2023 International Conference on Artificial Intelligence of Things and Systems (AIoTSys) | 979-8-3503-1227-0/23/$31.00 ©2023 IEEE | DOI: 10.1109/AIoTSys58602.2023.00052

An Overview of Security in Connected and Autonomous Vehicles

Bulut Gozubuyuk†, Wes Bailey†, Douglas Everson†, Zheng Dong‡, Long Cheng†, Mert D. Pesé†
†School of Computing, Clemson University, USA
‡Computer Science Department, Wayne State University, USA

***Abstract*—As the enabling technologies for connected and autonomous vehicles (CAV) continue to advance and these modes of transportation become more commonplace, there is a reasonable expectation that the systems will increasingly become targets for bad actors. The complexity and inter-connectedness of these devices offer myriad opportunities for security compromise, potentially resulting in unsafe operation or leakage of confidential information about the user. This paper conducts a brief review of the current state of CAVs with regard to security and privacy. We present a taxonomy for classification of these threats and use it to identify and enumerate existing threats in this space.**

I. Introduction

The connected and autonomous vehicle (CAV) has long been a product of science fiction but appears to be drawing closer to reality as the enabling technology steadily improves. The potential benefits of autonomous vehicles are profound, with implications in public safety, social mobility, and climate change. Whether through mass transit, ride-sharing services, or privately-owned CAV, there is a strong likelihood that the number of consumers engaging with self-driving cars will increase dramatically in the coming years. Prior studies indicate that there is a general lack of public awareness regarding the security issues and privacy implications for CAV users [1]. One of the drivers of CAV technology is the increased reliance on interconnected cyber physical systems. While this evolving paradigm presents an enormous growth opportunity for advanced products and services, it exposes a wider range of vulnerable entry points for malicious actors. There are numerous phases of activity within the cyber-physical envelope, including *sensory*, *computation*, *storage*, *actuation*, and *communication*. Each of these segments poses unique vulnerabilities and may require specific domain knowledge to mitigate realistic threats appropriately.

As self-driving systems develop in scale, capability, and complexity, so do the vulnerabilities and the corresponding opportunities for malicious actors. These potential threats might target the physical systems or software of the vehicles themselves or the enabling hardware and software in the surrounding support infrastructure. Additionally, the data generated by the operation of the self-driving systems may expose personal and confidential information that could be misused by unauthorized parties, creating a threat to user privacy. Security and privacy considerations must be considered a foundational layer in the design of CAV and not some kind of 'bolt-on-later' strategy. A typical vehicle lifetime is in the 15-year range, and the cutting-edge systems installed when the car was built must be supported and updated for functionality and security throughout this life cycle.

In this paper, we conduct a brief survey of the threat landscape presented by CAV related to security and privacy. We present a taxonomy for classification of threats to CAV based on different attack surfaces, and use it to examine, categorize, and discuss the representative vulnerabilities and mitigation strategies. This taxonomy is illustrated in Figure 1. This paper creates a kernel for future research and classification of threats to CAVs.

II. Threats to Vehicle Sensors

CAVs are highly complex and interconnected systems that often involve many sensors, such as GPS, LiDAR (Light Detection and Ranging Technology), cameras, IMU (Inertial Measurement Unit), radars and ultrasonic sensors, to capture the environmental circumstances for improving vehicle safety, efficiency, and mobility on roadways. This reliance on multiple sensors makes CAV vulnerable to a variety of threats, as discussed in the following.

A. GPS Attacks

Attacks to GPS systems are well established and have been the subject of a considerable amount of research. These can be broadly categorized as either jamming or spoofing attacks [2]. It is possible for a vehicle's GPS receiver to be jammed via local signal interference, causing the device to lose its satellite feed. The attacker can then create a locally delivered replacement signal with a higher power level that will be interpreted as the legitimate feed when the jamming is stopped and the receiver attempts to re-acquire the signal. GPS attacks can pose a serious threat to the security and reliability of CAV's localization, and can cause vehicles to drift off course and potentially lead to accidents. Shen *et al.* [3] studied the potential security risks of using multi-sensor fusion (MSF) for localization in CAV when GPS signals are being spoofed. Although MSF compensates for the potential loss or error of GPS signals by combining data from multiple sensors to achieve accurate and robust localization, authors in [3] demonstrated that the false GPS signals can still corrupt the fusion process and lead to the vehicle drifting off course.

There are several techniques that can mitigate the impact of GPS jamming and spoofing. For example, Mosavi *et al.* [4] noted that the Direct Sequence Spread Spectrum (DSSS) nature of the GPS signal has inherent anti-jam properties

979-8-3503-1227-0/23/$31.00 ©2023 IEEE
DOI 10.1109/AIoTSys58602.2023.00052

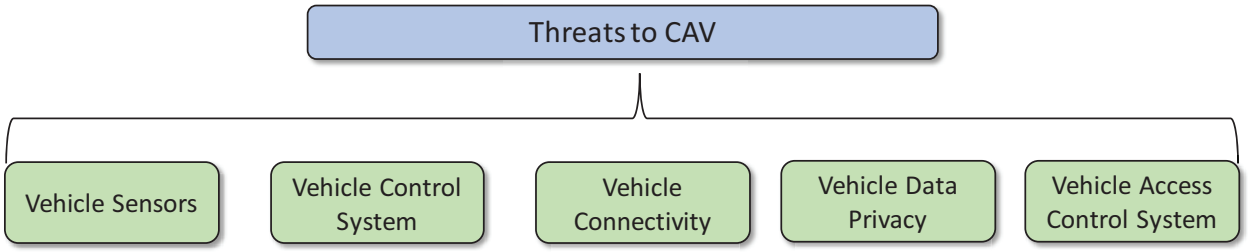

Fig. 1: Threat taxonomy for CAV.

but that a jammer with sufficient power can override those proetctions. They discussed additional mitigations, including adaptive antennas, adaptive filtering, and time-frequency filtering before presenting an experiment for a specific time-frequency filtering method called wavelet transform.

B. LiDAR Attacks

LiDAR is widely used in autonomous vehicles as a means of environmental perception and distance measurement. LiDAR hardware is vulnerable to spoofing attacks of the device's laser pulses which can be launched from nearby vehicles or stationary roadside devices. Cao *et al.* [5] proposed a method of monitoring a target LiDAR and using that timing to craft a signal perturbation that will create a false indication of an obstacle, possibly resulting in emergency avoidance action and injury to the vehicle or its occupants. A mitigation for this attack was later proposed by the same team, relying on certain physical invariants to detect false positive readings induced by the prior attack method.

C. Camera Attacks

CAVs use cameras for acquisition of visual data required to detect vehicle surroundings and inform spatial perception. These light-sensing devices are at risk of compromise or even permanent damage from low-cost, readily available light sources. Prior work has indicated that vehicle camera systems are at risk from both 'blinding' attacks and 'rapid on-off' attacks, both of which can disorient and disrupt the safe operation of the system. Malicious actors can craft visual data to be gathered by vehicle cameras that can then manipulate CAV's image classification algorithms, particularly the deep neural networks (DNN) that are increasingly used in CAV. Sato *et al.* [6] presented an attack on vehicle cameras using printed adhesive overlays that appeared to be dirty, patched sections of road, but were actually carefully crafted malicious input designed to spoof the neural network to mis-detect the road center line. The researchers were able to induce crashes in laboratory environments using this technique. Finally, Ji *et al.* [7] injected acoustic waves directed at the CAV camera to attack its image stabilizer hardware and causes image blurring which in turn affects the object detection performance.

D. IMU Attacks

Inertial measurement unit (IMU) sensors are components in modern connected and autonomous vehicles (CAVs) that can measure the vehicle's dynamics using accelerometers, gyroscopes and magnetometers. They, unfortunately, serve as a prime target for cyber-attacks intended to compromise vehicle stability and safety.

For instance, accelerometers measure the rate of change of vehicle velocity, giving Electronic Stability Control (ESC) systems crucial information that helps them keep a vehicle under control when turning [8]. Trippel *et al.* [9] showed that MEMS accelerometers are vulnerable to sonic attacks, i.e., the accelerometer output can be controlled by audio, which in turn may result in the ESC system responding improperly and causing vehicle instability.

E. Acoustic Sensor Attacks

Ultrasonic sensors are widely used in autonomous vehicles for ranging and obstacle detection. Due to the operational nature of these devices, they are vulnerable to jamming and spoofing by external signals. Xu *et al.* [10] proposed and demonstrated both random and adaptive spoofing attacks on ultrasonic sensors. They were able to induce a black-box system to incorrectly infer the presence of an obstacle, and also to incorrectly infer a clear path when an obstacle was actually there.

Voice assistant platforms (*e.g.*, Amazon Alexa) allow users to interact with their cars through verbal commands. However, voice-controlled vehicles are vulnerable to audio adversarial attacks. Due to a lack of proper authentication from users to voice assistant devices, an adversary can generate hidden voice commands that are either not understandable or inaudible by humans to compromise speech recognition systems.

III. Threats to In-vehicle Networks

Many threats to vehicle control systems stem from commonalities found across the CAV internal networking and hardware architecture. CAVs have a highly distributed in-vehicle network comprising numerous Electronic Control Units (ECUs). Sensors and actuators which are used to make navigation and

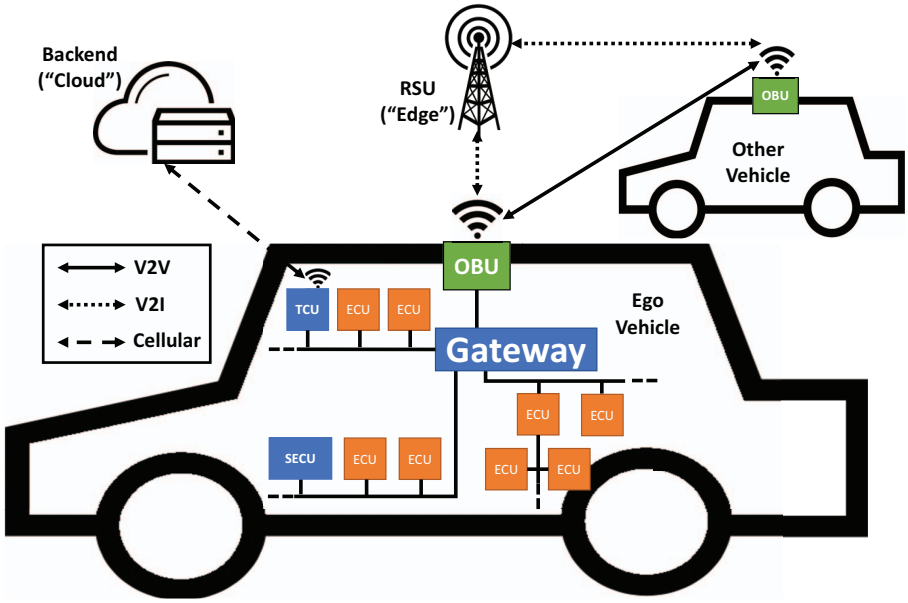

Fig. 2: Overview of CAV communication architecture.

control decisions are directly connected to ECUs. Data is exchanged between ECUs via an in-vehicle network (IVN), with the Controller Area Network (CAN) bus being the de-facto standard in contemporary vehicles. Other common communication protocols in the IVN encompass Automotive Ethernet, FlexRay and LIN. An overview of CAVs' communication architecture is depicted in Figure 2.

CAN is a broadcast-based protocol and every ECU is constantly listening to the traffic. An ECU decides to process the CAN message if its CAN ID matches its acceptance filter. Since CAN has not been designed with security in mind, recent research deals with enhancing it by the key cyber-security properties of confidentiality, authenticity, and availability. The main threat and key part of every cyber-attack against vehicles to date are *CAN injection attacks*, which can lead to serious malfunctioning of the vehicle. Examples of malfunctioning include, but are not limited to, arbitrarily accelerating, braking or steering the vehicle, but also tampering with body operations, such as breaking the HVAC or disabling the airbags. The most common form of CAN injection attack is message spoofing which entails suspending the authentic broadcast from a legitimate ECU and transmitting a message with identical CAN ID, but modified payload.

In particular, Pesé *et al.* [11] defined three categories of CAN injection attacks. 1) *Fabrication* attacks allow the adversary to fabricate and inject messages with a forged CAN header and payload at a higher frequency to override cyclic CAN messages sent by legitimate ECUs. 2) *Suspension* attacks on the compromised ECU prevent its broadcast of legitimate, potentially safety-critical CAN messages to the intended recipient(s). Suspension attacks comprise Denial-of-Service (DoS) attacks which exploit the CAN protocol design. CAN messages with smaller IDs are higher-priority and will always win arbitration on the CAN bus compared to messages with higher CAN IDs. An attacker can inject messages with low CAN IDs to effectively silence certain ECUs that transmit lower-priority messages. Another example is the bus-off attack which takes advantage of the CAN error handling mechanism. In the lack of an adversary, the latter can prevent faulty ECUs from negatively affecting CAN communications by putting them in a bus-off state after a repeated number of communication violations. An attacker can easily exploit this mechanism to deliberately suspend legitimate, non-faulty ECUs. 3) *Masquerade* attacks combine both of the above attacks by suspending the CAN broadcast of one ECU and deploying another ECU to fabricate malicious CAN messages. Last, but not least, eavesdropping on CAN traffic is possible due to the lack of encryption, which results in compromise of personal information or make CAN bus reverse engineering possible. The latter is a necessary precursor to CAN injection attacks since the attacker needs to form a well-crafted CAN message to achieve a visible outcome of vehicle malfunctioning.

Attacks on the CAN bus (or interchangeably any in-vehicle network) can be grouped into three generations. Figure 3 shows the three generations of in-vehicle network attacks.

A. First-Generation Attacks

First-generation attacks that started with the rise of automotive security literature in the early 2010s [13], [14] were mostly targeting physical interfaces, *i.e.*, the attacker needed to have physical access to their victim vehicle. Once the attacker was inside the vehicle, they could simply access the in-vehicle network (IVN) through a physical connector called Onboard Diagnostics (OBD-II) port. This interface is mandated in all

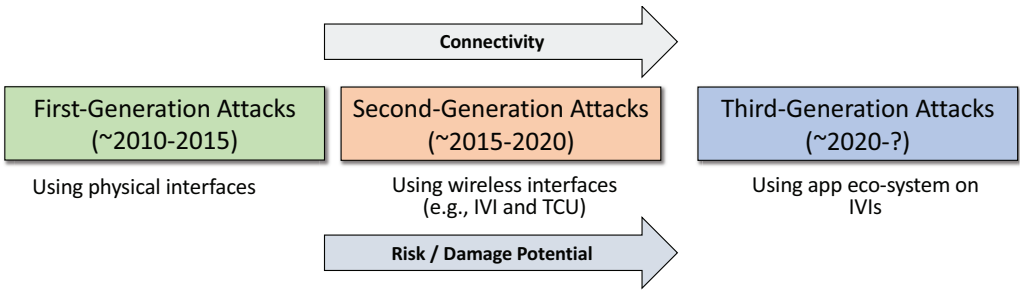

Fig. 3: Three generations of in-vehicle network attacks (as proposed by Pesé [12]).

US gasoline vehicles manufactured after 1996. With physical access to this port, it is possible to launch aformentioned CAN injection attacks, but also update ECU software on a CAV using the Unified Diagnostic Protocol (UDS). Key mitigations against CAN-based first-generation attacks include secure software design, digitally-signed messages, and ECU fingerprinting to assure messages were sent from the legitimate ECU. However, implementing aforementioned mitigations on the CAN bus is non-trivial. Providing message authentication is difficult due to the limited amount of space in CANs data fields along with the necessity of exchanging data in real-time. Furthermore, car makers deploy computationally weak ECUs due to cost reasons which limit the implementation of cryptographic algorithms. The added latency at the sender and receiver for encrypting/decrypting, as well as signing/verifying messages has a direct impact on hard real-time deadlines on the CAN bus which cannot be missed to conform with functional safety. Alternative mitigation strategies to add a layer of security while addressing these constraints have been proposed in recent literature [11]. In recent years, AUTOSAR SecOC [15] has emerged as an accepted solution among OEMs to add basic security principles to the CAN bus.

As electric propulsion systems supplant combustion engines, a growing proportion of CAVs, will be required to periodically plug in to charging stations. Like laptop computers, the electric vehicle charging port connects to power and data and form another entry point for first-generation attacks. This physical access point offers an entry point for abusive actors, and could not only expose the charging and electric system to intentional damage, but the data port may allow access to the control bus, component firmware, or onboard data storage devices. While the current J-1772 connection does not allow reception of data beyond the simple pulse to configure the charging output, future connections could take advantage of Power Line Communication (PLC) standards to provide more robust data transfer, increasing the potential of misuse.

It is not possible to fully secure the access point since the end user must be able to plug into charging ports in public areas where the location may not be fully secure. It is therefore incumbent on the vehicle designers and systems developers to ensure that appropriate levels of data encryption and secure code practices are implemented. The Open Charge Point Protocol (OCPP) provides security features in its second version to address some of the aforementioned vulnerabilities.

B. Second-Generation Attacks

Second-generation attacks went further and tried to gain IVN access without being physically inside a vehicle. For this purpose, attackers would exploit vulnerabilities in the wireless interfaces of ECUs, e.g., the WiFi or cellular connectivity of Telematic Control Units (TCUs). TCUs are devices embedded into automobiles that integrate various services and features into the vehicle. They provide connectivity using WiFi, Bluetooth, GPS, and mobile data interfaces. Many TCUs are part of In-Vehicle Infotainment (IVI) systems that comprise car radios and navigation systems. Since TCUs are connected to the IVN, CAN injection attacks that have been discussed in the previous subsection can be launched through a compromised TCU analog to first-generation attacks. The most comprehensive and impressive attack of this generation was the famous Jeep hack that happened in 2015 [16]. These hackers were able to obtain CAN bus access through several vulnerabilities in the TCU's software and hardware and could kill a running Jeep Cherokee on the highway (or steer it into a ditch). As a result of this hack, 1.4 million vehicles had to be recalled and a lawsuit that had been filed against the OEM and Tier-1 was just dismissed in 2020. Compared to the first-generation of attacks, this generation is more feasible to be conducted since no physical access is required. As a result, the risk and damage potential increases. Furthermore, these attacks are also more scalable as the high number of recalls proved.

A large influence in executing TCU attacks derives from the simplicity of publicly discoverable devices. Targeted devices were discovered by scanning known ports over specified IP address ranges. Using Network Address Translation (NAT) would substantially aid in obscuring the identity of target devices. Removing the transceiver interface from TCUs to prevent CAN communication is another suggested course of action, however this may cripple many of the TCUs functional purposes.

C. Third-Generation Attacks

Finally, third-generation attacks take the scalability and damage potential even further. As of the time of this writing, there are no known attacks yet, although the technology required for it is slowly maturing. A new IVI operating system

called Android Automotive OS (AAOS) was announced by Google in 2017. A custom flavor of the popular Android mobile operating system, its most distinct feature is its ability to connect to the IVN and read, as well as write data to it. Third-party apps will be gradually supported in a custom Play Store, but are limited to media, messaging, navigation, parking, and charging apps at the moment. With an increasing number of third-party apps, as well as OEMs heavily customizing AAOS, there is serious security risk coming from this platform [17]. Now, malicious entities will be able to access the vehicle and its IVN from anywhere, opening the doors for significant damage potential.

IV. Threats to Vehicle-to-Everything Communication

The capabilities of a CAV are facilitated and augmented by its connection to a wider network. As the telecommunications industry rolls out 5G, there is an expectation that most CAVs will be driven by the network capabilities introduced using the mobile edge of 5G to gain ultra low-latency, highly reliable, and high capacity data transfer. An example of novel interfaces for the connected CAV ecosystem are widely available mobile companion apps (e.g., BMW Connected) to remotely start or even steer the vehicle, further increasing the interconnection of carmakers' infrastructure with their cars. Vulnerabilities in this ecosystem can seriously impact safety.

The future of intelligent transportation systems (ITS) will be spearheaded by vehicle-to-everything (V2X) communication. V2X is one of the complementary technologies to enhance and support Advanced Driver-Assistance Systems (ADAS) and CAVs. Primarily, the V2X communication range is greater than the sensing ranges of current ADAS and CAV sensors, such as radar, LiDAR and cameras. Among others, V2X allows connected vehicles to talk to other vehicles (V2V), smart infrastructure (V2I) and pedestrians (V2P). All these protocols can be performed over either a cellular network or a short range network such as DSRC (Dedicated Short Range Communications) and LTE Sidelink. Figure 2 depicts these use cases. V2X can also be used with cars that have a lower level of automation, such as traditional cars, and help them avoid traffic congestion and prevent collisions. For these purposes, vehicles exchange Basic Safety Messages (BSMs) in the US which are defined in the SAE J2735 standard. BSMs contain state information about a vehicle, such as its location, speed, acceleration, heading and yaw rate. Vehicles listen to BSM broadcasts and can plan their future actions accordingly, *e.g.*, by slowing down or speeding up. This can enhance road safety as long as there is no malicious interference. The field of V2X security has received increasing scrutiny over the last decade, with various standardization bodies in the US and Europe working to add security to the respective V2X protocols. Depending on the attackers' capabilities and attack types, a holistic multi-layered security concept is required. For instance, BSMs from external attackers (*e.g.*, roadside attackers with V2X radio) will be discarded immediately due to lack of valid credentials to join the BSM broadcast. In contrast, internal attackers (*e.g.*, compromised ECUs) are "real" vehicles that are authenticated to exchange BSMs with their surrounding vehicles and other entities. They can launch a variety of attacks, such as Denial-of-Service (DoS), Sybil, replay, or false data injection. Compared to these three attack types which are all of adversarial nature, false data broadcast can also be caused by faulty sensors in non-malicious vehicles. This can be achieved through a compromised in-vehicle network or a malicious On-Board Unit (OBU) — the vehicle's external interface responsible for V2X communication.

5G networks are typically software defined networks (SDN) and are distributed to the edge to gain advantages such as decreased latency and improved reliability. As an SDN, there exists a common controller that is accessed by APIs from the network edge. In previous generations of wireless communications, there was limited software-based exposure to the control plane. By creating an SDN architecture, the attack surface for a Denial of Service (DoS) attack has been extended to the edge of the network, making monitoring and management more difficult. DoS attacks against a 5G network, VANETs, or any V2X communication compromise system availability of CAVs. Such attacks may be mitigated by insuring a secure trust management methodology.

Researchers in [18] proposed a DoS exploit against a group of vehicles equipped with Cooperative Adaptive Cruise Control (CACC) and connected via DSRC. The attack involves flooding the inter-vehicle network with excess packets, leading to delayed or dropped communication of relative vehicle position. This exploit could lead to collisions due to inaccurate distance data. In addition to DoS attacks on the inter-vehicle network, similar exploits can be used to compromise the vehicle's onboard network. For instance, the Toyota Global TechStream system is vulnerable to DoS attack and subsequent arbitrary code execution, where the Global TechStream is a maintenance system used by Toyota dealers and third-party vendors.

Message forgery attacks refer to vehicles using V2X communications and receive a "forged" message that informs that vehicle to perform actions with malicious intent, which can cause the vehicle to make a dangerous decision that injures an occupant or bystander [19]. Bad-mouthing, conflicting behavior, blackhole and sybil attacks all exploit poor trust management solutions to gaining access to vehicle communication systems. Inconsistent trust management practices and systems are often the root of attacks against the wireless communications and protocols involved in CAVs.

Finally, attacks on traffic infrastructure are increasing as a result of the proliferation of Vehicle-to-Infrastructure (V2I) communication. Roadside units (RSUs) are commonly used to interact with BSMs broadcast by CAVs to optimize traffic conditions. For instance, the Intelligent Traffic Signal System (I-SIG) uses real-time vehicle trajectory data transmitted from CAVs via DSRC to perform more effective traffic signal control in an intersection. Recent work [20] has shown that I-SIG is highly vulnerable to data spoofing attacks, effectively reversing the benefits of a CAV-based signal control system.

V. Threats to Vehicle User Data

CAV data privacy is a novel field that is receiving more attention due to the rise of telematics as part of increasingly connected vehicles and recent regulations (General Data Protection Regulation in the EU). Large amounts of data are being generated in CAVs which can then be shared with carmakers and third-parties. This is mainly driven by monetization opportunities for carmakers. CAV users have an expectation of a secure and private use of the services that enable a safe experience, so they deserve an awareness that their vehicle is a hyper-connected IoT (Internet of Things) platform. In addition to the customary vulnerabilities of IoT devices, CAV platforms introduce the complexity of mobility and frequent connections with location based services. These services can significantly enhance the usability of the CAV platform, but they also offer numerous opportunities for information leakage and unauthorized activity monitoring. As the complexity of systems advances, it is inevitable to increase the size of the data generated and processed. There is an inherent limitation to the computational power of an on-board processor, and there are a variety of strategies for distributing or relocating the heavier tasks either to an edge computer or a vehicular Cloud. In either case, there are a host of privacy implications related to the origin of the data, and the potential for an unauthorized party to use the disparate information to calculate or extract features that may expose Personally Identifiable Information (PII).

As CAV becomes part of the IoT ecosystem, in-vehicle network data (*e.g.*, vehicle performance data, driver's behavior data, location data) are transferred to multiple stakeholders such as car manufacturers and insurance companies for diagnostic and forensics purposes. However, sharing CAV data may raise privacy concerns.

Recent research has shown that vehicular sensor data is rich in PII [21]. It is possible to infer the driver's identity using in-vehicle network data, such as the vehicle speed, and steering wheel angle. Kar *et al.* [22] shown that drivers can be distinguished using only pre-trip vehicle sensor data from the CAN bus with high accuracy. Remeli *et al.* [23] demonstrated the feasibility of driver re-identification using the in-vehicle network data from the CAN messages by using off-the-shelf machine learning techniques without reverse-engineering the CAN protocol. Furthermore, Pesé [24] discussed privacy issues in Android Automotive that can be leverages as part of a third-generation attack which was discussed in Sec. III. To prevent from PII leakage by unauthorized parties, privacy-preserving schemes (*e.g.*, by applying differential privacy techniques) are needed for sharing in-vehicle network data to third-parties.

VI. Threats to Vehicle Access Control Systems

Modern automobiles' security architecture isn't complete without access control systems for vehicles, which play a critical role in avoiding theft by prohibiting unauthorized access. In the world of connected and autonomous vehicles (CAVs), these systems' dynamics have undergone a significant transformation. Vehicle access control systems have evolved to include complex digital solutions after being historically dominated by mechanical locks. These options include smartphone-based digital keys that are incorporated through specialized software, electronic key fobs, smart keys, and increasingly, smart keys.

These improvements in access control systems have produced a wide range of advantages that considerably improve the usability and convenience of vehicle operation. They enable drivers to remotely unlock, start, and even pre-condition their automobiles, expanding the range of control over vehicle operation. The user experience is further improved by these systems' introduction of cutting-edge features like customized driver profiles.

In spite of the fact that they provide better functionality as we move into the digital age, these advanced technologies also pose possible security risks. Additional vectors of attack that bad actors may be able to use are introduced with each new feature and degree of complexity. These systems use radio frequencies for key fobs and Bluetooth or NFC for smartphone keys, however the communication channels they use are vulnerable to assaults including jamming, signal interception, and relay attacks.

Additionally, these systems' software components introduce a further level of risk. Software flaws might be used to get around access restrictions, change how the car works, or even take full control of it. These systems, especially smartphone-based digital keys, are frequently connected with other car systems, which increases the risk because a breach might possibly give access to sensitive user data or crucial vehicle control systems.

In the following subsections, we survey attacks on three categories of vehicle access control systems.

A. Active Key Entry Attacks

Active key entry systems require user interaction, such as pressing a button, to lock or unlock the vehicle. Traditional remote key fobs fall into this category. The key fob sends a signal to the vehicle's receiver, initiating the locking or unlocking action. Despite being user-friendly, this communication method is inherently vulnerable to attacks known as relay attacks.

An attacker utilizes two specialized devices in a relay attack; one is positioned close to the key fob to pick up its signal, and the other is placed close to the vehicle to relay this signal. The attacker can unlock and possibly start the vehicle without really having the key since the vehicle is tricked into thinking the key fob is closer than it actually is [25]. The technology needed to carry out these attacks has also gotten easier to get. Relay devices may now be bought online by would-be attackers, lowering the entry barrier and raising the frequency of these attacks. Some even use software-defined radio (SDR) devices, which may be configured to mimic a variety of wireless devices, including key fobs.

Automobile makers and security specialists are looking into a number of solutions in response to these dangers. One such

technique entails using a distance bounding protocol, in which the car measures the amount of time it takes a signal to go from the key fob to the car and back, allowing it to calculate how close the key is to the door [26].

Relay attacks exploit the lack of replay protection in active key fob communication. Modern active systems commonly incorporate rolling codes, which significantly enhance security. Rolling codes generate unique and non-repeating codes each time the key fob is used, making it difficult for attackers to intercept and replay the transmitted code.

B. Passive Key Entry System Attacks

Passive key entry systems, also known as keyless entry systems or proximity-based systems, enable users to unlock or lock the vehicle without actively pressing a button on the key fob. Instead, they rely on the proximity of the key fob to the vehicle. As long as the key fob is within a certain range, usually a few feet or meters, the vehicle's sensors detect its presence and allow access to the vehicle. Despite their sophistication and convenience-enhancing features, keyless entry systems, which have increasingly become standard equipment in contemporary cars, are not immune from security vulnerabilities. For instance, relay attacks as discussed in previous subsection also apply to keyless entry systems. Advanced passive systems may utilize challenge-response authentication methods, where the vehicle and key fob exchange unique cryptographic challenges and responses to validate their authenticity and prevent relay attacks.

However, attackers have taken advantage of cryptographic flaws in keyless entry systems, and with the correct technological know-how, they are able to crack these methods to imitate the signals of the original key fob and get access without authorization [27], [28]. Such violations may result in unauthorised access and even possible car theft, which can have serious repercussions.

Jamming assaults, in which the attacker sends out radio signals at the same frequency as the key fob, have also interfered with the signal sent by the key fob. This interferes with the key fob's ability to communicate with the car, leaving it unable to receive the lock order and vulnerable to intrusion [29].

C. Smartphone Digital Key Attacks

Digital keys can be used for mobile key entry that enables users to use a smartphone application to unlock, start, and operate their vehicles. They not only provide a degree of functionality and convenience never before seen, but they also pose special security risks. Several carmakers are using digital keys for their cars [30]. Typically, a mobile companion app developed by the carmaker is provided on the smartphone that communicated with both the vehicle, as well as the carmaker's backend.

Due to their vulnerability to malware and other intrusions, smartphones have become a top target for attackers looking to obtain unauthorized access to automobiles. Since smartphone digital keys frequently communicate with the car through Bluetooth or Near Field Communication (NFC), it is possible to take advantage of these communication pathways to take over the vehicle. For instance, a man-in-the-middle attack, in which the communication between the smartphone and the vehicle is intercepted and modified, may be attempted by attackers. Carmakers expect that the deployment of Ultra-Wideband (UWB) technology for digital key entry will provide an additional layer of security due to precise and fine-grained localization of the smartphone relative to the vehicle. This countermeasure can easily thwart relay attacks.

Besides attacking the communication channel, the digital key app could be compromised by malware on the smartphone, either by modifying the app's features or collecting user credentials. Another issue is phishing attempts, which fool the user into revealing their login information. A potential attacker who gains access to the digital key app may be able to unlock the car, start the engine, or even track the location of the vehicle. Security solutions including robust app security, end-to-end encryption of communication channels, and two-factor authentication can be used to reduce these threats.

VII. Conclusion

In this paper, we provided an in-depth overview of the state of security and privacy in connected and autonomous vehicles (CAVs). We proposed a taxonomy for classification of threats to CAV based on different attack surfaces, and use it to examine, categorize, and discuss the representative vulnerabilities and mitigation strategies.

Though the focus of this work are CAVs, many of the physical systems, vehicle controls, and electronics in CAVs are still similar to traditional operator-driven cars. Therefore, some of the threat surfaces that we will see in CAVs have already been identified in existing cars. Many of the new vulnerabilities of CAVs are related to the fact that a CAV is essentially a giant, rolling conglomerate of IoT devices, each with its own potential for design vulnerability, misconfiguration, and misuse by the end user. The complexity of the interconnected onboard systems is daunting, but when we combine a constantly moving platform with continuously rolling connections to untrusted devices in the surrounding infrastructure, the threat level is quite extraordinary.

Authentication is an essential requirement in CAVs, as it prevents unauthorized access to CAV systems and supporting infrastructure. In order for a CAV to function properly and ensure the safety of occupants, the network and the components connected to it must be able to function even in the midst of a malicious attack. In this context, the Zero Trust Architecture (ZTA) offers a fundamental way of approaching CAV security.

In conclusion, the rapid technological development of CAVs emphasizes the significance of ongoing vigilance, research, and innovation in the field of vehicle cybersecurity. It is a difficult and ongoing task to strike a balance between the growth of technology and the maintenance of privacy and safety. However, by carefully navigating this complex environment and thinking strategically, we may help to realize a secure, effective, and safe future of transportation.

REFERENCES

[1] André de Lima Salgado, Ben Singh, Patrick C. K. Hung, Annie Jiang, Yen-Hung Liu, Anna Priscilla de Albuquerque Wheler, and Hossam A. Gaber. Preliminary tendencies of users' expectations about privacy on connected-autonomous vehicles. In *2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, page 296–301, Oct 2020.

[2] Kui Ren, Qian Wang, Cong Wang, Zhan Qin, and Xiaodong Lin. The security of autonomous driving: Threats, defenses, and future directions. *Proceedings of the IEEE*, 108(2):357–372, Feb 2020.

[3] Junjie Shen, Jun Yeon Won, Zeyuan Chen, and Qi Alfred Chen. Drift with devil: Security of multi-sensor fusion based localization in high-level autonomous driving under gps spoofing. In *Proceedings of the 29th USENIX Conference on Security Symposium (SEC)*, 2020.

[4] Mohammad Reza Mosavi, Matin Pashaian, Mohammad Javad Rezaei, and Karim Mohammadi. Jamming mitigation in global positioning system receivers using wavelet packet coefficients thresholding. *IET Signal Processing*, 9(5):457–464, 2015.

[5] Yulong Cao, Chaowei Xiao, Benjamin Cyr, Yimeng Zhou, Won Park, Sara Rampazzi, Qi Alfred Chen, Kevin Fu, and Z. Morley Mao. Adversarial sensor attack on lidar-based perception in autonomous driving. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, CCS '19, page 2267–2281. Association for Computing Machinery, Nov 2019.

[6] Takami Sato, Junjie Shen, Ningfei Wang, Yunhan Jia, Xue Lin, and Qi Alfred Chen. Dirty road can attack: Security of deep learning based automated lane centering under physical-world attack. page 19.

[7] Xiaoyu Ji, Yushi Cheng, Yuepeng Zhang, Kai Wang, Chen Yan, Wenyuan Xu, and Kevin Fu. Poltergeist: Acoustic adversarial machine learning against cameras and computer vision. In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 160–175. IEEE, 2021.

[8] Jonathan Petit and Steven E. Shladover. Potential cyberattacks on automated vehicles. *IEEE Transactions on Intelligent Transportation Systems*, 16(2):546–556, Apr 2015.

[9] Timothy Trippel, Ofir Weisse, Wenyuan Xu, Peter Honeyman, and Kevin Fu. Walnut: Waging doubt on the integrity of mems accelerometers with acoustic injection attacks. In *2017 IEEE European symposium on security and privacy (EuroS&P)*, pages 3–18. IEEE, 2017.

[10] Wenyuan Xu, Chen Yan, Weibin Jia, Xiaoyu Ji, and Jianhao Liu. Analyzing and enhancing the security of ultrasonic sensors for autonomous vehicles. *IEEE Internet of Things Journal*, 5(6):5015–5029, Dec 2018.

[11] Mert D Pesé, Jay W Schauer, Junhui Li, and Kang G Shin. S2-can: Sufficiently secure controller area network. In *Annual Computer Security Applications Conference*, pages 425–438, 2021.

[12] Mert Dieter Pese. *Bringing Practical Security to Vehicles*. PhD thesis, 2022.

[13] Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel, Tadayoshi Kohno, Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, et al. Experimental security analysis of a modern automobile. In *2010 IEEE symposium on security and privacy*, pages 447–462. IEEE, 2010.

[14] Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham, Stefan Savage, Karl Koscher, Alexei Czeskis, Franziska Roesner, and Tadayoshi Kohno. Comprehensive experimental analyses of automotive attack surfaces. page 16.

[15] Autosar specification of module secure onboard communication, 2022. https://www.autosar.org/fileadmin/user_upload/standards/classic/4-2/AUTOSAR_SWS_SecureOnboardCommunication.pdf.

[16] Charlie Miller and Chris Valasek. Remote exploitation of an unaltered passenger vehicle. *Black Hat USA*, 2015(S 91), 2015.

[17] Mert Pese, Kang Shin, Josiah Bruner, and Amy Chu. Security analysis of android automotive. *SAE International Journal of Advances and Current Practices in Mobility*, 2(2020-01-1295):2337–2346, 2020.

[18] Zoliekha Abdollahi Biron, Satadru Dey, and Pierluigi Pisu. Resilient control strategy under denial of service in connected vehicles. In *2017 American Control Conference (ACC)*, page 4971–4976, May 2017.

[19] Rongxing Lu, Lan Zhang, Jianbing Ni, and Yuguang Fang. 5g vehicle-to-everything services: Gearing up for security and privacy. *Proceedings of the IEEE*, 2020.

[20] Qi Alfred Chen, Yucheng Yin, Yiheng Feng, Z Morley Mao, and Henry X Liu. Exposing congestion attack on emerging connected vehicle based traffic signal control.

[21] Mert D Pesé and Kang G Shin. Survey of automotive privacy regulations and privacy-related attacks. 2019.

[22] Gorkem Kar, Shubham Jain, Marco Gruteser, Jinzhu Chen, Fan Bai, and Ramesh Govindan. Predriveid: Pre-trip driver identification from in-vehicle data. In *Proceedings of the Second ACM/IEEE Symposium on Edge Computing (SEC)*, 2017.

[23] Mina Remeli, Szilvia Lestyán, Gergely Acs, and Gergely Biczók. Automatic driver identification from in-vehicle network logs. In *2019 IEEE Intelligent Transportation Systems Conference (ITSC)*, page 1150–1157, 2019.

[24] Mert D Pese. A first look at android automotive privacy. Technical report, SAE Technical Paper, 2023.

[25] Aurélien Francillon, Boris Danev, and Srdjan Capkun. Relay attacks on passive keyless entry and start systems in modern cars. *IACR Cryptology ePrint Archive*, 2010:332, 01 2010.

[26] Tao Yang, Lingbo Kong, Wei Xin, Jianbin Hu, and Zhong Chen. Resisting relay attacks on vehicular passive keyless entry and start systems. In *2012 9th International Conference on Fuzzy Systems and Knowledge Discovery*, pages 2232–2236, May 2012.

[27] Flavio D. Garcia, David Oswald, Timo Kasper, and Pierre Pavlidès. Lock it and still lose it —on the (In)Security of automotive remote keyless entry systems. In *25th USENIX Security Symposium (USENIX Security 16)*, Austin, TX, August 2016. USENIX Association.

[28] The Brussels Times. Researchers hack a tesla model x in minutes. https://www.brusselstimes.com/142131/belgian-researchers-hack-a-tesla-model-x-in-minutes-ku-leuven-cosic-imec-bleutooth-

[29] Roel Verdult, Flavio Garcia, and Josep Balasch. Gone in 360 seconds: Hijacking with hitag2. pages 237–252, 01 2012.

[30] Cars that use digital keys in 2023. https://www.kbb.com/car-advice/vehicles-using-digital-keys/, journal=Cars that use digital keys - kelley blue book.