frame Injection*: Attackers can use a malicious node as a starting point. The malicious node could be a laptop connecting the OBD port, a reprogrammed ECU, or the telematics system infected by malware. Worst case scenario, a reprogrammed ECU which can communicate via WiFi, Bluetooth or other wireless/remote technologies. In most existing studies, custom made software are developed to inject frames to the network. Setting appropriate frames' ID makes the target node on the CAN bus accept these fake frames [22].

4) *Replay Attack*: A replay attack is very similar to the above attacks, in fact, if attackers already are done with all the above methods, this would be the final nail in the coffin. Attackers now commands the malicious node to send valid frames to the CAN bus at the appropriate time. For a stationary car, attackers can open the door, start the engine, turn on the lights and drive the car away by injecting valid CAN frames to the car's in-vehicle network. Koscher et al. in [22] proved that the replay attack can be implemented in a real car scenario. Other related work to replay attacks have also been made by Hoppe and Dittmann, testing how to implement a replay attack in a simulated environment [23].

5) *DoS Attack*: DoS attacks (Denial of Service) are a possibility, because the frame ID indicates to the CAN bus, which frame should be transmitted first. No node is allowed to send frames in the network if there is a frame with the highest priority. Attackers can abuse this to command the malicious node to broadcast a frame with high priority all the time. In [22], the authors disabled the communication of individual components on the CAN bus via a DoS (Denial of Service) attack.

Fig. 2. Potential attack surfaces (<https://www.intellias.com/the-emerging-future-of-autonomous-driving/>)

D. Countermeasures of Communication Layer

A CAN network is vulnerable to attacks if attacker gains access to a malicious node, which could be a laptop connecting the OBD port, a reprogrammed ECU, or the telematics system infected by malware. Since the CAN bus has no authentication or encryption, security measures are needed to the CAN bus network. By enhancing in-vehicle network security, adding the functions of encryption and authentication, could be the two methods that might be effective countermeasures to provide confidentiality and reliability for a CAN frame [24]. Implementing this would seem like easy task, but it can cause different problems for the system. Efficient key management are needed to avoid scenarios like, attackers gaining access to private keys or worse. If more authentications are implemented, it can also degrade the transmission efficiency, which influences the vehicle maneuverability, especially for time-critical components [25]. Devices which are connected to the CAN bus system needs to implement authentication and encryption if you want to avoid the above attacks.

Woo et al. [24] proposed a security protocol, using AES encryption to encrypt the CAN frames. By extending the ID field and the 16-bit CRC field, that are used to verify the identity of the transmitted ECU, combining it with a counter to record the generation of frames, makes the proposed protocol robust to replay attack. In [25], Nilsson et al. proposed a mechanism to transmit a MAC (Message Authentication Code) by different frames. A 64-bit MAC is divided into four 16-bit parts and transmitted in four frames. This mechanism can help to improve the transmission efficiency of the authenticated frames.

E. Attacks on Control Layer

Control layer, as described above, is all the components of driving such as, steering, brakes, engine and transmission. If attackers decide to attack these components, it can end up creating a catastrophic event on a real car scenario of a moving car on the highway. As described in the sensing layer attacks and communication layer attacks, if both these are compromised, the control layer is vulnerable and cannot detect malicious frames from legit frames.

If sensors, radar, cameras are compromised, the control layer would not be directly affected, with exception to brake control, which will brake for you, if sensors detect an object in front of the car in a moving state. The brake control will not know the difference between a fake object or a real object. In both cases the car will attempt to brake. However, if communication layer is also compromised, attackers can trick your car into ignoring the message that sensors are sending via the CAN bus network and therefor car will not automatically slow down.

The control layer is affected, if a psychical attack on the car itself is happening, like tampering with the brakes, tires or any other part of the car, which are accessed from the outside. The other way of tampering can be compromising the two other layers (sensing and communication). In other words, if you cannot access the car psychically, you would have to compromise the either of the two layers, for you to gain access to the control layer.

1) *Control Override Attack*: A control attack, attempts to override the pilot of the vehicle attempts to take corrective actions against potential threats. Jo et al. [26] identifies security risks in Android OS-based telematics systems that enabled drivers to remotely unlock and lock car doors, start and stop the car engine using CAN. The article presents a scenario, where attackers download OTA (Over the Air) firmware, and then add methods to remotely control the car. It refers to the wireless delivery of new or updated software or firmware to devices such as smartphones and tablets.

2) *Injection Attack*: Injection attacks occurs when an attacker injects malicious messages like described in the communication layer section. Mazloom et al. [27], shows that using the MirrorLink protocol, which are used to link smartphones to infotainment systems in the vehicle, are vulnerable to attacks that leads to attackers gaining access to the CAN bus system and can inject malicious messages. According to Mazloom et al. they were able to generate a heap overflow within the MirrorLink and take control of a process inside the infotainment system. attackers can use similar invented methods to gain access to the in-vehicle network and send fake messages.

3) *In-Vehicle Network Access Attack*: If attackers successfully gains access to a OBD port, they gain access to the in-vehicle network. OBD ports are points of entry to the car which are vulnerable to attackers inserting an external device into the port. The OBD port enables the gathering of diagnostic information, access to the in-vehicle network, and the installation of malware [28]. Valasek and Miller [29] were able to transmit and receive messages over CAN bus using an ECOM cable (CAN to USB converter) and homemade connectors to connect to the OBD port.

F. Countermeasures of Control Layer

A control attack is very serious, if you are driving your car and you are not able to switch back to manual steering, braking or even accelerating, you will be in great danger of a potential crash. Therefore, it is of great importance that manufactures design your car in such a way, that attackers have a very hard time, accessing your cars internal organs, such as OBD ports, USB, wireless/remote and even electrical charging Countermeasures to telematics system vulnerabilities discussed by Jo et al. [26] suggests that code obfuscation (encryption of source code) could be implemented and proper code signing of any new firmware to prevent malicious or unauthorized code.

Injection attacks could gain access via smartphone technology, and it is important that manufactures make sure that the only apps, which connect with the cars internal organs, are certified, and well tested before allowing the connection. As Mazloom et al. [27], also states in their report: Their hope is that, this analysis will help motivate and spur more secure designs and implementations of smartphone to IVI platforms (In-Vehicle Infotainment).

IV. RELATED WORK

In [4] is being discussed different attacks on authenticity, integrity and confidentiality. In this article the focus is more

Attack	Ease of Attack	Detection probability	Threat level	Layer	References	Countermeasures
GPS Spoofing	High	Low	Low	Sensing layer	[14],[15] [16]	[14]
Jamming	High	High	Low	Sensing Layer	[14], [16]	[18],[19]
Injection	Moderate	Low	Moderate	Sensing Layer	[17]	[20]
Remote attacks(Sensor attacks)	High	Moderate	Moderate	Sensing Layer	[16], [17]	[17]
Frame Sniffing	Moderate	Low	Low	Communication Layer	[21]	[23],[24]
Frame Falsifying	Moderate	Low	Moderate	Communication Layer	[21]	[23],[24]
Frame Injection	Moderate	Low	High	Communication Layer	[21]	[23],[24]
Replay Attack	Moderate	Low	High	Communication Layer	[21],[22]	[23],[24]
DoS Attack	High	High	High	Communication Layer	[21]	[23],[24]
Control override attack	Low	High	High	Control Layer	[25]	[25]
Injection attack	Low	Moderate	High	Control Layer	[26]	[26]
In-vehicle network access attack	Low	Moderate	High	Control Layer	[27],[28]	[25],[26]

Table 1. Summary of attacks and countermeasures

made towards understanding attacks in different layers of the car, whereas we add consideration of threat levels and countermeasures.

In [1], the section on machine learning research and security measures gives a good look into how machine learning can give an extra edge of security in self-driving vehicles. The article also provides attacks and countermeasures.

In our work, we created an overview of most attack categories on modern cars, discussed their threat levels and countermeasures. Our results are summarized in Table 1.

V. DISCUSSIONS

All the threats and attacks described above, are all a force to be reckoned with. Table 1 shows the different threat levels, detection and how easy it is to carry out the attack. Some attacks are harmless but could grow into a serious problem over time. The damage that potential attackers could do with the correct knowledge and funds are truly frightening. Without a doubt the future generation of autonomous cars will be safer and better, if manufactures do their homework and does proper testing of all security measures made in the car. one of most crucial parts of the car would be the in-vehicle communication.

The lack of authentication and encryption are truly alarming and the cars of tomorrow, would be in dire need of these two countermeasures. In Table 1, it is important to compare the ease of the attack with the detection probability, since these two can describe how often cars would be attacked by this type of attack. Threat level are measured depending on the danger for the driver of the vehicle. Another crucial part, would be implementing security measures for sensors, radar and LiDAR in order to prevent attackers from attacking the eyes of the fully automatic car. If your car can not see, it

will not function either, so more testing and solutions would have to be found, as attackers will start to abuse the logic of those sensing organs. As the need for remote access to cars grows, in form of apps, information on screen and other things connected to the vital organs of the car. These devices need to be tested and researched for potential breaches and exploits, before enabling them to interact with the car.

Countermeasures presented in this article, are only some of the solutions to the problem, but by combining multiple solutions like described in the section about GPS spoofing, would make it even harder for attackers to figure out new ways of exploiting weaknesses in the design. Most manufactures today, regard their countermeasures to attacks as confidential information, since attackers would be able to use this knowledge to preform new attacks on modern cars.

VI. CONCLUSION

Our work hopefully raises lot of questions about our current state of security in modern and autonomous cars, to find solutions and a better understanding of known attacks. Hopefully manufactures already found suitable solutions to most urgent issues pointed out, but there is a long way to go before cars can become safe from hacking since there are many potential vulnerabilities.

We are working on creating a simulation framework to truly understand how different sensors with data fusion and machine learning can help to detect if one or more sensors are being attacked. Fortunately, the difficulty of attacking more sensors at the same time is much higher than attacking a single, so this is a promising direction. All communication needs be secured by authentication and encryption, in-vehicle and externally, but we also need to establish a concept for modern and autonomous cars which will allow cars to operate

safely also in case V2V and V2X fail to work and correct GPS coordinates are not received, e.g., due to jamming attacks. Jamming can never be avoided, only detected and mitigated. We cannot allow our roads to become blocked by helpless cars due to cyber-attacks or simple jamming attacks.

REFERENCES

- [1] Z. El-Rewini, K. Sadatsharan, D. Flora, S. Siby, J. Plathottam, P. Ranganathan, "Cybersecurity challenges in vehicular communications," *Vehicular Communications*, Volume 23, June 2020.
- [2] J. Liu, W. Sun, Yongpeng Shi, "In-vehicle network attacks and countermeasures: challenges and future directions," *IEEE Netw.*, 31 (2017), pp. 50-58.
- [3] W. Choi, K. Joo, H.J. Jo, M.C. Park, D.H. Lee, "VoltageIDS: low-level communication characteristics for automotive intrusion detection system," *IEEE Trans. Inf. Forensics Secur.*, 13 (2018), pp. 2114-2129.
- [4] A. Chowdhury, G. Karmakar, J. Kamruzzaman, A. Jolfaei and R. Das, "Attacks on Self-Driving Cars and Their Countermeasures: A Survey," *IEEE Access*, vol. 8, pp. 207308-207342, 2020.
- [5] J. Shea Choksey and C. Wardlaw, accessed 17 Aug 2021. <https://www.jdpower.com/cars/shopping-guides/levels-of-autonomous-driving-explained>
- [6] M.A. Talib, S. Abbas, Q. Nasir, M.F. Mowakeh, "Systematic literature review on Internet-of-Vehicles communication security", *International Journal of Distributed Sensor Networks*, SAGE journals, 2018.
- [7] KeenLab, "Experimental Security Assessment of BMW Cars", accessed 17 Aug 2021. https://keenlab.tencent.com/en/whitepapers/Experimental_Security_Assessment_of_BMW_Cars_by_KeenLab.pdf
- [8] KeenLab, "Exploiting Wi-Fi Stack on Tesla Model S", accessed 17 Aug 2021. <https://keenlab.tencent.com/en/2020/01/02/exploiting-wifi-stack-on-tesla-model-s/>
- [9] J. Deng, L. Yu, L. Fu, H. Oluwakemi, R.R. Brooks, "Security and data privacy of modern automobiles", *Data Analytics for Intelligent Transport Systems*, Elsevier Inc., 2017, pp. 131-163.
- [10] J. Petit, S.E. Shladover, "Potential cyberattacks on automated vehicles", *IEEE Trans. Intell. Transp. Syst.* 16 (2015) 546-556.
- [11] O. Henniger, L. Apvrille, A. Fuchs, Y. Roudier, A. Ruddie, B. Weyl, "Security requirements for automotive on-board networks", 9th International Conference on Intelligent Transport Systems Telecommunications, 2009.
- [12] information is beautiful, "Million Lines of code", accessed 17 Aug 2021. <https://informationisbeautiful.net/visualizations/million-lines-of-code/>
- [13] KeenLab, "Experimental Security Research of Tesla Autopilot", accessed 17 Aug 2021. <https://keenlab.tencent.com/en/2019/03/29/Tencent-Keen-Security-Lab-Experimental-Security-Research-of-Tesla-Autopilot/>
- [14] A. Greenberg, "Hackers Remotely Kill a Jeep on the Highway—With Me in It", accessed 17 Aug 2021. <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>
- [15] M.L. Psiaki and T.E. Humphreys, "GNSS spoofing and detection," *Proc. IEEE*, vol.104, no. 6, pp.1258-1270, Jun. 2016.
- [16] Software-Defined GPS Signal Simulator, Github, accessed 18 Jan, 2021. <https://github.com/osqzss/gps-sdr-sim>
- [17] C. Yan et al., "Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicles," *DEFCON24*, 2016.
- [18] J. Petit et al., "Remote attacks on automated vehicles sensors: Experiments on camera and LiDAR," *Proc. of BlackhatEU15*, 2015.
- [19] C. Yang, L. Feng, H. Zhang, S. He and Z. Shi, "A Novel Data Fusion Algorithm to Combat False Data Injection Attacks in Networked Radar Systems," *IEEE Transactions on Signal and Information Processing over Networks*, vol. 4, no. 1, pp. 125-136, March 2018.
- [20] M. Köhler, F. Gumbmann, J. Schür, L. Schmidt and H. Blöcher, "Considerations for future automotive radar in the frequency range above 100 GHz," *German Microwave Conference Digest of Papers*, Berlin, 2010, pp. 284-287.
- [21] X. Mao and D. Inoue, "Demonstration of In-Car Doppler Laser Radar at 1.55 μm for Range and Speed Measurement", *IEEE Transactions on Intelligent Transportation Systems*, 14(2):599-607, 2013.
- [22] K. Koscher et al., "Experimental Security Analysis of a Modern Automobile", *Proc. IEEE Symposium on Security and Privacy*, 2010.
- [23] T. Hoppe and J. Dittmann, "Sniffing/Replay Attacks on CAN Buses: A Simulated Attack on the Electric Window Lift Classified using an Adapted CERT Taxonomy", *Proc. 2nd Workshop on Embedded Systems Security*, 2007.
- [24] S. Woo, H.J. Jo and D.H. Lee, "A Practical Wireless Attack on the Connected Car and Security Protocol for In-Vehicle CAN", *IEEE Trans. Intelligent Transportation Systems*, vol. 16, no. 2, pp. 993-1006, 2015.
- [25] D.K. Nilsson, U.E. Larson and E. Jonsson, "Efficient In-Vehicle Delayed Data Authentication Based on Compound Message Authentication Codes", *Proc. Vehicular Technology Conf.*, 2008.
- [26] H.J. Jo, W. Choi, S.Y. Na, S. Woo, D.H. Lee, "Vulnerabilities of Android OS-based telematics system", *Wirel. Pers. Commun.* 92 (2017), pp. 1512-1530.
- [27] S. Mazloom, M. Rezaeirad, A. Hunter, D. McCoy, "A security analysis of an in vehicle infotainment and app platform", *Proceedings of the 10th USENIX Conference on Offensive Technologies*, 2016, pp. 232-243.
- [28] P. Carsten, M. Yampolskiy, T.R. Andel, J.T. McDonald, "In-vehicle networks: attacks, vulnerabilities, and proposed solutions", *Proceedings of the 10th Annual Cyber and Information Security Research Conference*, 2015.
- [29] C. Valasek, C. Miller, "Adventures in Automotive Networks and Control Units", *Technical Report*, 2014.
- [30] R. Ferreira, J. Gaspar, N. Souto; P. Sebastião, "Effective GPS Jamming Techniques for UAVs Using Low-Cost SDR Platforms", *2018 Global Wireless Summit (GWS)*, IEEE Xplore, 2018.