An Analysis of Autonomous Vehicle (AV) Security Attacks and Effective Countermeasures

By
Siddhartha Edara, Will Beal, Nick Colloton, and Hashim Aljarrash (Team Grade)
Computer Engineering and Mechanical Engineering Departments
College of Engineering
University of Wisconsin-Madison

To
Aaron Hiltner
Interegr 397, Section 001
December 10th, 2020

Executive Summary:

Autonomous Vehicles (AVs) were designed to reduce the number of errors committed by human drivers, yet these vehicles themselves are vulnerable to many security threats. This was proven by a group of researchers in India in 2019 when they showed how easy it is to control everything from deploying airbags on command to controlling the steering, acceleration, and brakes of an AV [1]. Today, AVs are designed based on industry standards. These standards don't address potential vulnerabilities and thus most AVs lack basic security measures. These vulnerabilities include manipulating the data external sensors perceive, inserting malicious code into an AVs communication system, and rerouting external signals such as GPS and Wi-Fi [2]. Thus, if the future happens to rely on such systems one must ensure that these systems have established safety standards to avoid future disasters.

Sensors found on AVs are placed around the vehicle to determine the outside environment, as well as to measure the speed, acceleration, and position of the vehicle. These sensors then send this information to electronic control units (ECUs) that interpret and act upon these signals from the sensors [3]. The ECUs cannot operate independently and are therefore connected to a controller area network (CAN) bus. The CAN bus allows the ECUs to communicate with each other and creates a network of controllers to operate the vehicle in harmony [3]. Any of these points could be vulnerable to a security breach and compromise the safety of the vehicle.

In this report, we identified that an AV's components are vulnerable to attacks with varying levels of feasibility. An AV's external sensors are vulnerable to jamming, spoofing, acoustic quieting, and OBD-port code injection attacks. Jamming is a relatively simple, low-cost attack that requires minimal knowledge of the AV's design specifics. Spoofing is another low-cost method of attack; however, it is difficult to conduct and requires further knowledge of the AV's component specifications. We also found that the ECU and CAN modules are vulnerable to low-cost, relatively simple attacks that use the vehicle's On-Board Diagnostic (OBD) port for code injections. And we found that AVs are susceptible to cyberattacks similar to traditional attacks faced by any device connected to the internet.

Finally, we recommend that the National Highway Traffic Safety Administration (NHTSA) develop standards for the security requirements in autonomous vehicles. These standards should address all of the possible attack points within the AV system and use holistic defense measures, including component redundancies and firewalls, to prevent potential security threats. Car

companies will then be required to have their autonomous vehicles comply with the standards set forth by the NHTSA before they are able to be sold in the U.S. These standards can significantly impact the automotive industry by ensuring proper measures for current and prospective AV developers. These standards can also impact consumers by raising public confidence in AV safety and preventing future attacks or accidents that could put lives at risk.

Table of Contents

Section 1: Introduction

According to a report by the National Highway Traffic Safety Administration, 94% of accidents are attributed to driver error [4]. These accidents also contribute to traffic congestions and overall delays in transportation [5]. Autonomous Vehicles (AVs) were designed to fix these issues. Yet, these AVs are at risk to many security threats such as sensor jamming and spoofing, malicious code injections within the AVs communication bus, and also rerouting of GPS and Wi-Fi signals. Given the sensitivity of an AV's functional components, and the nature of its operating conditions such as high speed highway driving, unpredictable behavior could lead to imminent and life threatening dangers such as accidents.

Current autonomous vehicles are designed based on regulatory standards for how the different aspects of the autonomous system will communicate with each other. While these standards do suggest mitigations to potentially vulnerable systems [6], they lack enforcement from government policies in the US due to AVs being an emerging technology [7]. These vulnerabilities include manipulating the data external sensors perceive, inserting malicious code into an AVs communication system, and rerouting external signals such as GPS and Wi-Fi [3]. There has been significant research conducted to try and understand the risk level involved in hacking these systems and how difficult it would be to do so.

A group of researchers in India in 2019 discovered just how easy it is to hack an autonomous vehicle using equipment costing less than 30 USD in order to gain access to the central controls of the vehicle [1]. They also provided measures to validate the security of the cars systems to prevent malicious hacking, saying that having validation or standards for security can prevent "millions" of people from becoming victims to these attacks. The goal of this report is to assess the research done by this group, and the many others that have analyzed the current automated vehicle technology. We first analyzed how each component in the autonomous vehicle system works, communicates, and how vulnerable it could be. We then assessed the ways in which the system could be attacked by a hacker and what the consequences of the attack could be. Finally

we assess what defensive measures can be taken to ensure that the system stays secure and keeps passengers and pedestrians safe.

After taking into consideration all of the vulnerabilities that have been discovered, their potential threat level and ease of hacking, we concluded that regulatory bodies should mandate the use of well-established security countermeasures such as hardware redundancy and the bolstering of software security protocols. In addition, coherent strategies and regulations for overall defensive design should be further developed to ensure widespread security of the AV network, as opposed to disjointed Threat Analysis and Risk Assessment (TARA) methodologies that differ by organization. With the growing number of connected vehicles and infrastructure systems, steps need to be taken to ensure industry-wide compliance with security requirements.

Section 2: Autonomous Vehicle Overview

Today, AVs are categorized within six levels from Level 0, inferring no automation, to Level 5, inferring fully autonomous behavior [8]. Note, this report focuses its analysis on strictly Level 5 AVs. These AVs differ from conventional vehicles in that they use multiple onboard sensors, a central computing system that determines control, and network systems for Vehicle-to-Everything (V2X) communications [5]. On-board sensors, such as cameras, LiDAR, and proximity sensors, surround an AV and are used to determine an AV's current status and environment [5]. This information is used by the internal computing software to control various components of the vehicle known as Electronic Control Units (ECUs) [5]. These ECUs are modules that perform a specific function within the AV such as determining proximity to other vehicles, controlling steering, brake, acceleration, and detecting nearby objects such as traffic signals and stop signs [3]. Examples of ECUs in AVs include the Engine Control Module, Emergency Brake Control Module, Transmission Control Module, and the Radio and Remote-Control Module among others [3]. These ECUs, among other software and hardware components, communicate with one another through an internal Controller Area Network (CAN) bus [3]. This bus acts as a “central network” where different ECUs can communicate messages with each other [3].

Within the AV industry, the CAN bus is designed based upon accepted standards, with one such standard being ISO 11898 [9]. This standard overviews how data packets should be structured to be sent within the CAN bus [9]. Apart from these internal systems, an AV also has an On-Board Diagnostic (OBD) port that allows an external user, such as the vehicle owner, to access and analyze conditions within the AV [3]. Since the OBD port relays data sent via the CAN bus, a user could debug issues within the vehicle through this port. These additions allow AVs to

control a vehicle without human supervision but can also be easily manipulated from intruding sources. These intrusions are either in the form of physical or remote attacks.

Section 2.1: Autonomous Vehicle Categorical Attack Overview

Physical attacks can be further broken down into invasive and non-invasive attacks [3]. Invasive attacks are attacks that require an attacker to physically alter internal AV components typically through code-injections using the OBD port, whereas non-invasive attacks only require an attacker to be within close proximity of the AV under attack [3]. In an invasive attack, an attacker attempts to gain control of the vehicle through the OBD port of the AV. Through this port, an attacker could inject code or data that could modify components, such as ECUs, or trigger failures within the AV [3]. In addition, an attacker could install software that tracks and remotely relays data within the AV back to the attacker leading to privacy issues for AV owners [3]. The main reason for these OBD related attacks is due to low security present in the CAN bus. With minimal security, users can hook low costing devices via the OBD port to infiltrate malicious messages throughout the CAN bus. Researchers, Javier Vazquez-Vidal and Alberto Garcia Illera designed such a low costing device, known as CAN Hack, that is used primarily for code injections [1].

On the other hand, non-invasive attacks don't require an attacker to have physical access to the vehicle or its OBD port [3]. Instead, an attacker focuses on reading data being transmitted to/ from an AV through wireless mediums [3]. These attacks require the use of external hardware devices such as programmable chips like Arduinos [1]. An attacker, within close proximity of an AV, could use said devices for "capturing and analyzing timing information, power consumption, electromagnetic leaks, acoustic signal analysis, and data remanence" [3]. Physical attacks require the attacker to have access or be within proximity of an AV, thus making it hard for hackers to perform attacks against a large fleet of vehicles.

In contrast, remote attacks target vulnerabilities in the AVs external sensors and/or network systems and can be performed without proximity to a single AV. For external sensors, attacks primarily fall under being spoofing, jamming, or acoustic quieting of the sensors [10]. Jamming occurs when an attacker constantly blasts a sensor with a high amplitude signal. This causes the sensor to be unusable as it will be unable to perceive anything outside of this signal [10]. Spoofing attacks are more difficult to produce. Here, an attacker is trying to replicate an object in an AVs path by correctly timing "pulses" of noise [10]. This could cause the AV to act upon an object that doesn't exist. By contrast, Acoustic Quieting occurs when an attacker quiets a sensor's signal by either absorbing the signal using special materials such as fur coats or plastic foams or

by sending out a counter signal that can cancel out that sensor's signal [10]. For example, in the case of a proximity sensor, an attacker could either mask an object in a signal absorbing material or send out signals that counter the reply message back to the sensor for it to detect the obstructing object. Attacks on network systems in an AV follow the above-mentioned tactics but target GPS and Wi-Fi systems. Here an attacker can confuse the AV by providing incorrect GPS or other communication data [3]. For example, GPS spoofing involves an attacker broadcasting a fake GPS signal with the hope that the AV receives the information only from the fake signal [3]. These types of attacks are more dangerous as they can affect multiple AVs at a single time.

The primary reason these attacks are prevalent in the current AV design industry is due to how supply chains work [2]. An internal technology, such as a chip, produced by a manufacturer higher up in the chain may be unknowingly vulnerable and will thus prevail as a design flaw throughout the AV's design [2]. The reason for these unknown vulnerabilities is primarily due to the massive code bases required for implementing each unit. According to Parkinson et al., an AV "can have around 100 million lines of code across 50-70 ECUs" [2]. With such a large codebase it becomes impossible "to perform careful code reviews," especially when one considers how most manufacturers outsource much of the development of these AV design elements on strict guidelines [2]. These guidelines limit a contractor from adding security measures beyond what is listed in the contract [2]. Also, AVs are still an emerging technology and are not restricted by government policies; thus, security flaws are left open for white-hat hackers and academia to research [2]. According to a report from The *Journal of the American Planning Association*, most cities have not discussed policies against AVs but plan to do so once the technology reaches a specific point [7]. Most, if not all, cases that involve attacking an AV have been conducted in a research setting and have had limited damage [2]. Currently, AVs on the road are at Level 2 and require human intervention as they are not fully autonomous [11].

Section 2.2: Autonomous Vehicle Components

Before delving into a detailed analysis of the aforementioned attacks, we present an overview of the major components utilized in AV design that we will touch on throughout this report. These include:

a) External sensors such as ultrasonic sensors, inertial measurement units, LiDAR, and cameras
b) Internal components such as ECU and CAN
c) Communication systems such as GPS, Bluetooth, and Wi-Fi

Figure 1 showcases external sensors, internal ECU components, and the communication systems used by an AV in accordance with its surroundings.

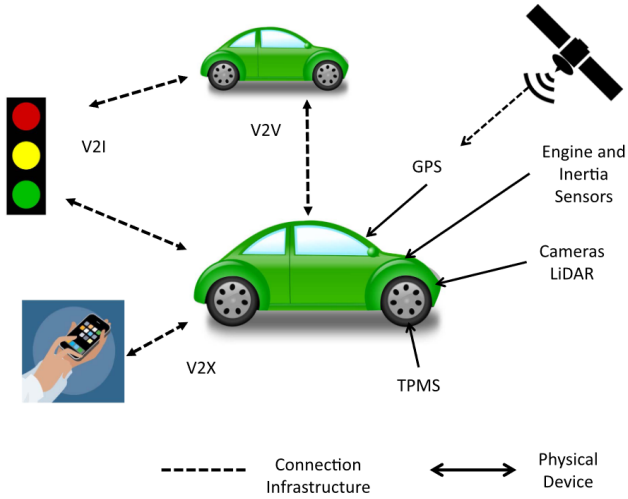

Figure 1. AV Components Communicating with Surroundings. AVs are built on a variety of external and internal components. These include external sensors for understanding the immediate surroundings, internal components for controlling the AV, and wireless systems for communication with other vehicles or users. Source from [2].

Autonomous vehicles map their environment by using low-level sensors such as Ultrasonic Sensors, Inertial measurement units (IMU), Light Detection and Ranging (LiDAR) sensors, and Cameras. Ultrasonic sensors can determine how far or close an object in close-proximity is from the AV and are used primarily in assistive parking technologies [10]. These sensors measure distance by emitting short pulses of ultrasonic waves within their operating frequency and then measuring how long each pulse takes to return to the sensor [10]. Inertial measurement units monitor vehicle dynamics and adjust vehicle behavior by utilizing sensors such as inclination sensors, accelerometers, and gyroscopes. These sensors provide the vehicle with velocity, acceleration, and orientation data. LiDAR sensors map the vehicle environment to navigate and plan trajectories and detect objects to avoid obstacles. LiDAR sensors map the distance between the vehicle and objects by measuring the time a pulse of light takes to reach an object. Autonomous vehicles also use Cameras and infrared systems to recognize objects such as road signs, detect obstacles in both static and dynamic methods, and lane detection. Camera systems can be either mono-vision or stereo-vision depending on the number of cameras. Mono-vision systems require support from other sensors to provide accurate data to determine aspects such as depth. Stereo-vision systems determine depth by using the overlapping regions of multiple cameras [2].

Autonomous vehicles also use 50-70 engine control units (ECU) to control vehicle functionality by acquiring, processing and controlling electrical signals delivered from and to sensors and devices. ECUs control powertrain components such as electric motors and charging systems, safety components such as active braking collision avoidance systems, body components such as mirrors, windows, and vehicle immobilizing. ECUs also control component data communication and wireless communication such as Bluetooth. These ECUs are connected by communication protocols such as the Controller Area Network (CAN) bus. A CAN bus is a serial communication protocol that provides distributed real-time control in an efficient manner [2].

Differential Global Positioning Systems (GPS) sensors utilize GPS infrastructure that uses satellites to provide the vehicle's navigation control module (NCM) ECU with data that determine the vehicle's absolute position that is accurate to one meter. AVs also contain Bluetooth and Wi-Fi modules for connectivity to media and devices such as smartphones, the CAN bus, and other connected Internet Protocol enabled microprocessor chips that can communicate and pass-on sensor data to receivers [2].

Section 3: Attack Measures and Analysis

In this section we present our research findings and analysis on attacks per component of an AV. We primarily utilized an article from Yan et al. who rigorously tested multiple external sensors in a controlled environment [10] and an article from *IEEE Transactions on Intelligent Transportation Systems* that details multiple forms of attack in an extensive literature review of nearly 100 sources [2]. We based our analysis on the following criteria:

Table 1. Description of our attack analysis criteria used when analyzing attack feasibility and potential consequences.

Analysis Criteria	Description
Required hardware costs for conducting the attack	● Low costing attacks that require minimal hardware equipment that can be found readily available such as Raspberry PIs and Arduinos ● High costing attacks that require less readily available equipment such as specialized lab equipment

Proximity of an attacker to the AV(s) under attack	● Physical access attacks that require an attacker to physically alter the AV prior to performing an attack ● Close-proximity attacks that require an attacker to be close to the AV under attack ● Remote attacks that have no limit on the number of AVs under attack and can be performed at any location
Amount of required prior knowledge	● Minimal prior knowledge, which implies an attacker can perform an attack without understanding minute details of a particular component under attack ● Non-minimal prior knowledge, which implies an attacker has a detailed understanding of the component under attack
Ease of conducting the attack	● A simple attack that can be performed in a short amount of time with minimal failure ● A difficult attack that implies the attack requires extreme precision and failure of conducting the attack is more likely
Potential danger from the attack	● Life-threatening attacks which put the user under attack in imminent danger ● Non-life-threatening attacks which pose no threat to the user but may limit functionality within the AV

For your convenience we have provided a table detailing the above criteria per attack at the end of this section.

We break our analysis in multiple sections targeting attacks on different domains of an AV. We begin with an analysis on external sensor attacks including ultrasonic sensors, inertial measurement sensors, LiDAR, and cameras. Next, we analyze attacks on internal components targeting ECUs and the CAN bus. Finally, we provide an analysis of wireless attacks that can be performed on AVs.

Section 3.1: External Sensor Attack Analysis

Sensors surrounding an AV provide sensory information for the AV to understand its surroundings. Attacks made on these sensors compromise the system as a whole and can prove

vital to users utilizing the AV(s). This section provides an analysis of attacks on ultrasonic sensors, IMUs, LiDARs, and cameras.

Section 3.1.1: Ultrasonic Sensors

Ultrasonic sensors are susceptible to jamming, spoofing, and acoustic quieting attacks. Any one of these attacks can cause a vehicle to abruptly stop or continue moving into an obstacle, making these attacks life-threatening. On the bright side, these attacks require close proximity to an AV making it hard for an attacker to impact fleets of AVs. Also, providing countermeasures for simple attacks, such as jamming, has already been extensively researched and can be seen implemented in the Tesla Model S [10].

Jamming attacks are extremely simple to perform and require minimal hardware equipment. Research done by Yan et al. showcased this ease by successfully jamming multiple different ultrasonic sensors with only an Arduino Uno board that constantly outputted a high amplitude signal in the range of the sensor at play [10]. This same research also showcased the difficulty in spoofing, as it took Yan et al. multiple trials until an accurate spoofing attack could be done [10]. Making spoofing attacks viable would require an attacker to have a deeper understanding of nuances within the ultrasonic sensor used in the AV under attacks. These nuances include an understanding of the internal technology used for the sensor, the timing of the pulses sent from the sensor, etc. Thus, while spoofing is a low-cost attack, it isn't easy to execute and requires a deeper understanding of the sensors used in the AV under attack. In contrast to the previous two, acoustic quieting is a much more difficult attack to execute. While an attacker could utilize "sound absorbing materials," such as plastic foam, to absorb ultrasonic signals, these materials aren't discreet [10]. Instead, attackers would likely utilize Active Noise Cancelling (ANC) technology to cancel out the AVs signals from the ultrasonic sensor. This works similarly to noise cancellation software and according to Yan et al. is feasible but requires specialized hardware equipment [10].

Section 3.1.2: Inertial Measurement Units

IMUs provide an AV with control information related to speed and acceleration. Attacks on these sensors can be life-threatening as an attacker would manipulate the AV into a high-speed scenario. These attacks are similar to spoofing attacks as an attacker will need extensive knowledge of the minute tolerances of the sensor before performing the attack [2]. Also, an attacker will need physical access to the vehicle's OBD port making it harder to perform these attacks on a fleet of AVs. Once access to the OBD port is retrieved an attacker can utilize low

costing hardware and software such as CarShark for modifying CAN packets sent via the CAN bus to alter the AVs speed and acceleration [2]. Parkinson et al. also note that these types of attacks haven't been extensively researched, thus additional attack possibilities may exist [2].

Section 3.1.3: LiDAR

LiDARs provide an AV with vital sensory information including a mapping of potential obstacles on an AVs path. These sensors are susceptible to jamming and spoofing attacks with minimal costing hardware. With equipment such as a Raspberry PI and a low-powered laser, an attacker can jam or spoof the LiDAR sensor by emitting pulses of the laser towards the sensor [2]. Attacks of this type put the user in immediate danger and can cause a vehicle to abruptly stop, making it dangerous in high-traffic scenarios. Similar to other sensors, jamming attacks are extremely easy to implement and don't require any prior knowledge whereas spoofing attacks are more difficult and require an attacker to understand the pulse interval required to spoof the sensor [2]. Regardless, both attacks require an attacker to be within close-proximity of the AV, minimizing the threat of these attacks being large scale [2].

Section 3.1.4: Camera

Cameras are typically used in scenarios where visual sensory is required. These sensors are extremely sensitive to jamming attacks that blind the camera, proving to be life-threatening for a user. This was seen in the tragic Tesla case where the AV's camera was unable to distinguish the sky from a white trailer on an extremely sunny day [2]. While the previous case isn't an attack on an AV, it showcases the sensitivity of the camera utilized in AV design. An attacker could replicate such a scenario utilizing the high-beams on a car, making these attacks low costing and easy to implement. In addition, minimal knowledge is required and these attacks would require an attacker to be in close-proximity to the AV [2].

Section 3.2: Internal AV Components Attack Analysis

The ECU and CAN bus of an AV are the most vital in its design as they control everything from control, navigation, and even media. Attacks on these components are the most dangerous and put the user in immediate danger as an attacker has control over all aspects of the vehicle. Typically attacks are carried out in two ways: 1) through the OBD port of the AV or 2) through

Bluetooth exploitation. Attackers could modify the internal AV codebase through the OBD port or could connect via Bluetooth through a compromised device such as a phone and then modify internal ECUs [2]. Both types of attacks are low costing, require minimal knowledge, and are easy to implement. The main difference stems from proximity as OBD port injections require physical access whereas Bluetooth exploitations can be done remotely [2].

Section 3.3: Wireless Systems Attack Analysis

The GPS within an AV is susceptible to jamming and spoofing attacks due to the system's "transparent architecture" [2]. Attackers can freely research this architecture making spoofing attacks easily attainable. Since GPS receivers only care about the strongest available GPS signal, an attacker could potentially trick a system by broadcasting a stronger mimicked GPS signal [2]. This is shown in Figure 2 where an attacker misguides an AV by spoofing its GPS signal. This would misinform the AV of its current location causing it to change its route [2]. Thus, the user is not put in a life-threatening situation, making this attack more of a nuisance. According to Parkinson et al., these types of attacks require extensive hardware equipment in close-proximity to the AV to generate such a strong artificial GPS signal [2]. Also, Parkinson et al. noted that while reports have been written showcasing potential methods of GPS spoofing, they are primarily "proof-of-concept attacks" and the current hardware capabilities make it nearly impossible for these types of attacks to be readily available to the public [2].

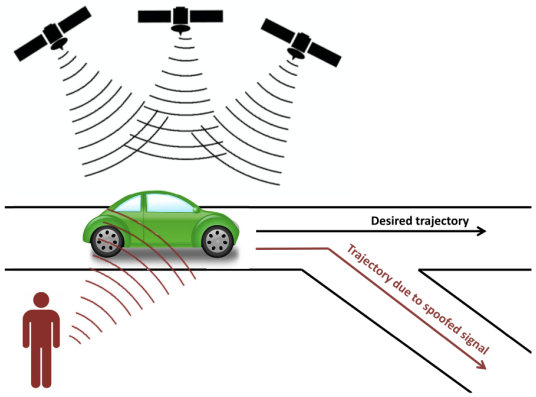

Figure [3]. GPS Spoofing Attack. An attacker can spoof the GPS signal by broadcasting a stronger signal causing the route of the car to change. Source from [2].

Wireless attacks on AVs follow similar structure to wireless attacks in other areas of cyber-security. These attacks aren't limited to AVs in specific but are general attacks that can be performed on any wirelessly connected device. An AV has the potential of seeing password

attacks, Denial of Service (DOS) attacks, Network Protocol attacks, Phishing attacks, and Rogue Update attacks [2]. In a password attack, an attacker attempts to break into an AV by utilizing common algorithms for brute-forcing the password [2]. In a DOS attack, an attacker places high load on AV's network blocking its communication with nearby AVs and other devices [2]. Network protocol attacks are attacks on particular vulnerabilities in a communication protocol such as TCP [2]. Phishing attacks are attacks that potentially trick a user into providing "sensitive information" about their AV through familiar forms or surveys [2]. Finally, rogue updates are attacks where an AV updates from a non-trusted source and can alter an AVs codebase [2]. Overall, wireless attacks are low costing attacks that require relatively minimal knowledge about AV specifics. They are easy to execute and can be carried out remotely. Thus, these types of attacks are life threatening not just for an AV user but for the general public as they can target a fleet of AVs at once.

Table 2. Overview of attack analysis based on criteria provided in Table 1. Attacks are listed according to the order laid out in the above discussion. The table uses the following color coding: green signifies the attack is low impact, orange signifies the attack is moderate impact, and red signifies the attack is high impact.

Technology	Attack	Hardware Cost	Proximity	Knowledge	Ease	Danger
Ultrasonic Sensors	Jamming	Low	Close-Proximity	Minimal	Easy	Life-Threatening
	Spoofing	Low	Close-Proximity	Non-Minimal	Difficult	Life-Threatening
	Acoustic Quieting	High	Close-Proximity	Non-Minimal	Easy	Life-Threatening
Inertial Measurement Units	OBD-Port Code Injection	Low	Physical Access	Non-Minimal	Difficult	Life-Threatening
LiDAR	Jamming	Low	Close-Proximity	Minimal	Easy	Life-Threatening
	Spoofing	Low	Close-Proximity	Non-Minimal	Difficult	Life-Threatening

Camera	Jamming	Low	Close-Proximity[1]	Minimal	Easy	Life-Threatening
ECU/ CAN	OBD-Port Code Injection	Low	Physical Access	Minimal	Easy	Life-Threatening
	Bluetooth attacks	Low	Remote Access	Minimal	Easy	Life-Threatening
GPS	Jamming	Low	Close-Proximity	Minimal	Easy	Non-Life Threatening
	Spoofing	High	Close-Proximity	Minimal	Difficult	Non-Life Threatening
Wireless	DOS/ DDOS Password Attacks Network Protocol Attacks Phishing Rogue Updates	Low	Remote Access	Minimal	Easy[3]	Life-Threatening[2]

[1] - Attacks are also susceptible to natural events such as sunlight.

[3] - These attacks can be easily performed by experienced hackers.

[2] - Depends on what an attacker targets. In some cases it may be non-threatening.

Section 4: Defensive Measures

Defensive measures for AV security systems fall into four categories: preventative, active, passive, and collaborative [3]. Preventive measures include encryption, authentication, and strategies to prevent attacks from external sources [3]. Active defenses detect and prevent attacks

by monitoring the AV network for erratic data [3]. Passive measures utilize software to detect an attack and alert the driver [3]. Finally, collaborative defense uses information from nearby AVs to detect discrepancies, such as sharing GPS information, which could indicate an attack. Figure X below shows a breakdown of some countermeasures by defense type. While defensive strategies for specific attacks exist, the design of AV security systems must be holistic. Focusing on a limited number of countermeasures for a list of attacks only protects from the identified threats. If the design of an AV security system only prevents a limited selection of attacks, hackers could use any other method to gain access to the vehicle. Hackers could develop methods and strategies not yet encountered in cybersecurity to circumvent the defenses put in place. This section produces a design strategy that hopes to mitigate attacks according to category.

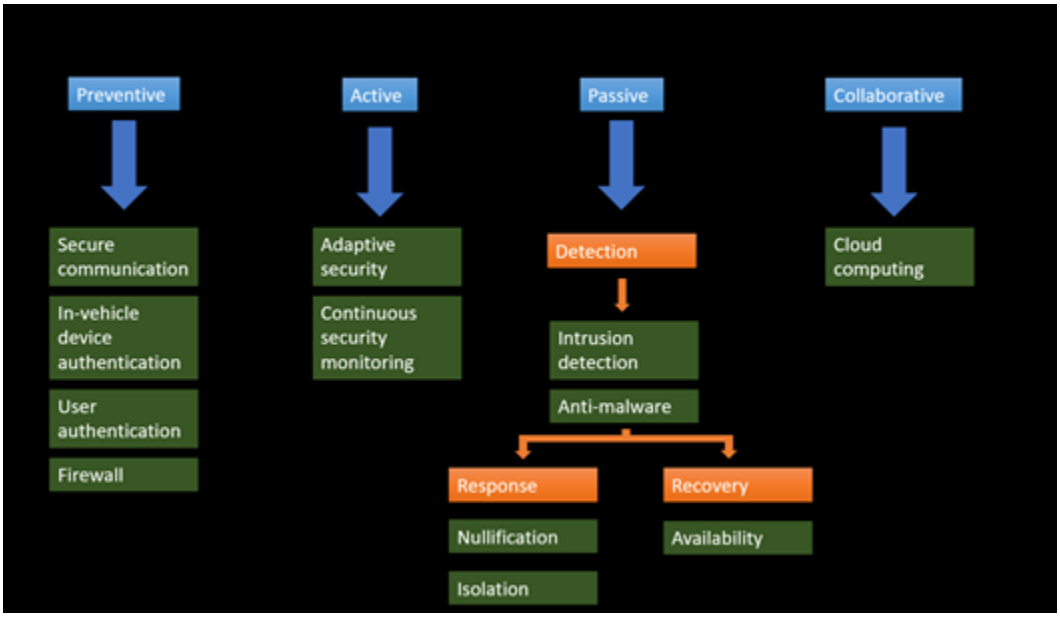

Figure 3. AV defense countermeasures fall under four categories: preventive, active, passive, and collaborative [3].

Source [8] finds that a well-defined strategy for a robust design of AV security systems does not yet exist. Autonomous vehicles use several sensors to understand the environment and utilize communication with other AVs and infrastructure for more information. Thus, the design of cybersecurity countermeasures must consider both systems. The design of security systems based on a limited number of possible attacks is inherently flawed, as this approach fails to account for the possibility of new attacks from different points of entry into the AV system.

Source [3] describes common countermeasures and methods for AV security design. Preventive measures aim to prevent attacks from succeeding in gaining access or otherwise affecting the vehicle. Examples of preventive measures include encrypted communication between AV components, authentication to prevent access from unrecognized sources, and firewalls to block

access to certain parts of the CAN and in-vehicle network [3]. Active measures for defense use methods to adapt to and detect compromised systems. Such methods include continuously scanning data coming from sensors into the AV network to detect anomalies and adaptive security countermeasures [3]. Adaptive security makes it harder for attackers to gain access to the vehicle by changing the specific countermeasure used, thereby making the attacker less likely to predict and plan a successful attack.

Passive defenses are further separated into three categories: detection, response, and recovery measures [3]. Detection measures can alert either the ECU or driver of the presence of an attack, which can then trigger an attack response protocol put in place by the manufacturer. The response measures, including nullification and isolation, are how the vehicle responds to an attack. Nullification could include anti-jamming in response to detected GPS signal jamming or otherwise taking steps to directly thwart the detected attack [3]. Isolation can refer to isolating the vehicle from the nearby vehicle communication network, thereby preventing the spread of malicious data to the surrounding road users [3]. Additionally, the vehicle can isolate the compromised sensor or component, thereby eliminating the influence the attacker can have on vehicle operation [3]. Recovery from the attack primarily depends on the ability of the vehicle to identify and eliminate the detected attack. Once this is done, the vehicle needs to be able to return to normal operation safely and quickly [3]. If a compromised AV system is left dysfunctional the vehicle might be unable to operate normally, such as the takedown of the vehicle's vision system. Without cameras and sensors, control must be returned to the human operator or the vehicle must otherwise not attempt to operate autonomously.

Security design generally follows a decision-making process centered on the objectives for AV attack mitigation [8]. Figure X illustrates a high-level proposed strategy for AV security system design [8]. Development begins with outlining the safety standards by defining the safety objective. Potential attack points such as sensors and communication networks are then assessed. The ease of attack and consequences of component compromise are considered alongside the formation of the adversarial model. The adversarial model specifies the capabilities and goals of attackers [8]. The security objective is then formed, which informs the design of security systems throughout the vehicle. Because attacks on AV systems can result in severe injury or death, the ability for the systems to withstand attacks is paramount. In the case of components which have a direct link to the operation of the vehicle, security is of the highest importance [8].

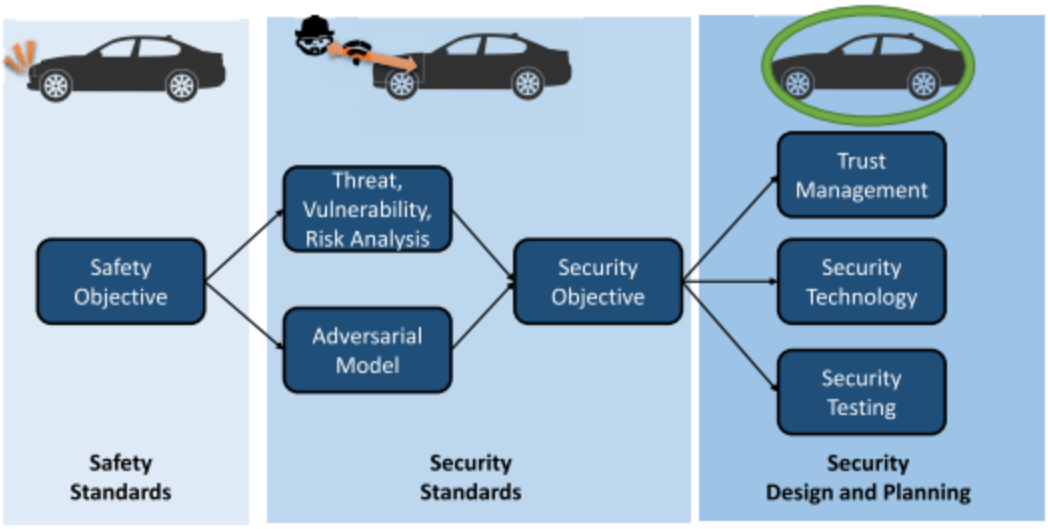

Figure 4. Overview of AV security system design approach for resiliency to multiple attack modes [8].

Because AVs depend on several systems for operation, it is difficult to identify and assign standard practices for developing secure systems. As the number of AVs in use increases, the effort and strategies of attackers can change [12]. To simplify the various systems, it can be helpful to differentiate "security perimeters" [8]. The security perimeters categorize AV systems based on sensitivity, connection modes, and exposure to attacks. For example, the communication between two vehicles can be categorized separately from the individual vehicle's steering controls. This allows for more general approaches to the design of the distinct categories, as opposed to taking an approach focused on the entire vehicle.

The design of AV safety systems must also consider failures not related to cyber-attacks on vehicles. [5] presents examples of various modes of failure and how AVs can react safely. Two types of failure are defined: vehicle-related and infrastructure-related. Vehicle-related failures include those of hardware, software, mechanical components, communication systems, and interaction platforms [5]. These types of failures can be the result of attacks or of simple malfunctions but have the same net result. Active and passive countermeasures can be used to mitigate the effects of such failures. In the event of a single sensor failure or inadequate information from a single type of sensor, redundancy allows for multiple backups to meet a minimum operational safety. Additionally, attacks on a sensor type (i.e, cameras) might not necessarily be critical if LiDAR and radar remain active. Monitoring anomalies in sensor readings helps alleviate failures from spoofing sensors or incorrect readings and could be used to determine the presence of a malfunction or attack. Passive countermeasures aim to protect the

passengers in the vehicle in the event of a major system failure or crash. These countermeasures include the crumple zone, airbags, and seatbelts [5]. Additionally, measures to detect and account for anomalous information can be implemented. Once the threat is detected and neutralized, the vehicle's ability to return to normal and safe operation is the final step. Infrastructure-related countermeasures include roadway design principles that can reduce the likelihood of a catastrophic event. Additionally, AVs could report roadway hazards to a local network of vehicles, giving advanced warning to the vehicle and passengers.

The vulnerabilities of AVs and the severity of the systems at risk require further research in cybersecurity techniques. AV security and safety are developing fields, and as such there are few standards that can be applied across all AV applications. Report [13] recommends that cybersecurity be a fundamental part of the design process for AVs, instead of a series of design decisions made after-the-fact. Active and passive defense strategies are crucial to the safety of AVs as they provide a preliminary measure in determining anomalies in sensor readings, but no federal guidelines exist for manufacturers to reference [13]. More robust legislation and better incentives will push manufacturers to design systems which meet or exceed certain safety requirements. These reports concur that the lack of industry-wide standards and lack of public information makes research difficult [8], [2], [5]. [8] also acknowledges that organizations can implement their own Threat Analysis and Risk Assessment (TARA) methodology, including various predictive and experimental methods already commonly used in cybersecurity settings. This further contributes to the lack of a coherent standard for AV design. As such, these reports share similarities in specific mitigation techniques, but find there is no coherent strategy for overall defensive design.

Section 5:Ethical Considerations

This problem is very much an ethical problem at its core. According to the National Society of Professional Engineers, it is the ethical obligation of an engineer to "Hold paramount the safety, health, and welfare of the public."[14]. It is the responsibility of engineers to ensure that the things they create are reliable and safe. Driving is inherently dangerous and something that we risk every day when stepping into a vehicle. In 2019 alone it was estimated that 38,800 people lost their lives in a car accident in the United States [15]. When someone steps into an autonomous vehicle, however, they are now taking that risk out of their own hands and putting it into the hands of the engineers that designed the system. If the system designed is not secure then that risk could also be put into the hands of malicious attackers.

If these automated driving systems are not regulated to specific standards they will be susceptible to significant technical attacks [2]. These attacks can put the passengers in the vehicle in significant danger, as well as people in other vehicles and unsuspecting pedestrians [1]. While the convenience of autonomous vehicles is very appealing and could provide many benefits, if not done safely the potential risks and dangers could outweigh the benefits. This level of danger must warrant engineers to take serious measures and be very strict in following standards to keep all parties safe.

Section 6: Conclusion and Recommendations

Widespread adoption of secured autonomous vehicles will provide a safer and more efficient transportation network. AVs are dependent on external sensors and internal ECUs connected by a bus to function. These vehicles would be interconnected and able to communicate with other vehicles and the vehicle's environment, using wireless modules to deliver an optimum safe and reliable service. As such, they could be vulnerable to malicious interference that could result in accidents. This interference can come in the form of physical or remote attacks. Physical attacks would require the attacker to be near the vehicle and have a limited scope. Remote attacks on the other hand are more serious as they have no such restriction and can affect multiple vehicles at once. Examples of remote attacks include wireless attacks that mirror the cyber attacks affecting any device connected to the internet.

To combat these threats, we recommend that the National Highway Traffic Safety Administration develop safety standards that all autonomous vehicles will be required to comply with before being sold in the United States. These standards should address all of the possible attack points by focusing on the sensitivity, connection modes, and attack exposure of the components. The standards should then utilize holistic defense measures, including component redundancies, firewalls, and encryption to create a safe and secure AV system.

To mitigate remote attacks, we want to prevent unauthorized access to communicated or stored data. To do so it is recommended to implement established cybersecurity protocols focusing on the development of authentication and encryption techniques, firewalls, and anti-malware software. Physical and vehicle-related safety and security concerns can be lessened by the introduction of redundancies and backups to compensate for component failure and incorrect readings.

Implementing and utilizing these standards in the development and production of autonomous vehicles would lead to an increase of public trust in AV technology and wider adoption of AV's.

This in turn would lower accident rates and increase the efficiency of traffic systems. That said, it is worth noting that an ideal implementation of this technology could lead to the phasing out of some professions that depend on the operation of vehicles, threatening the livelihood of millions of people.

Furthermore, we recommend further study of new and unconventional defense mechanisms to further reinforce AV security. Such mechanisms could include data clouds and the deployment of unmanned aerial vehicles (UAVs) as support nodes to prevent, detect, and recover from remote attacks such as jamming.

References

[1] Sharma, Pooja & Jha, Vaibhav & Arora, Vasudha & Jain, Prateek. "Towards the Prevention of Car Hacking: A Threat to Automation Industry," Indian Journal of Science and Technology, vol. 12, pp. 1-6, 2019. doi: 10.17485/ijst/2019/v12i41/145568.

[2] S. Parkinson, P. Ward, K. Wilson and J. Miller, "Cyber Threats Facing Autonomous and Connected Vehicles: Future Challenges," in IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 11, pp. 2898-2915, Nov. 2017, doi: 10.1109/TITS.2017.2665968.

[3] V. L. L. Thing and J. Wu, "Autonomous Vehicle Security: A Taxonomy of Attacks and Defences," in 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 164–170, Dec. 2016, doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.52.

[4] S. Singh, "Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey," *Traffic Saf. Facts - Crash Stats*, Art. no. DOT HS 812 115, Feb. 2015.

[5] J. Cui, L. S. Liew, G. Sabaliauskaite, and F. Zhou, "A review on safety failures, security attacks, and available countermeasures for autonomous vehicles," *Ad Hoc Netw.*, vol. 90, p. 101823, Jul. 2019, doi: 10.1016/j.adhoc.2018.12.006.

[6] Economic Commission for Europe Inland Transport Committee, "Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system" *World Forum for Harmonization of Vehicle Regulations,* June, 2020.[Online]. Available: http://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/ECE-TRANS-WP29-2020-079-Revised.pdf.

[7] Y. Freemark, A. Hudson, and J. Zhao, "Are Cities Prepared for Autonomous Vehicles?," *Journal of the American Planning Association*, vol. 85, no. 2, pp. 133–151, Apr. 2019, doi: 10.1080/01944363.2019.1603760.

[8] A. Chattopadhyay, K.-Y. Lam, and Y. Tavva, "Autonomous Vehicle: Security by Design," *IEEE Trans. Intell. Transp. Syst.*, pp. 1–15, 2020, doi: 10.1109/TITS.2020.3000797.

[9] H. Zeltwanger, "CAN Standard Review: Changes and Enhancements of the ISO 11898," *SAE 2000 World Congress*, pp. 2000-01–0143, Mar. 2000, doi: 10.4271/2000-01-0143.

[10] C. Yan, W. Xu, and J. Liu, "Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-driving Vehicle," *DefCon,* p. 13, doi: 10.1145/1235.

[11] "New Level 3 Autonomous Vehicles Hitting the Road in 2020," *IEEE Innovation at Work*, Jan. 10, 2020. https://innovationatwork.ieee.org/new-level-3-autonomous-vehicles-hitting-the-road-in-2020/.

[12] G. De La Torre, P. Rad, and K.-K. R. Choo, "Driverless vehicle security: Challenges and future research opportunities," *Future Gener. Comput. Syst.*, vol. 108, pp. 1092–1111, Jul. 2020, doi: 10.1016/j.future.2017.12.041.

[13] C. Kennedy, "New Threats to Vehicle Safety: How Cybersecurity Policy Will Shape the Future of Autonomous Vehicles The Autonomous Vehicles Issue: Note," *Mich. Telecomm. & Tech. L. Rev.*, vol. 23, no. 2, pp. 343–356, 2017 2016.

[14] National Society of Professional Engineers. "NSPE Code of Ethics for Engineers." NSPE.org. https://www.nspe.org/resources/ethics/code-ethics.

[15] National Safety Council, "Motor Vehicle Deaths Estimated to Have Dropped 2% in 2019." NSC.org. "https://www.nsc.org/road-safety/safety-topics/fatality-estimates#:~:text=In%202019%2C%20an%20estimated%2038%2C800,2%25%20decrease%20over%202018%20figures."