Autonomous Vehicle Security

Shreyas Ramesh
Cybersecurity
University at Buffalo
(State University of New York)
Buffalo, USA
Ramesh3@buffalo.edu

***Abstract*— Autonomous vehicles (AVs) are expected to offer many benefits, such as improved safety, efficiency, and mobility. However, they also pose significant challenges in terms of security and privacy, as they rely on complex software systems that can be vulnerable to various attacks. In this paper, we survey the current state of AV security research, focusing on the main types of attacks that can target AVs, such as hacking, spoofing, jamming, and sabotage. We also review the existing methods for evaluating and mitigating the security risks of AVs, such as penetration testing, vulnerability scanning, intrusion detection, and secure communication protocols. Finally, we discuss some of the policy implications and recommendations for enhancing the security and privacy of AVs in terms of regulation, standardization, education, and public awareness. The paper aims to provide an overview of the current challenges and opportunities for securing autonomous vehicles in the context of their implementation, adoption, and societal impact**.

***Keywords*— Autonomous vehicles, artificial intelligence, blockchain, privacy, cybersecurity, cyberattacks.**

I. INTRODUCTION

Autonomous vehicles (AVs) are self-driving cars that can navigate and interact with their environment without human intervention. They have the potential to revolutionize transportation, improve safety, efficiency, and convenience, while reducing traffic congestion and emissions. However, AVs also pose significant challenges and risks for society, such as ethical, legal, social, technical, and economic issues. Therefore, it is essential to address these challenges and risks in a comprehensive and responsible manner, and to develop trust and acceptance among the stakeholders and the public.

Modern cars are fitted with a range of autonomy features. In order to distinguish such cars with varying degrees of autonomy in a consistent manner, the society of automotive engineering (SAE) proposed 6 levels of autonomy in their standards. Level 0 means no automation while level 6 denotes the highest level of automation. For levels 0-2, a human needs to constantly monitor the driving environment. For levels 3-5, the driving systems performs the monitoring of the environment [1].

As you keep increasing the autonomy of the vehicle, security concerns of the machine also increases. For cars operating in level 3 and above, it is imperative to make sure that it is fitted with an increased number of sensing and communication devices. In addition to security and safety concerns, AV's also have issues related to data privacy and protection. By jailbreaking an AV, threat actors can gain access to a huge amount of sensitive personal data, including information about location, biometric data and passwords for connected devices. Security experts agree that cybersecurity and privacy challenges are becoming increasingly important as AV's become a reality.

The remainder of this paper is organized as follows:

- Main Techniques.
- Security Issues.
- Future Trends.
- References.

II. MAIN TECHNIQUES

A. Sensors

Sensors are key components for autonomous driving: they allow the vehicle to monitor its surrounding environment, as well as collect the data needed in order to drive safely. Currently AV's generate upto 25 GB of data per hour, but with progression in technology it will increase exponentially. The generated data is analysed and processed by an onboard computer to build a path from one point to another. The three primary sensors in an AV are LiDAR, RADAR and cameras [2].

RADAR sensor uses radio waves for object detection within a certain range. It is used in AV to recognize the environment of a vehicle in real-time. LiDAR uses a shorter wavelength laser to achieve higher measurement accuracy and better spatial resolution than RADAR. Video cameras read traffic lights and road signs and monitor pedestrians and obstacles.

The global navigation satellite system (GNSS) is the most widely used technology for providing accurate position information on the surface of the earth. The best-known GNSS system is the Global Positioning System (GPS), which provides Positioning, Navigation, and Timing (PNT) services to the users. The receiver is always on the lookout to locate atleast four satellites. It then uses this information to figure out its own position using a process called trilateration.

B. Electronic control unit (ECU)

It is an embedded system that controls the state of vehicle engine and manages the sensors inside the vehicle. Small and medium sized vehicles include 50 ECU's whereas luxury vehicles have around 150 ECU's. Each ECU collects information from one or many sensors and uses this data to take necessary action.

C. Inter-Vehicle Communication

AV system networks enable on-vehicle communication between multiple components such as ECU's, sensors and actuators. These networks allow components designed by different manufacturers to exchange data and resolve operational dependencies. The most commonly used system networks are Controller area network (CAN), TTCAN, FlexRay or Local Interconnect Network (LIN) [3]. Example of applications on different system networks:

1) LIN and CAN: Display, Alarm, Lighting, A/C, Windows, Seat mirrors, Windshield, wipers and headlamps.

2) TTCAN and FlexRay: Engine, Transmission, Braking, Steering, Suspension, Assistance, Safety and Diagnostics.

D. Vehicle to everything communication technology

This technology allows the AV to communicate with everything in its surrounding making driving a safe and smooth experience for everyone. This technology (V2X) consists of vehicle to vehicle (V2V), vehicle to infrastructure (V2I), vehicle to pedestrian (V2P) and vehicle to network (V2N) communication pathways [2]. By utilizing all these different communication networks, the vehicle is able to maintain an understanding of its surroundings enabling it to take better driving decisions. Another form of communication network required for AV's is the mobile cellular network. A standardised set of cellular vehicle to everything (C-V2X) was designed to enable communication between AV's and roadside infrastructure. C-V2X supports both short and long range transmissions and enables highly reliable, real-time communication at high speeds in high density traffic.

V2X communication technologies also have the potential to facilitate communication between Autonomous Vehicles (AVs) and Unmanned Aerial Vehicles (UAVs), offering various services to ground-based AVs. UAVs are seen as a crucial component in realizing the future of intelligent transportation systems for connected AVs. Some key applications of UAVs for ground-based AVs include utilizing UAVs and edge computing devices for traffic monitoring, providing edge/fog computing services, serving as incident or accident reporters, and functioning as dynamic roadside units (RSUs) [2]. For example, UAVs can serve as mobile aerial base stations, assisting AVs and creating an interconnected automated system with diverse capabilities. Additionally, due to their high mobility, UAVs can improve AVs' perspective and enhance visibility in surrounding areas.

The convergence of these different technologies allows AV's to revolutionize the future of commute and transport.

III. SECURITY ISSUES

While AV's are relatively new teachnology, it borrows heavily from other forms of technology used by threat actors to further their malicious goals. In order to safeguard life and property in the age of AV, it is imperative to understand the security implications and discover potential mitigation measures. Documented below are the security issues and problems that arise due to AV's and a few possible mitigation steps.

Phases of attacks

An attack on AV is a complicated subject with attackers approaching it in different phases depending on their objectives. The four phases of an attack an AV are:

In the first phase attackers can exploit vehicle communication protocols by sending spoofed messages to AVs or other vehicles, manipulating their behaviour or location. They can instruct an AV to deviate from its planned route or stop in a dangerous situation. Additionally, they can disable the communication system of an AV using denial-of-service attacks.

In Phase 2, attackers can exploit vehicle sensors and perception algorithms in autonomous vehicles (AVs). They have the capability to tamper with sensors or manipulate sensor data processing, which AVs rely on for perceiving their environment. This includes introducing noise or false signals into radar or lidar data, as well as injecting adversarial examples into the vision system. These actions can lead to incorrect decisions by AVs and failures in detecting obstacles and hazards [4].

During Phase 3, attackers can compromise the software and cloud server of autonomous vehicles (AVs), which control the vehicle's actions and update its maps and parameters. They can inject malicious code or instructions to override driver input or cause unintended actions. Additionally, vulnerabilities in the software allow them to gain unauthorized access to sensitive information or valuable data.

In Phase 4, attackers can manipulate the user interface of an AV to influence driver or passenger behaviour and trust. They may display fake warnings, alter feedback signals, or inject false information into the navigation system. These actions cause confusion, distraction, and panic among users. Hackers carefully consider various factors when exploiting a vehicle's human-machine interface in order to achieve their goals [4].

A. Attacks against communication system

Attackers can cause a denial of service attack by flooding the system with tons of dummy messages, thereby reducing efficiency and performance of the network. Even if a DOS attack is detected, it is difficult to stop it within the context of AV's. In an ecosystem of cooperative vehicles, any vehicle can falsify a large number of false identities and transmit dummy messages to others vehicles and RSU's [3]. Distributed denial of service attacks is also a very real possibility of multiple vehicles colluding and attacking a single vehicle from different directions. If a DDOS attack occurs on an AV, the internal network would be rendered incapacitated to provide communications with other vehicles.

Attackers can also perform a jamming attack. This attack essentially prevents AV's from being able to communicate with V2V and V2I channels. It is possible by causing intentional interference using noisy signals or messages. Even a low-cost Arduino DIY jammer was successful in jamming many ultrasonic sensors present in Tesla Model S [2].

B. Attacks against navigation system

LiDAR's are devices which use rotating laser beams. The device is used in the detection of obstacles and helps to navigate the autonomous vehicle through its surroundings. The data generated by the LiDAR system provides information about where obstacles exist in an environment and the position of the autonomous vehicle with respect to the obstacle. It basically shows curvatures in roads, infrastructure, vegetation and elevation. Attackers can create noise, fake reflections and spoof objects to trick the system into believing something that does not exist. By chaining both reflections and spoof techniques, an attacker can effectively control the course of movement of an AV.

Another key technology used in AV navigation is GPS. An attacker can simulate a positioning attack on the satellite. Thereby, a malicious actor can send false location information to unsuspecting vehicles if this signal is stronger than authentic GPS signal [4]. A common occurrence is vehicles losing GPS signals within tunnels; an opportunistic attacker can take advantage of this situation to send false GPS information to the vehicle.

C. Attacks against software

An AV is basically a car being run on software and as such, malicious actors can use their ingenious creativity to install malicious software on the on-board computer system. This way, just like a computer, a threat actor will have access to the AV whenever they want. The malicious software can do a bunch of things including disrupting sensors, manipulating data or even taking control of the car.

Depending on the code design and vulnerabilities on the AV, a threat actor can also perform remote code executions. This is extremely dangerous as this would allow a malicious actor to take control of vital driving functions including acceleration and braking.

Another vector of attack is the Man-in-the-middle attack. The attacker exploits the Wireless Communication Module (WCM) of an AV, which is responsible for transmitting and receiving data from the cloud services or other vehicles. The attacker pretends to be the WCM or another vehicle and sends malicious messages to the AV, instructing it to perform a specific action such as braking, swerving, or changing lanes. The attacker intercepts the signals from the legitimate WCM or other vehicles and sends them back to the AV, altering their content or timing. This action could cause the AV to deviate from its intended path or trigger an inappropriate reaction. The attacker can also use the same method to access the personal data or preferences of the users of the AV and compromise their privacy or security [5].

Machine Learning (ML) and Deep Neural Networks (DNNs) are essential in Avs for processing sensory data and making informed decisions at different levels. However, these techniques have been recently found vulnerable to several attacks that attempt to manipulate the learning system and lead it to produce an incorrect result [2]. The most well-known attacks are evasion, poisoning and inference, while there are also trojaning, backdooring and reprogramming attacks. Adversarial poisoning attacks target the data used to train the learning system by introducing poisoned data into the training dataset.

D. Case studies on real cars

In recent years, numerous research studies have demonstrated different methods by which malware can infect the AV systems. For example, in 2019, a group of researchers proved the ability to hack a Tesla Model 3 vehicle in few seconds by exploiting a weakness in the browser of the infotainment system to get inside the vehicle's computers and run their own source code. Another research group at Leuven in Belgium were able to steal a Tesla Model X vehicle by injecting malware through the firmware update into the key fob via Bluetooth connection. Security researchers also demonstrated the ability to perform a remote car hacking against a Chevy Malibu by exploiting a vulnerability in the Bluetooth.

IV. FUTURE TRENDS

To develop more resilient and reliable systems that can cope with various threats, such as cyber-attacks, hardware failures, or software bugs, one direction for AV security is to use redundant sensors, controllers, and communication networks. Additionally, implementing verification and validation methods ensures the correct operation of the system. AV security should enhance the privacy and data protection of the users and vehicles. To achieve this, we can use secure and encrypted communication protocols, anonymize or aggregate the data collected by sensors, and apply access control and authentication policies to prevent unauthorized access or tampering [5].

The legal and ethical challenges that arise from the deployment of autonomous vehicles can be addressed by taking a third direction for AV security. This involves developing standards and regulations for testing, certification, and operation of the systems, as well as creating a framework for liability and accountability in case of accidents or incidents. Various stakeholders, such as researchers, manufacturers, regulators, and users should collaborate and innovate to foster AV security. They can achieve this by organizing workshops, conferences, and challenges to share knowledge, experiences, and best practices. Additionally, creating incentives and rewards for developing novel solutions and technologies will further support these efforts.

The age of AV's is here. Despite the benefits of autonomous vehicles, these network-based engines are highly susceptible to privacy and security attacks. Security should be a priority and not an afterthought when building AV's and the different attacks showcased in this paper prove exactly that.

V. REFERENCES

[1] Chattopadhyay Anupam and Lam Kwok-Yan, "Security of Autonomous Vehicle as a Cyber-Physical System", Retrieved from: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8303906.

[2] Bendiab Gueltoum, Hameurlaine Amina, Germanos Georgios, "Autonomous Vehicles Security: Challenges and

Solutions Using Blockchain and Artificial Intelligence", Retrieved from: https://ieeexplore.ieee.org/document/10023964

[3] Abdulla O. Al Zaabi, Chan Yeob Yeun, Ernesto Damiani. "Autonomous Vehicle Security: Conceptual Model." Retrieved from: https://ieeexplore.ieee.org/document/8903691

[4] Firoz Khan, Seifedine Kadry, Lakshmana Kumar Ramaswamy, Maytham N. Meqdad (2021). "Autonomous vehicles: A study of implementation and security". Retrieved from: https://www.researchgate.net/publication/350486877

[5] Ashish Nanda, Deepak Puthal, Joel J. P. C. Rodrigues, Sergei A Kozlov. "Internet of Autonomous Vehicles Communications Security: Overview, Issues, and Directions". Retrieved from: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8809661&tag=1