A Survey of Autonomous Vehicle Technology and Security

Mustafa Saed
HATCI Electronic Systems Development
Superior Township, Michigan, USA
msaed@hatci.com

Kevin Daimi and Samar Bayan
University of Detroit Mercy
Detroit, Michigan, USA
{daimikj, bayansa}@udmercy.edu

Abstract—Fully autonomous vehicle will soon be a reality. This will present a vector of issues and challenges including economic, social, safety, environmental, and security problems. Security will participate in enhancing safety of passengers and pedestrians. With the current non-autonomous vehicles, the work on security is ongoing and mainly in its research status. The sophisticated technology of autonomous vehicle will furnish a path of even more complicated security issues. In this paper, the autonomous vehicle technology and its security will be briefly surveyed to allow researcher the opportunity for further research in this field. In particular, the paper will address the five levels of autonomous vehicle and its current state with regards to these levels, the internal architecture of the vehicle, and security threats facing this vehicle technology.

Keywords—Autonomous Vehicle; Autonomous Vehicle Architecture; Level of Autonomy; Security Attacks; Security Defenses.

I. INTRODUCTION

Vehicles were first invented to facilitate the transportation of people. In 1769, the first stream road engine was invented by Nicolas-Joseph Cugnot [1]. A few years later, vehicles used the internal combustion engines powered by hydrogen and oxygen mixture [2]. Vehicles became gasoline powered in 1885 [3], and the first true electric car was invented in 1888 [4]. Electric cars were popular between the 19th and 20th centuries due to their level of comfort and ease of operation. Since then, vehicles had been improved so much especially with the introduction of artificial intelligence in 1960 [5]. Researchers started to think of ways to overcome the driver's role, so they added autonomy to vehicles. Autonomy allowed vehicles to be categorized from a regular vehicle with no autonomous characteristics to full autonomous vehicle capable of moving by itself. In 2019, level 3 autonomous vehicle, Tesla Model 3, had been introduced to the market [6].

Autonomous vehicles include the classical vehicle characteristics with the additional autonomy flavor. They are expected to collect enormous data from various sources and replace humans in driving. These accumulating data will be huge and will open further research venues for many fields including technological, data science, and security. With full autonomy, humans are no longer needed to control the vehicle's movements. However, autonomy as defined by National Highway Traffic Safety Administration varies depending on the way the control functions are handled by the vehicle. The full autonomous vehicle extracts information from the surrounding environment via various signals, analyzes these signals and executes appropriate path of movement [7]. This implies that in all the phases of this procedure, human will not even play any role in the environmental perception. With these high control functions, the vehicle becomes more dependent on communication networks internally and with exterior environment [8]. This exceedingly reliance on communication networks will unlock the gates for even more sophisticated security attacks. There are two types of communications in autonomous vehicles, Inter-vehicle and intra-vehicle communications [8]. Intra-vehicle communications, represented by buses, are responsible for data transfer between the autonomous vehicle's components. Inter-vehicle communications deals with transferring of data between the vehicle and the external environment including other vehicles, infrastructure and smart road signs. This makes the autonomous vehicle more vulnerable to various security attacks that are classified based on type of the attacker, motivation for the attack, type of the attack, and the target for the attack [9]. Consequently, the attacker will be able to collect information from the autonomous vehicle, modify it, and cause harm for both vehicles, their passengers, and possibly passengers of other vehicles. Thus, innovative and leading-edge security measures will be demanding due to the sophistication of the communication process.

To ensure autonomous vehicle network security and avoid potential attacks, different defenses have been proposed. These security techniques satisfy a collection of requirements pointed out by data integrity, data confidentiality, user and in-vehicle authentication, and availability [10]. For this reason, new cryptographic techniques should be established to enhance the autonomous vehicle's security and ensure that the original data is not altered to make certain vehicle's performance will not deteriorate and the safety for all is granted.

This paper deals with surveying the current and future technology of autonomous vehicle and its security. To this end, the levels of autonomous vehicles are introduced in Section II. Section III presents the architectural technology of autonomous vehicles, and the threats that autonomous vehicles are vulnerable to are explained in Section IV. Autonomous vehicle security is covered in Section V. The paper is then concluded in Section VI.

II. AUTONOMPUS VEHICLE LEVELS

The mission of full autonomous vehicle is to transport passengers to their destination without the need for a human driver. The National Highway Traffic Safety Administration (NHTSA) defines autonomous vehicle as "those in which at least one aspect of safety-critical control function occurs without direct driver input" [11]. This definition reveals that autonomous vehicles are categorized by levels ranging from Level 1 to Level 5 [12] [13]. According to NHTSA, Cruise control, automatic braking, and lane keeping are considered examples of automation systems, or safety-critical control functions. The National Highway Traffic Safety Administration does not consider vehicles equipped with vehicle-to-vehicle services for safety warnings as autonomous vehicle. Level 0 refers to vehicles with no autonomy. The driver in Level 0 autonomous vehicles has full control over all tasks within the vehicle. Both NHTSA and Society of Automotive Engineers (SAE) [11] [14] depicted the levels of autonomy as shown in Figure 1.

The five levels of autonomous vehicle represent the various magnitude of automation that the vehicle is equipped with. The transition from a lower level to a higher level signifies the increase in automation. This style will continue until full automation (Level 5) is reached.

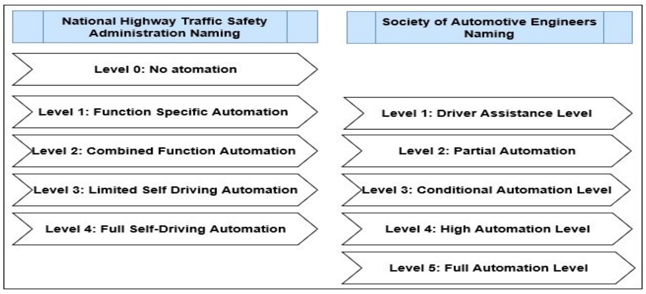
National Highway Traffic Safety Administration Naming
Society of Automotive Engineers Naming
Level 0: No atomation
Level 1: Function Specific Automation
Level 1: Driver Assistance Level
Level 2: Combined Function Automation
Level 2: Partial Automation
Level 3: Limited Self Driving Automation
Level 3: Conditional Automation Level
Level 4: Full Self-Driving Automation
Level 4: High Automation Level
Level 5: Full Automation Level

Figure 1. NHTSA and SAE Autonomous Vehicles Levels

A. Level 1 - Driver Assistant

At this level, the driver is responsible for monitoring the outer environment and taking decisions to control the vehicle's movements. The system shares only one of the control functions with the driver: steering and acceleration speed, or braking control [15]. Human will execute most of the driving tasks [16]. An example of Level 1 autonomous vehicle is Jaguar Land Rover. The vehicle is responsible for off-road cruise control. In an off-road cruise control, the driver is responsible for steering while the system will set the appropriate speed. The maximum speed is predetermined by the driver [17].

B. Level 2 - Partial Automation

The automated system is in charge of two of the primary control functions of driving at this level [11]. It fully controls the steering and acceleration tasks with limited driving conditions [18]. The driver handles the remaining tasks including environmental monitoring. An example of Level 2 autonomous vehicle is Tesla Model S [19]. Tesla introduced a technology that makes the vehicle capable of accelerating, maintaining lane position, and parking without the help of the driver. The driver is only responsible for holding the steering wheel and monitoring the environment [19].

C. Level 3 - Conditional Automation

The automated system is fully responsible for monitoring the environment and performing the safety-critical functions. The automated system will handle driving and monitor the envrionment. The autonomous vehicle anticipates the driver to accomplish backup for the system and resume driving when needed [1]. The difference between Level 2 and Level 3 autonomous vehicles is that at Level 3 the driver may not constantly monitor the environment during driving. The system can share this task with the driver [11].

D. Level 4 - High Automation

The vehicle at this level is fully charged to control driving. The difference between Level 3 and 4 is characterized by the needed interference of the driver in case of failure. This implies that Level 3 system expects the intervention of driver for backup, but Level 4 system works without any expectation from the driver [12]. This level has some limitations determined by maximum speed, and low speed, and adverse weather conditions, such as snow falling [20].

E. Level 5 - Full Automation

Level 5 does not expect the vehicle to have steering wheel and performs all environmental analysis and planning techniques to reach destination by itself [18]. Level 5 vehicles are similar to level 4 but with with no limitations [20]. The vehicle at this level will no longer need steering wheel, pedals or human to control tasks [16]. Google is working on building Level 5 autonomous vehicle through its company Waymo [21]. This level could be referred to as full vehicle automation.

III. Current State of Vehicle Autonomy

Autonomous levels describe the role human plays while driving. However, Level 4 and 5 autonomous vehicles are not implemented yet. This is due to the difficulty of making the system totally reliable on itself without expecting human interference. This means that the vehicle will fully analyse and even take care of any failure case [22]. At the present time, the autonomous vehicle technology lends itself to Level 3 autonomous vehicle. In Table I, autonomous vehicles currently manufactured by auto industry are demonstrated. Moreover, many manufacturers announced that they will have Level 4 autonomous vehicles available in year 2020-2021 including Toyota, Volvo, Renault-Nissan, Hyundai, and Ford [24].

TABLE I. RECENT AUTONOMOUS VEHICLES AND THEIR LEVELS

Manufacturer	**Mobileye [23]**	**Tesla [24]**	**Audi [25]**
Model		Model S	A8
Automation Level	Level 2	Level 2	Level 3

IV. Autonomous Vehicle Threats

Understanding the autonomous vehicle threats stems from understanding the sophisticated autonomous vehicle technology and architecture. The autonomous vehicle needs to analyze data from the surrounding environment. These data are collected from perception sensors, other vehicles and various smart infrastructures [7].

A. Autonomous Vehicle Architecture

When analyzing the security of a system and identifying the associated threats, it is essential to understand the underlying architecture to establish the needed security protocols. The way autonomous vehicle analyses things is similar to people's action-perception technique. The approach consists of perception, planning and control systems [7] [8] [26]. First, the perception system is responsible for sensing the environment and finding out the location of the autonomous vehicle [27]. The location can be represented in three ways; relative location, absolute location, and hybrid location [7]. Relative location is calculated by adding the distance and orientation of the vehicle to the initial position. The global positioning system, GPS, is in charge of providing the absolute vehicle location. Hybrid location is a mixture of both, relative and absolute locations. The goal is to find the real-time efficient location. Autonomous Vehicle uses the hybrid location technique to localize itself [7]. Sensing the environment is represented by lane line identification, obstacle detection, and road signs analysis. This is delivered through cameras, LIDAR, and Radar [8]. The Light Detection and Ranging (LiDAR) supplies high-resolution, three-dimensional information about the vehicle's surrounding environment. Having completed the perception, the Planning System picks up data from perception system, analyzes it and makes the appropriate decision for movement. The input for this subsystem is a combination of the perception system's output data, feedback from the control system, and the Inter-vehicle communication data. Finally, the Control System implements the decision taken by the Planning System through a large number of Electronic Control Units (ECUs). This PPC architecture (perception, planning, and control architecture) is similar to perception, cognition, and action systems of the humans [28]. Details of these systems and their relationships are depicted in Figure 2.

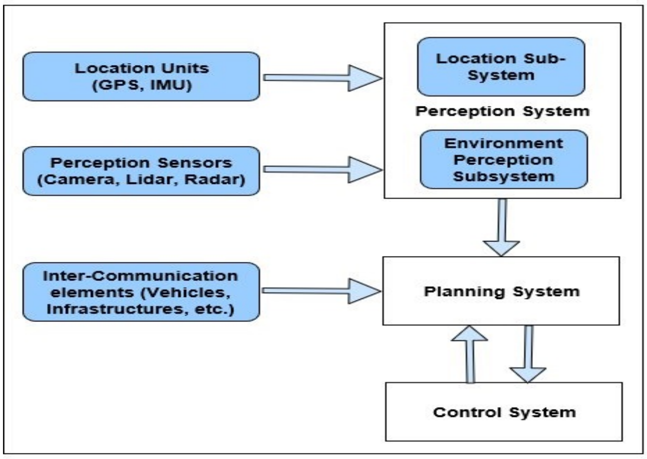
Location Units (GPS, IMU)
Perception Sensors (Camera, Lidar, Radar)
Inter-Communication elements (Vehicles, Infrastructures, etc.)
Location Sub-System
Perception System
Environment Perception Subsystem
Planning System
Control System

Figure 2. Internal Architecture of Autonomous Vehicle

For proper performance, each system needs three components; sensors, processors and communication technologies [29]. The autonomous vehicle, as shown in Figure 2 above, collects data from onboard sensors, such as camera, lidar and radar, and from outer components including vehicles and infrastructure. The communication technologies within these two categories are referred to as intra-vehicle communication and Inter-vehicle communications. Inter-vehicle communication allows vehicle's parts to communicate and exchange information. It employs different buses to achieve this communication, such as Control Area Network (CAN), FlexRay, Local Interconnect Network (LIN), Media Oriented System Transport (MOST), and ethernet [8]. The bus technologies used by two selected Autonomous Vehicles (AVs) are shown in Table II below.

TABLE II. AV INTRA-VEHICLE COMMUNICATIONS BUSES

	Tesla Model S	Audi A8
Level	2	3
Technologies	CAN, LIN, Ethernet [8]	CAN, LIN, FlexRay, MOST [8]

Furthermore, the autonomous vehicles can collect real-time data from everything around it to enhance decisions taken by its planning system. These relations are categorized as vehicle to vehicle (V2V), vehicle to infrastructure (V2I), vehicle to road signs (V2RS), vehicle to internet of things (V2IOT) and vehicle to everything (V2X). Inter-vehicle networks are divided into low power technologies, such as Bluetooth and Zigbee, and IEEE 802.11 family technologies including WiFi and Dedicated Short Range Communication (DSRC), and base station driven technologies, such as Worldwide Interoperability for Microwave Access (WiMAX) and LongTerm Evolution for Vehicle (LTE-V) [8]. As depicted in Figure 3, the most popular networks, LTE-V and DSRC, currently deployed by the autonomous vehicles are demonstrated.

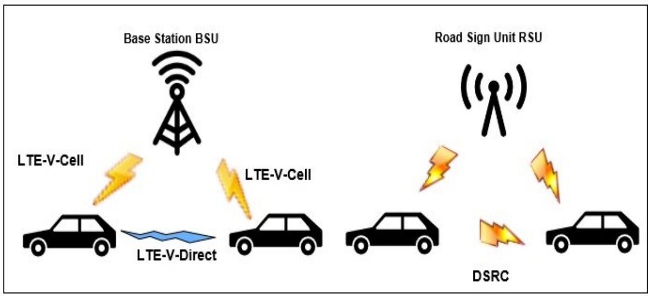

Figure 3. Inter-Vehicle Communications- LTE-V and DSRC

Hence, the autonomous vehicle is vulnerable to security attacks due to increased internal communication (intra-vehicle communications) and Inter-vehicle communications.

B. Autonomous Vehicle Threats

The autonomous vehicles are coupled to different communication techniques. This makes it vulnerable to different types of attacks. For example, the vehicle-to vehicle V2V connectivity in the autonomous vehicles increases the ability of the attacker to join multiple vehicles in a vehicular botnet [30]. The vehicular botnet is a collection of networked vehicles controlled by the attacker [31]. Here multiple bots will join botnet and will execute whatever the attacker instructs them to do to the vehicle network. Various attacks are provided in Section V.

Other types of security attacks include password and key attacks, Denial of Service (DoS), Network protocol attacks, and Rogue Updates attack [32]. The first one is classified into dictionary, rainbow and brute force attacks. The attacker tries multiple attempts by using list of words, precomputed hashes or alpha-numeric combination to crack the password [32]. In other words, the attackers try to discover passwords by using every possible password commonly used and stored in a predefined file or database. In brute force attack, attackers try every possible combination of letters, digits, and other characters to discover the password. Finally, Rainbow attack consumes less time than the other two types by using a large store of precomputed hashes and comparing the stolen hashed password with those in the store.

In autonomous vehicle, DoS attack can be achieved through single node (within a vehicle), V2V communication or V2I communication [33]. A bogus Electronic Control Unit (ECU), which can be any device that succeeds in communicating with the ECUs, can send huge number of messages to other ECUs (single node), and a vehicle or group of vehicles can initiate large number of messages to a vehicle or even the infrastructure (V2V or V2I). Even worse, a bogus infrastructure can bombard vehicle with many messages (I2V). The Dedicated Short-Range Communication (DRC) and Wireless Access in Vehicular Environments (WAVE) are used as communication mediums that enable messages exchanged between vehicles and the entire Vehicle to Infrastructure (V2I) environment. Several types of attacks associated with wireless V2X communication protocols have been demonstrated by security experts that could disrupt the availability and the performance of autonomous vehicles. Potential Attack Scenarios include an attacker jamming the main wireless communication medium so that the network will no longer be available for legitimate users. This would cause a DoS attack that prevents authentic users (autonomous vehicles) from being able to communicate with each other or with the whole infrastructure. Furthermore, an attacker can achieve a DoS attack by generating a high volume of false messages which flood the network impeding the performance of any decision-making processes of the autonomous vehicle. An attacker can compromise the communication network and change the content of a warning message or send fake messages to other vehicles to disrupt the smooth road functionality or cause accidents. For example, an attacker who receives a warning message “Road Constructions Warning” from a nearby vehicle can change the content of the message and send the message “Road is clear” instead. Also, an attacker can compromise the confidentiality of autonomous vehicles’ operations by eavesdropping. An example of this attack could be the collection of location and routing information of specific autonomous vehicles in order to further harm the passengers in these vehicles or even steal the vehicles. Due to the fact that the exchanged messages are encrypted, this attack would require decrypting the exchanged messages to be successful.

The above scenarios lead to great damage to the autonomous vehicle communication system due to the bulk amount of data being sent. In network protocol attack, the attacker analyses the protocols to find out the weak points that can be exploited. Some researchers showed that CAN and FlexRay protocols are most vulnerable to this type of attacks. Rogue Updates attack occurs when the software of Electronic Control Units (ECU) are updated by versions not from the automakers (manufacturer). The Control Area Network (CAN) bus has limited number of bits (64 bits) dedicated to message transmission. This limitation does not allow strong encryption of messages and the authentication of these messages and their senders. Therefore, it is vulnerable to such attacks and other types of attacks as specified below. FlexRay protocol is based on both the Physical and Data Link layers. All the possible attacks on these two layers, including DoS, find their way to the FlexRay protocol. For this protocol, only one node can produce the main signal while other nodes can only create idle signals. DoS will be achieved by continuously sending the main signal.

Modern vehicles have over fifty attack points (over 50 generic attack points that hackers can exploit in order to attack a vehicle) including the in-vehicle systems (CAN, FlexRay, Ethernet communication protocol), the Mobile Network Operations (MNO) and the backend operations. Due to the additional technology that is introduced into autonomous vehicles, the number of attack points is increasing. At the same time, an increasing number of hacking tools, including software and hardware specifically designed to monitor and control the in-vehicle network, systems, and applications, are becoming available. Hacking tools can be used by researchers or hackers that are interested in exploiting the vehicle environment for their own benefits. Most of them are becoming open-source and are available for free. More importantly, the risk of a successful attack to an autonomous vehicle is dramatically increasing, since there is no fallback. Vehicle operations rely on technology and a potential compromise could have fatal consequences.

Attacks that result from increased connectivity of the autonomous vehicle are classified in to Physical Access Attack, Close-Proximity Attacks, and Remote Access Attacks.

Physical access attacks are categorized into Invasive and Noninvasive attacks [9] [34]. This classification is based on whether the attack is through device mounted on the autonomous vehicle or not. Invasive physical attacks are subdivided in turn into Side Channel Attacks, Clock Glitch Attacks, and Power Glitch Attacks [33]. Side Channel Attack occurs when the attacker builds up an alternative path for the data [9]. In Clock Glitch Attack, the signals from instruction sequence of the modules are inspected. The latter then is injected with fault signals resulting from exploiting timing violations [35]. Power Glitch Attack is done through analyzing the power consumptions of the electronic control units [36].

Invasive Physical attack exploits the weak points within the autonomous vehicle. Examples of such points are the Onboard Diagnostic Unit OBD and the media system [32]. All cars made after 1996 are required to have an Onboard Diagnostics Board connection (OBD-II) located within two feet of the steering wheel. All vehicles manufactured after 2008 must share the same OBD-II protocol. The OBD-II’s initial function was to monitor mandated emissions equipment. Today, the port is used to monitor and control multiple functions. Service personnel plug equipment into this port for both diagnostics and ECU programming, typically via Windows-based computers, creating at least two paths for the introduction of malware. First, dealership computers typically connect to the Internet (often required by manufacturers) for daily code/firmware updates. During that process, malware could be downloaded and affect their computers. They in turn could spread the malware when they connect them to a vehicle’s OBD-II port. A second path is accomplished through hacking into the dealership’s wireless network. In addition to dealerships and mechanics, parents can connect an app to the OBD-II port to remotely monitor their children’s driving, and fleet managers use apps to keep track on how their fleet vehicles are being driven. These are further sources of attacks through the OBD-II protocol. Not only hackers intend on introducing malware, but clever thieves can access the port to clone “smart keys” and simply drive away with a stolen car. Attackers exploit these vulnerabilities to have access to the internal communication buses. Both Onboard Diagnostic Unit and the media system are connected to the CAN bus in the autonomous vehicles [9]. These invasive attacks are classified into Code Modification Attacks, Code Injection Attack, Packet Sniffing, and In-vehicle Spoofing [32]. Code modification attacks are characterized by modifying the codes transferred through CAN bus. Code Injection Attack works in a similar way by injecting harmful codes through CAN bus. Packet Sniffing is a passive attack that allows viewing transmitted data between modules for the purpose of collecting information. In-vehicle Spoofing is also a passive attack where in which attacker is masquerading or pretending to be another identity to modify data [9]. These are executed through mounted devices and exploits the internal communications.

Remote Access Attacks are represented by the ability of the attacker to control the vehicle remotely. They evolve as a result the expansion of wireless communications in the autonomous vehicle in addition to the growth of external interfaces including the smart cameras and Lidar. They can be categorized as Malware Injection, Signal Spoofing, and Fault Injection Query Attacks [34]. Signal Spoofing attacks exploit the external communications. These include GPS spoofing in which the attacker broadcasts incorrect GPS data [9]. Malware Injection attacks can be considered as code injection attack through the external wireless communications. Here the data is injected through these connections. These can be successful through exploiting the external communications of the autonomous vehicle.

V. AUTONOMOUS VEHICLE SECURITY

Autonomous Vehicle Security can be ensured by using various strong encryption and authentication algorithms and techniques to minimize the attack surface. Designing security for a system follows a number of steps: determining the objective, assessing the sensitivity, estimating capabilities, and determining the control features [10]. Various security attacks on AV are illustrated in Figure 4. The security requirements for autonomous vehicle are as follows: authentication, data confidentiality, data integrity, authorization, privacy, and traceability (tracking the malicious entities) [10]. These are depicted in Figure 5.

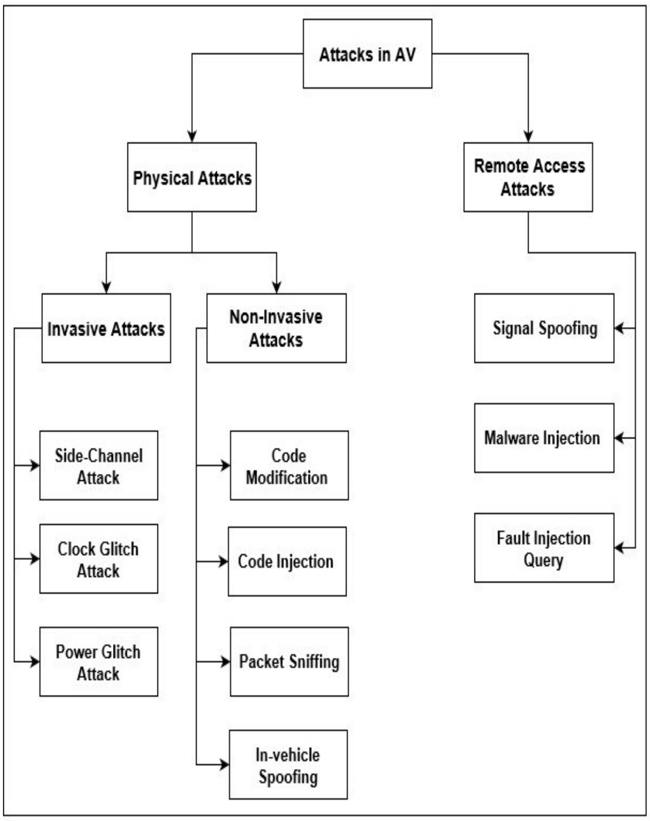

Figure 4. Security Attacks on AV

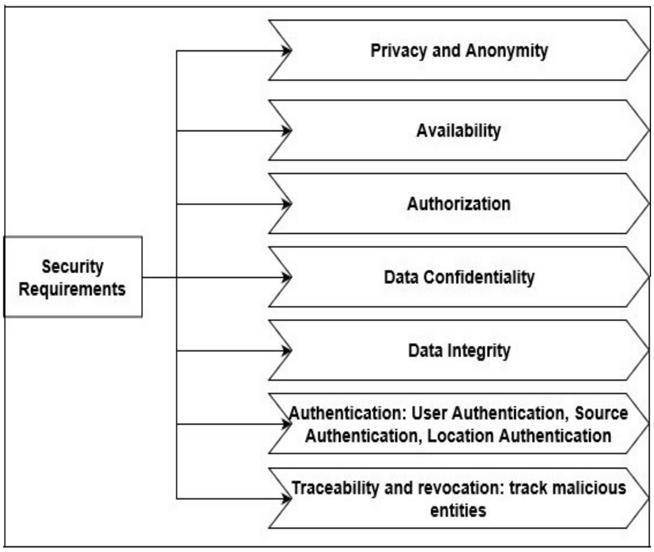
Security Requirements
Privacy and Anonymity
Availability
Authorization
Data Confidentiality
Data Integrity
Authentication: User Authentication, Source Authentication, Location Authentication
Traceability and revocation: track malicious entities

Figure 5. Security Requirements for Data Transfer in AV

Note that all the attacks mentioned in Figure 4 can impact all levels of autonomous vehicle. However, as the degree of automation increases (moving from lower level to higher level), the impact of these attacks becomes more severe.

Autonomous Vehicle (AV) defenses are classified into four categories; Active Defenses, Preventive Defenses, Passive Defenses and Collaborative Defenses [9] [34]. These are clarified in Figure 6. Preventive defense tends to stop the attack when it occurs by increasing the security measures. This type of defense includes authenticating the user and the in-vehicle device, securing the communications, and controlling the network traffic (through firewall). These are implemented to ensure data confidentiality through using symmetric and asymmetric encryption processes and enforcing message integrity through the use of Message Authentication Code (MAC) or hash techniques.

Active defenses can be done by continuously monitoring the security scales of the autonomous vehicle or by applying adaptive security. The latter is characterized by reconfiguring the attack targets and improving tactics to have better control when the attack occurs [9].

The autonomous vehicles can cooperate to empower their cybersecurity. In future autonomous vehicles, Vehicle To Internet of Things, V2IOT, will be introduced within the clouds to reduce communication channels. Hence, this will further enhance the security by making targeting autonomous vehicle harder for attackers [37]. This collaborative defense that occurs in collaboration with cloud services will be part of cloud computing.

Passive defenses are carried out to detect, respond to, and recover from a security attack once it occurs. It can be summarized by finding ways to prevent malwares and code injection and modification techniques. Responding to these attacks to counteracting their impact is exercised using electronic or cyber capability, such as GPS anti-jamming device [38] or isolation. Isolation refers to detaching the autonomous vehicle from Inter-vehicle communication network to avoid harms to others.

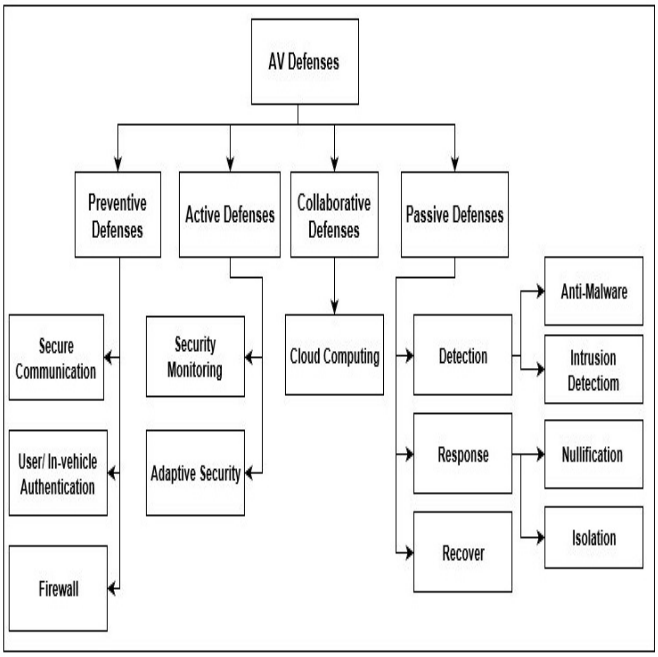

Figure 6. Defenses Types for Various Security Attacks

A number of European projects that are meant to enhance security techniques for the autonomous vehicle are ongoing. These include Secure Vehicle Communications (SEVECOM), Secure Hardware Extension(SHE), and E-safety Vehicle Intrusion Protected Applications (EVITA). SEVECOM works on enhancing the security of communications between autonomous vehicles. SHE aims at enhancing cryptographic processes to increase security [39].

Vehicular Ad-Hoc Networks (VANETs) is technique used for the Inter-vehicle communications. This can be protected against security threats regarding authentication and confidentiality due to the use of the digital signatures and private keys [40]. However, they still augment the possibility of vehicular botnets [31]. For this reason, researchers worked on improving the security for VANETs by verifying and certifying correctness of cryptographic authentication [41], analyzing messages sent by VANETs (in low level autonomous vehicles) [42]-[45], and analyzing trustworthiness of the sender [46].

VI. Conclusion

Vehicles were first introduced to provide transportation only for people. Through time and with the development of technology, vehicles were gaining more interest and are further improved. The goal of this improvement was to increase the security of people and this led to increased intelligence in data analysis within the vehicle itself. For this reason, autonomous vehicles were born. Nowadays, auto industry is capable of delivering level 3 autonomous vehicles. Some automakers are expecting full autonomous vehicle to be presented after couple years. Due to the increase usage of the communication networks within the autonomous vehicle, the vehicle is becoming more vulnerable to various security attack types. These attacks will have severe negative impact on the networks within the vehicle and could lead to disastrous incidents if attackers gain control over the autonomous vehicle. To overcome these attacks different defenses are combined with cybersecurity techniques. The purpose of these defenses is to ensure integrity, authenticity, and confidentiality of data transmitted within the autonomous vehicles. In particular, to prevent these attacks or at least minimize their impact, strong encryption and authentication need to be implemented. Intrusion Detection Systems (IDSs), and honeypots or honeynets should be considered. In parallel with these approaches, more smart sensors have to be introduced to replace the classical sensors. This will allow for cryptographic capabilities within these sensors as computing capabilities will be included.

References

[1] E. Eckermann, “World History of the Automobile,” SAE Press, pp. 14-14, 2001.

[2] H. Michelet, “L'inventeur Isaac de Rivaz,” pp. 1752 - 1828 Editions Saint-Augustin, (in French), https://books.google.com/books?id=Wf-nrnUaZxAC&pg=PA26&dq=François+Isaac+de+Rivaz#v=onepage&q=François%20Isaac%20de%20Rivaz&f=false [Retrieved: May, 2018].

[3] "DRP patent No. 37435," Archived from the original (PDF) on 4 February 2012, https://web.archive.org/web/20120204045616/http:/home.arcor.de/carsten.popp/DE_00037435_A.pdf, [Retrieved: May 2019].

[4] I. S. Jacobs and C. P. Bean, “Fine Particles, Thin Films and Exchange Anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, pp. 271–350, 1963.

[5] “Where to? A History of Autonomous Vehicle,” 2014, https://www.computerhistory.org/atchm/where-to-a-history-of-autonomous-vehicles/, [Retrieved, May 2019].

[6] M. Kane, "US Plug-In Electric Car Sales Charted,” January 2019". http://InsideEVs.com, [Retrieved: May, 2019].

[7] J. Zhao and Q. C. B. Liang, "The Key Technology Toward the Self Driving Car," International Journal of Intellegent Unmanned Systems, vol. 6, pp. 2-20, 2018.

[8] J. Wang, J. Liu, and N. Kato, "Networking and Communications in Autonomous Driving, A Survey," in IEEE Communication Surveys and Tuorials, 2018.

[9] V. L. L. Thing and J. Wu, "Autonomous Vehicle Security: A Taxonomy of Attacks and Defences," in Proc. the IEEE International Conference on Internet of Things (iThings), IEEE Green Computing and Communications (GreenCom), IEEE Cyber, Physical and Social Computing (CPSCom), IEEE SmartData (SmartData), Chengdu, China pp. 164-170, 2016.

[10] E. B. Hamida, H. Noura, and W. Znaidi, “ Security of Cooperative Intelligent Transport Systems: Standards, Threats, Analysis and Cryptographic Countermeasures,” Electronics, vol. 4, pp. 380-423, 2015.

[11] National Highway Traffic Safety Administration, “Preliminary Statement of Policy Concerning Autonomous Vehicle,” https://www.nhtsa.gov/.../rulemaking/pdf/Automated_Vehicles_Policy.pdf , [Retrieved: May, 2019.

[12] K. Hyatt and C. Paukert “Self Driving Cars: A Level-By-Level Explainer of Autonomous Vehicle,” https://www.cnet.com/roadshow/news/self-driving-car-guide-autonomous-explanation/, [Retrieved: May, 2019].

[13] J. Short and D. Murray,” Identifying Autonomous Vehicle Technology Impacts on the Trucking Industry,” November 2016. http://atri-online.org/wp-content/uploads/2016/11/ATRI-Autonomous-Vehicle-Impacts-11-2016.pdf, [Retrieved: May, 2019].

[14] SAE International, “Automated Driving, Levels of Driving Automation are Defined in New SAE International Standard J3016,” 2014, http://www.sae.org/misc/pdfs/automated_driving.pdf, [Retrieved: May, 2019].

[15] I. Harner, “The 5 Autonomous Driving Levels Explained,” https://www.iotforall.com/5-autonomous-driving-levels-explained/, October 2017, [Retrieved: May, 2019].

[16] M. Burgess, “ When Does A Car Become Truly Autonomous? Levels of Self-Driving Technology Explained,” 2017, https://www.wired.co.uk/article/autonomous-car-levels-sae-ranking, [Retrieved: May, 2019].

[17] M. Burgess, " We Went Off-Road In Jaguar Land Rover's Autonomous Car," 2016, https://www.wired.co.uk/article/self-driving-autonomous-land-rover-jaguar-technology, [Retrieved: May, 2019].

[18] S. Lin, Y. Zhang, C. Hsu, M. Skach, E. Haque, L. Tang, J. Mars, " The Architectural Implications of Autonomous Driving: Constraints and Acceleration," in Proc. the Twenty-Third International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS'18), Williamsburg, VA, USA, 2018, pp. 751-766.

[19] J. Stewart, "Tesla's Cars have driven 140M Miles on Autopilot. Here's How," https://www.wired.com/2016/08/how-tesla-autopilot-works/, [Retreived: May, 2019].

[20] Paul Godsmark, "The Definitive Guide to the Levels Of Automation for Driveless Cars," 2017. https://driverless.wonderhowto.com/news/definitive-guide-levels-automation-for-driverless-cars-0176009/, [Retrieved, May, 2017].

[21] M. Burgess, " Google has spun its self-driving car team out into a new company", December 2016, https://www.wired.co.uk/article/waymo-google-car-driving, [Retrieved: May, 2019].

[22] D. Fagella, "Self-driving Car Timeline for 11 Top Automakers," 2017, https://venturebeat.com/2017/06/04/self-driving-car-timeline-for-11-top-automakers/, [Retrieved: May 2019].

[23] Mobileye, "Mobileye C2-270 Essentials," 2017, http://prevenireaccidente.ro/brosuri/Mobileye%20C2-270%20Essentials%20Book%20-%20to%20print.pdf, [Retrieved: May, 2019].

[24] F. Lambert, "Tesla has a New Autopilot '2.5' Hardware Suite with More Computing Power for Autonomous Driving," https://electrek.co/2017/08/09/tesla-autopilot-2-5-hardware-computer-autonomous-driving/, [Retrieved: May, 2019].

[25] V. Nguyen,"2019 Audi A8 Level 3 Autonomy First-Drive: Chasing the Perfect 'Jam'," https://www.slashgear.com/2019-audi-a8-level-3-autonomy-first-drive-chasing-the-perfect-jam-11499082/, [Retrieved: May 2019].

[26] M. Mody, J. Jones, K. Chitnis, R. Sagar, G. Shurtz, Y. Dutt, M. Koul, M. G. Biju, and A. Dubey, "Understanding Vehicle E/E Architecture Topolgies for Automated Driving: System Partitioning and Tradeoff Parameters," in Proc. the Autonomous Vehicles and Machine Symposium, 2018, pp. 358(1)-358(5).

[27] J. R. Van Brummelen, M. O'Brien, D. Gruyer, and H. Najjaran, "Autonomoous Vehicle Perception System: The Technology of Today and Tomorrow", Trasportation Research Part C, vol. 89, pp. 384-406, 2018.

[28] R. Blake and M. Shiffrar, "Perception of Human Motion," Annual Review of Psychology, vol. 58, pp. 47-73, 2007.

[29] A. M. Wyglinski, X. Huang, T. Padir, L. Lai, T. R. Elsenbarth, and K. Venkatasbramanian, "Security of Autonomous Systems Employing Embedded Computing and Sensors," IEEE Micro, vol. 33, no. 1, pp. 80-86, 2013.

[30] M. T. Garip, M. E. Gursey, P. Reiher, and M. Gerla, "Congestion Attacks to Autoonomous Cars Using Vehicular Botnets," in Proc. the NDSS Workshop on Security of Emerging Network Technology (SENT'15), San Diego, CA, USA, 2015.

[31] M. T. Garip, P. Reiher, and M. Gerla, "Ghost: Concelaing Vehicular Botnet Communication in the VANET Control Channel," in Proc. the International Wireless Communications and Mobile Computing Conference (IWCMC), Paphos, Cyprus, 2016, pp. 1-6.

[32] S. Parkinson, P. Ward, K. Wilson, and J. Miller, "Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges," IEEE Transactions on Intelligent Transportation systems, vol. 18, no. 11, pp. 2898-2915, 2017.

[33] H. Hasbullah, I. A. Soomro, and J. B. A. Manan, "Denial of Service (DoS) Attack and its Possible Solution in VANET," International Journal of Electronics and Communication Engineering, vol. 4, no. 5, pp. 813-817, 2010.

[34] A. M. Jones, "Secure Isolation for Autonomous Vehicle Architecture," Future System Design, 2017, https://www.technologyscotland.scot/wp-content/uploads/2018/11/Secure-Isolation-for-Autonomous-Vehicle-Architectures.pdf, [Retrieved: May, 2019].

[35] L. Zussa, A. Dehbaoui, K. Tobich, J.M. Dutertre, P. Maurine, L. Guillaume-Sage, J. Clediere, and A. Tria, "Efficiency of a Glitch Detector against Electromagnetic Fault Injection," https://www.date-conference.com/files/proceedings/2014/pdffiles/08.3_1.pdf, [Retrieved: May, 2019].

[36] P. Luo, C. Luo, and Y. Fei, "System Clock and Power Supply Cross-Checking for Gitch Detection," https://eprint.iacr.org/2016/968.pdf, [Retrieved: May, 2019].

[37] A. Chattopadhyay and K. Y. Lam, "Autonomous Vehicle: Security by Design," ArXiv, 2018.

[38] Y. Cui and S. S. Ge, " Autonomous Vehicle Positioning with GPS in Urban Canyon Environments," IEEE Transaction on Robotics and Automation, vol. 19, no. 1, pp. 15-25, 2003.

[39] L. W. Li, L. Apvrille, and A. Bracquemond, "Design and Verification of Secure Autonomous Vehicles," in Proc. the 12th ITS European Congress, Strasbourg, France, 2017.

[40] A. Matar, M. Ashraf, and S. Nouh, "VANETS and Autonomous Driving," 2014, https://www.academia.edu/10109589/VANETS_and_Autonomous_Driving, [Retrieved: May 2019].

[41] J. Hubaux, S. Capkun, and J. Luo, "The Security and Privacy of Smart Vehicles", IEEE Security and Privacy, vol. 2, no. 3, pp. 49-55, 2004.

[42] M. El Zarki, S. Mehrotra, G. Tsudik, and N. Venkatasubramanian, "Security Issues in a Future Vehicular Network," European Wireless, vol. 2, 2002.

[43] P. Golle, D. Greene, and J. Staddon, "Detecting and Correcting Malicious Data in VANETs," in Proc. the 1st ACM International Workshop on Vehicular Ad Hoc Networks, pp. 29-37, New York, NY, USA, 2004, pp. 29-37.

[44] T. H. J. Kim, A. Studer, R. Dubey, X. Zhang, A. Perrig, F. Bai, B. Bellar, and A. Lyer, "Vanet Alert Endorsement Using Multi-Source Filters," in Proc. the 7th ACM International Workshop on Vehicular Internetworking (VANET'10), Chicago, Illinois, USA, 2010, pp. 51-60.

[45] T. Leinmuller, E. Schoch, and F. Kargl, "Position Verification Approaches for Vehicular Ad Hoc Networks", IEEE Wireless Communications, vol. 13, no. 5, pp. 16-21, 2006.

[46] F. Dotzer, L. Fischer, and P. Magiera, "Vars: A Vehicle Ad-Hoc Network Reputation System", in Proc. the Sixth IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, Taormina-Giardini Naxos, Italy, 2005, pp. 454-456.