From Mechanical Lock-Picking to Autonomous Driving Deception: A Comprehensive Review of Vehicle Attacks, Cyberattacks, and Defenses

Karim Lounis
Intelligent Software Systems Security group
Department of Intelligent Systems Engineering
The National School of Artificial Intelligence
Sidi AbdAllah, Algiers, Algeria
karim.lounis@ensia.edu.dz

***Abstract*—Modern vehicles have evolved into highly interconnected Software-Defined Cyber-Physical Systems (CPS), integrating embedded electronics, wireless communications, artificial intelligence, and Advanced Driver Assistance Systems (ADAS). While these technological advances have significantly improved vehicle safety, efficiency, and driving automation, they have also introduced a rapidly expanding cyber-physical attack surface. Consequently, automotive cybersecurity has become an active research area encompassing attacks on physical vehicle components, access and authentication mechanisms, electronic and software systems, and autonomous driving technologies. Although numerous studies and surveys have investigated these security threats, the existing literature remains fragmented, often focusing on specific vehicle subsystems or individual technologies. This paper presents a comprehensive survey of attacks and defense mechanisms targeting modern vehicles through a unified and orthogonal taxonomy that classifies the literature into four research directions: attacks on vehicle body and physical systems, vehicle access and engine start systems, electronic and software systems, and ADAS and autonomous driving systems. For each direction, the associated security issues, representative attacks, and existing countermeasures are systematically reviewed and analyzed. Furthermore, the survey identifies current research trends, highlights existing research gaps, and discusses future challenges toward the development of comprehensive and resilient automotive security solutions.**

***Index Terms*—Vehicle security, Automotive cybersecurity, Cyber-Physical Systems, Software-Defined Vehicles, Vehicle Attacks, Advanced Driver Assistance Systems Security, Autonomous Vehicle Security, ECU Security, CAN Bus Security, Security Taxonomy, Artificial intelligence, Vehicle Theft, Survey.**

I. Introduction

OVER the past century, the automotive industry has undergone a radical paradigm shift (viz., Fig. 1). Passenger vehicles, once defined primarily by internal combustion engines, mechanical linkages, and closed-loop hydraulic systems, have evolved into highly sophisticated Cyber-Physical Systems (CPS) [1]. Bruce Scheneir once said "A car is a hundred plus computer distributed system with four wheels and an engine" [2]. In fact, modern Software-Defined Vehicles (SDVs) function as distributed computing platforms on wheels, integrating more than one hundred Electronic Control Units (ECUs), hundreds of millions of lines of software code, and numerous wired and wireless communication interfaces [3], including Cellular Vehicle-to-Everything (C-V2X), Wi-Fi, Bluetooth, and Global Navigation Satellite Systems (GNSS). This technological transformation has significantly enhanced vehicle performance, fuel efficiency, occupant safety, and driver convenience, culminating in Advanced Driver Assistance Systems (ADAS)[1] and increasingly autonomous driving capabilities [4]–[6]. Nevertheless, these advances have also dramatically expanded the vehicle attack surface. Whereas vehicle theft once required physical proximity and mechanical expertise [9]–[44] attackers can now exploit security vulnerabilities in software [148]–[154], wireless communication interfaces and protocols [16]–[18], and intelligent sensing systems [119]–[121] to remotely compromise safety-critical functions such as steering, braking, airbags deploying, seatbelt pretensioners, electronic stability control, and acceleration [7].

Interestingly, improvements in automotive security have fundamentally changed the nature of vehicle-related intentional security threats (i.e., attacks). Historical analyses attribute the substantial decline in vehicle theft over recent decades to the widespread adoption of modern security technologies, particularly electronic engine immobilizers introduced in the late 1980s [10]–[14]. Their integration contributed to an estimated 80% reduction in vehicle theft in the United States of between 1990 and 2020 [8], with newer vehicles equipped with secure immobilization technologies exhibiting significantly lower theft rates than earlier models. While these technologies have made modern vehicles considerably more resilient against traditional physical attacks [27]–[37] while reducing vehicle-related crime rate [23], they have simultaneously accelerated the transition toward cyber-enabled attacks that exploit the growing dependence on electronics [194]–

[1]ADAS (Advanced Driver Assistance Systems) are electronic systems that assist drivers by combining sensors, perception algorithms, and control mechanisms to improve vehicle safety and driving convenience through functions such as lane keeping, adaptive cruise control, automatic emergency braking, parking assistance, and self-driving (autopilot).

[199], software [132], wireless connectivity [130], and intelligent perception systems [120]–[122].

A. Vehicle Security

The automotive security threat landscape has expanded far beyond conventional theft and physical tampering [9]–[15]. Contemporary attackers increasingly target keyless entry systems through relay [104]–[115] and replay attacks [87]–[91], exploit security vulnerabilities in infotainment platforms [16]–[18] and wireless interfaces [16]–[18], abuse diagnostic ports (e.g., OBD-II and J1939) [176]–[178] and in-vehicle networks to gain unauthorized access to Electronic Control Units (ECUs) [16]–[19], and manipulate Controller Area Network (CAN) communications to influence vehicle behavior [194]–[199]. More recently, the incorporation of artificial intelligence into autonomous driving systems has introduced an entirely new class of cyber-physical attacks [119]–[121]. Rather than compromising software directly, attacker can deceive perception algorithms [120]–[122] by manipulating the vehicle's physical environment through adversarial traffic signs, projected pedestrians, spoofed obstacles, or by compromising the advanced driver assistant system (ADAS) components, such as cameras, light detection and ranging (LiDAR), radio detection and ranging (RADAR), global positioning system (GPS), or ultrasonic acoustic sensors [124]–[128]. As a result, modern vehicles are no longer threatened solely by attacks against their electronic infrastructure but also by attacks targeting the integrity of their perception and decision-making processes.

The rapid diversification of attack vectors has been accompanied by an equally diverse body of automotive cybersecurity research. Existing studies investigate a broad spectrum of security issues, ranging from vehicle theft and physical sabotage [31]–[35] to wireless authentication [161]–[163], embedded software security [148]–[154], in-vehicle communication protocols [166]–[170], hardware security [184]–[187], and AI-enabled perception attacks [118]–[123]. Notwithstanding, the literature remains highly fragmented, with most existing surveys concentrating on individual technologies, such as CAN bus security [156]–[162], keyless entry systems [100]–[116], over-the-air software updates [148]–[154], or autonomous driving security [132]–[137], rather than providing a holistic perspective of the vehicle as an integrated cyber-physical system. Consequently, attack classifications often overlap, making it difficult to compare research efforts, identify emerging trends, or determine which areas have received relatively little attention. This fragmentation hinders the development of a unified understanding of the automotive threat landscape and complicates the identification of research gaps that warrant further investigation.

B. Motivation and Objectives

To address this limitation, there is a clear need for a comprehensive and orthogonal taxonomy that organizes the existing literature according to the primary subsystem under attack. Such a classification minimizes overlaps between categories while collectively covering the complete vehicle attack surface, thereby providing a unified framework for reviewing security issues, attack techniques, and corresponding defense mechanisms. More importantly, an orthogonal taxonomy facilitates the identification of mature research domains, reveals underexplored areas requiring further investigation, and highlights opportunities for developing integrated defense strategies that protect multiple vehicle subsystems rather than isolated technologies.

Motivated by these observations, this survey classifies the existing literature into four orthogonal research directions: (1) attacks on vehicle body and physical systems, (2) attacks on vehicle access and engine start systems, (3) attacks on electronic and software systems, and (4) attacks on ADAS and autonomous driving systems. Unlike many existing surveys that additionally consider connected-vehicle infrastructures, such as V2X (Vehicle to Everything) communications and intelligent transportation systems, this work deliberately focuses on attacks targeting the vehicle itself as a standalone cyber-physical system. For each research direction, the survey identifies the associated security issues, categorizes attacks according to the compromised security service, reviews representative countermeasures, and discusses open challenges and future research opportunities.

C. Contributions

While several existing surveys focus exclusively on legacy physical theft or strictly on internal CAN (Controller Area Network) bus security vulnerabilities, this paper bridges the gap between historical automotive theft vectors, in-vehicle attacks, keyless attacks, and modern ADAS/Autonomous Vehicle (AV) cyber-physical attacks. Therefore, the primary contributions of this paper are summarized as follows:

- **An Orthogonal Taxonomy of Vehicle Attacks.** We propose a comprehensive and orthogonal taxonomy that classifies attacks targeting modern vehicles into four major research directions: attacks on vehicle body and physical systems, attacks on vehicle access and engine start systems, attacks on electronic and software systems, and attacks on ADAS and autonomous driving systems. The proposed taxonomy provides a unified framework for organizing the automotive cybersecurity literature while minimizing overlaps between research domains.
- **A Comprehensive Survey of Automotive Attacks.** Following the proposed taxonomy, we review and categorize the existing literature on vehicle attacks, covering conventional physical threats, wireless and authentication attacks, software and in-vehicle network attacks, as well as adversarial attacks targeting autonomous driving technologies. For each research direction, the surveyed attacks are further classified according to the underlying security issues and the compromised security services.
- **A Systematic Review of Defense Mechanisms.** For every category of attacks, we analyze the defense mechanisms proposed in the literature, including preventive,



Fig. 1. From left to right: A mid-1920s black Dodge Brothers Sedan (produced around 1924–1926); a 2020 hybrid (i.e., equiped with an electric and combustion engine) red Toyota Camery; and a 2026 fully electric white Jaguar I-PACE SUV (self-driving RoboTaxi vehicle).

detective, and corrective security solutions. Their effectiveness, advantages, and limitations are discussed to provide a comprehensive understanding of the current state of automotive security.

- **Identification of Research Trends and Future Challenges.** Based on the surveyed literature, we identify emerging research trends, highlight existing gaps and underexplored areas, and discuss future research directions toward the development of comprehensive and resilient security architectures for next-generation software-defined and autonomous vehicles.

By providing a unified taxonomy together with a comprehensive review of attacks, countermeasures, and open research challenges, this survey offers researchers and practitioners a structured reference for understanding the evolving automotive threat landscape and for guiding future research in vehicle cybersecurity.

D. Paper Organization

The remainder of the paper is organized as follows. In Section II, we discuss the general related work. In Section III, we propose a generic taxonomy of attacks on vehicles. Following the proposed taxonomy, in Sections IV, V, VI, and VII, we review the attacks against vehicles and discuss possible countermeasures. Then, in Section VII (Discussions and Perspectives), we analyze the reviewed attacks and countermeasures to identify standing challenges, emerging research trends, and highlight exising gaps and unexplored areas. Finally, we conclude the paper in Section IX.

II. Related Work

The rapid digitalization of modern vehicles has transformed automobiles into highly interconnected cyber-physical systems [1], leading to an equally rapid expansion of automotive cybersecurity research. Existing studies have investigated security threats from multiple perspectives, including physical attacks against the vehicle (e.g., vehicle theft and partial theft) [9]–[15], attacks targeting keyless entry and start systems [100]–[116], electronic and in-vehicle network vulnerabilities [16]–[19], and, more recently, attacks against Advanced Driver Assistance Systems (ADAS) and autonomous driving technologies [132]–[137]. As a result, numerous research work and surveys have attempted to either solve specific challenges or organize this growing body of work by focusing on particular subsystems or application domains. Nonetheless, most existing research work and reviews remain specialized, emphasizing a single aspect of vehicle security while overlooking others, thereby providing only a fragmented view of the overall security threat landscape.

The earliest body of research primarily concentrated on physical vehicle security (i.e., the body part), where vehicles were viewed as tangible assets vulnerable to theft, partial theft, vandalism, tampering, vehicle fraud, and physical manipulation. These studies investigated conventional security issues such as vehicle theft [27]–[37], carjacking [36], vehicle crimes prevention [23], physical assaults [37], counterfeit replacement parts [19], [27], unauthorized physical access, VIN and license plate tampering [15], stolen vehicle recovery [41]–[43], privacy violations through hidden surveillance devices [38], [39], and fraud related to vehicle identity or condition [40]. Researchers also analyzed physical attacks that compromise the fundamental security principles, i.e., authentication, confidentiality, integrity, and availability, while proposing countermeasures ranging from mechanical locks and immobilizers [10]–[14] to biometric authentication [24], digital tachographs [16], electronic licensing systems [16], GPS tracking [42], blockchain-based ownership management [50]–[52], and physical unclonable functions (PUFs) [19]. Although this line of research established the foundation of automotive security, its primary focus remained on protecting the vehicle as a physical object rather than as a complex cyber-physical platform. Throughout the remaining part of this paper, we use the notation **RD1** to refer to this research direction.

As vehicles became increasingly equipped with wireless communication technologies and electronic authentication mechanisms, research shifted toward vehicle access and engine start systems (a.k.a., RKE— Remote Keyless Entry Systems, and PKES— Passive Keyless Entry and Start Systems) [87]–[116]. This direction investigates attacks against keyless entry systems, such as rolling-code protocols [96], relay [104]–[115] and replay attacks [87]–[91], radio frequency (RF) jamming [95]–[97], cryptanalysis of wireless protocols [98],

and various methods for bypassing immobilizers or proximity verification mechanisms [106]–[112]. Consequently, considerable effort has been devoted to developing secure authentication schemes based on cryptography [87]–[89], rolling-code protocols [103], distance-bounding techniques [107]–[109], ultra-wideband (UWB) ranging [110], frequency hopping [105], PUFs [57]–[59], and artificial intelligence-based solutions [113]–[115]. Despite substantial progress, the continuous evolution of relay and wireless attacks demonstrates the persistent challenge of securing increasingly sophisticated vehicle access technologies. Similar to the previous line of research, throughout the remaining part of this paper, we write **RD2** to refer to this research direction.

Furthermore, the introduction of dozens of Electronic Control Units (ECUs), high-speed in-vehicle networks, and software-defined vehicle architectures significantly broadened the attack surface, motivating extensive research on electronic and software security. Existing literature investigates vulnerabilities associated with ECUs, Controller Area Network (CAN) buses, LIN buses, diagnostic interfaces such as OBD-II, over-the-air (OTA) software updates, firmware integrity, communication protocols, and cloud-connected vehicle services. Researchers have demonstrated numerous attacks including CAN message injection [156]–[162], ECU compromise [172]–[175], firmware modification [16]–[18], diagnostic abuse [176]–[178], and software exploitation [148]–[154]. To address these security threats, proposed defenses include secure boot mechanisms [181]–[183], cryptographic authentication [161]–[163], hardware security modules [184]–[187], intrusion detection systems [167]–[170], CAN firewalls [179], software authentication [16]–[18], blockchain-based logging [174], secure architectures [199], honeypots [188]–[190], and Security Operations Centers (SOCs) dedicated to automotive environments [191]. This research direction, which we denote as **RD3** throughout the paper, has become one of the most active areas of automotive cybersecurity due to the increasing software complexity of modern vehicles.

More recently, the emergence of autonomous vehicles has introduced an entirely new research direction focusing on ADAS and autonomous driving systems. Unlike traditional vehicle cybersecurity, this area studies attacks targeting perception, localization, sensor fusion, and decision-making components. Existing works investigate adversarial machine-learning attacks against deep-neural networks [118]–[121], LiDAR [122] spoofing, GPS spoofing [122], ADAS sensors manipulation [120]–[122], object camouflage [129], fabricated traffic signs [119], and perception inconsistencies caused by malicious physical perturbations [119]–[121]. Correspondingly, researchers have proposed numerous countermeasures, including multi-sensor fusion [124]–[126], sensor redundancy [137], perception consistency verification [135], GPS anti-spoofing approaches [122], LiDAR resilience techniques [131], robust deep neural networks [129], adversarial training [138]–[143], AI-based intrusion detection [167]–[170], and V2X-assisted cooperative perception [71]–[80]. The growing reliance on AI has therefore shifted automotive cybersecurity beyond protecting communication protocols toward ensuring trustworthy machine perception and autonomous decision making. Throughout the remaining part of this paper, we denote this research direction by **RD4**.

While these four research directions (i.e., **RD1**, **RD2**, **RD3**, and **RD4**) collectively cover a substantial portion of automotive cybersecurity research, another major branch of the literature focuses on connected-vehicle infrastructures, including Vehicle-to-Everything (V2X), Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), cloud-assisted transportation systems, edge computing, and intelligent transportation networks [71]–[80]. These studies primarily investigate communication security, privacy preservation, trust management, authentication protocols, denial-of-service attacks, blockchain-enabled vehicular networks, and secure cooperative driving. Since these topics concern the security of external communication infrastructures rather than the vehicle itself, they are beyond the scope of this survey. Accordingly, this paper deliberately concentrates on attacks and countermeasures targeting the vehicle as a standalone cyber-physical system, encompassing its physical structure, access mechanisms, electronic and software subsystems, and autonomous driving capabilities.

TABLE I summarizes the aforementioned literature by categorizing existing research according to the four research directions (i.e., **RD1**, **RD2**, **RD3**, and **RD4**), the security issues they address (prefixed by ►), the corresponding attack categories following Stallings' attack classification [200] (prefixed by ♦), and the defense mechanisms (prefixed by ■) that were proposed or discussed in the literature. Stallings' attack classification classifies attacks according to which fundamental security service is compromised, essentially, authentication (fabrication), confidentiality (interception), integrity (modification), and availability (interruption).

III. Attack Classification on Vehicles

Classifying security threats in general, and security attacks, in particular, has always been an effective practice to help security engineers better understand possible security threats and attacks on a given information system. By providing a classification of security threats, one can easily focus on specific types of security threats rather than having a haphazard long list of threats that would require additional efforts to understand and filter threats of one's concern. In this section, we propose a security threats classification for vehicles. The proposed classification is illustrated in Fig. 2. In this classification, there are five classes (four shown in gray rectangles, and one in a red rectangle). The considered classes are briefly defined as follows:

—**Class 1:** Entiteled "Attacks on Vehicles' Body and Physical Systems", covers the various types of attacks where a malicous individual aims to cause harm to the vehicle, the different physical components of the vehicle, and to the possible occupants and passengers of the vehicle. This class alings with research direction **RD1**, defined in the previous section.

TABLE I

SUMMARY OF RELATED WORK WITH RESPECT TO THE FOUR DIFFERENT RESEARCH DIRECTIONS (RDS), COVERED SECURITY ISSUES (►), COVERED ATTACK CLASSES (⧫), AND DISCUSSED/PROPOSED COUNTERMEASURES (■) TO MITIGATE THE DIFFERENT ATTACKS AND CYBERATTACKS ON VEHICLES.

RDs	Security Issues and Attack Categories	Defense Mechanisms (Countermeasures)
RD1	**Vehicle Security Issues** ► Vehicle theft [9]–[15], [20], [21], [23]–[25], [27]–[37], [43], [87] ► Partial vehicle theft [9], [11], [15], [20], [24], [27]–[29], [33], [34], [43] ► Vehicle crimes prevention [10], [15], [20], [23], [29], [35] ► Carjacking [10], [12], [20], [30], [36] ► Vehicle IT Component replacement [16] and counterfeit parts [19], [27] ► Vehicle vandalism and immobilization [26], [37] ► Driver physical authentication [12], [28], [44] ► Theft of vehicle for export [9], [34], [43] ► Stolen vehicle recovery [9], [22], [41]–[43] ► In-vehicle eavesdroping and spying [38], [39] ► Mileage fraud and vehicle physical condition fraud [40] **Attack Category (Stallings')** ⧫ Interception attacks [12], [35], [36], [38], [39] ⧫ Fabrication attacks [9]–[12], [14], [19], [24], [25], [28], [29] ⧫ Modification attacks [11], [14], [16], [29], [40] ⧫ Interruption attacks [10]–[14], [20], [22]–[25], [28]–[37], [43]	■ Central Locking [10] ■ Immobilizers [10]–[14], [16], [23], [27], [29], [31]–[35] ■ Alarm system [10], [11], [27], [29] ■ Tracking devices [10], [12], [25], [30], [41], [42] ■ Steering lock [11], [29] ■ Ignition shut-off switch [11], [27], [29] ■ Fuel valve switch [11], [27], [29] ■ GSM technology (use of SMS to send alerts) [12], [25] ■ Spy Cam technology [12] ■ Vehicle parts labeling and VINs stamping [15] ■ Digital tacograph [16] ■ Electronic licence place [16] ■ PUFs (Physical Unclonable Functions) [19] ■ Law enforcement deployment [21] ■ Recovery location learning [9], [22] ■ Biometric-based systems [24] ■ Blockchain [50]–[52] and Artificial Intelligence [9], [28], [44] ■ Driver, buyer, and passengers awareness [40], [44]
RD2	**Vehicle Security Issues** ► Vehicle access control [16], [24], [87]–[98], [100]–[116] ► Vehicle key security [32], [87]–[98], [100]–[116] ► Keyless entry security [87]–[98], [100]–[103], [105], [106], [108]–[116] ► Relay attack [87], [89], [90], [92], [93], [99], [100], [104]–[115] ► Replay attack [87]–[91], [94], [96]–[98], [102], [103], [105], [112], [115], [116] ► Signal jamming on keyless systems [95]–[97], [103], [105] ► Roll-Jamming and roll-back attack [55], [56], [96], [97], [103], [105] ► Cryptanalysis on keyless algorithms (e.g., Hitag-2) [98] ► Proximity verification [87], [89], [90], [92], [93], [99], [100], [104]–[115], [117] **Attack Category (Stallings')** ⧫ Interception attacks [32], [87]–[100], [102], [103], [105], [107]–[116] ⧫ Fabrication attacks [16], [24], [56], [87]–[94], [97]–[116] ⧫ Modification attacks [88]–[90], [94], [96], [98], [105] ⧫ Interruption attacks [88]–[90], [95]–[97], [103], [105]	■ Keyless systems [16], [87]–[92], [94], [95], [99], [103]–[115] ■ Biometric-based systems [24] ■ Cryptography [87]–[89], [94], [98], [100]–[103], [105] ■ Rolling-code mechanism [94], [103] ■ Driver awareness [32] and digital tacograph [16] ■ Distance-bounding protocols [87], [92], [105], [107]–[109] ■ Ultra-Wideband (UWB) [93], [110] ■ BLE (Bluetooth Low Engergy) [110], [112], [113] and Wi-Fi [113] ■ GPS (Global Positionning System) [112], [113] ■ Traditional locking mechanisms [87]–[91], [94], [105] ■ Timestamping [102] and Coordinate tracing [111] ■ Sound-proximity verification [104] ■ Side-channel leakage [106] and RF-fingerprinting [85], [86], [115] ■ Frequency hopping techniques [105] and RSSI [113] ■ PUFs (Physical Unclonable Functions) [57]–[59] ■ Artificial Intelligence [86], [99], [113]–[115]
RD3	**Vehicle Security Issues** ► Vehicle IT Component replacement [16], [17] ► Vehicle software/firmware update [16]–[18], [26], [81], [132], [148]–[154] ► Vehicle communication interface security [16], [17], [26], [130] ► ECU security [16]–[19], [26], [81], [130], [132], [156]–[159], [171]–[175] ► Diagnostic interface (OBD-II or J1939) security: [81], [82], [176]–[178] ► CAN bus security [56], [81], [130], [132], [156]–[162], [172], [173], [194]–[199] ► LIN bus security [163], [164] and Flexray bus [165] ► Vehicle message security [155], [156], [158], [159] ► OTA (Over The Air) vehicle software update security [148]–[154] **Attack Category (Stallings')**: ⧫ Interception attacks [16], [17], [26], [81], [132], [156], [158], [161], [162] ⧫ Fabrication attacks [16]–[18], [26], [81], [132], [155], [158], [161]–[163], [171] ⧫ Modification attacks [16], [17], [26], [81], [132], [155], [161], [163], [192] ⧫ Interruption attacks [17], [26], [81], [132], [161], [192], [194]	■ Cryptography [16], [26], [155], [156], [159], [161]–[163], [172] ■ PKI (Public Key Infrastructure) [16] ■ Software authentication [16]–[18], [26], [81], [132], [148]–[154] ■ PUFs (Physical Unclonable Functions) [19], [132], [171], [187] ■ IDS (Intrusion Detection Systems) [82], [132], [160], [166]–[170] ■ Physical protection [16], [17], [26], [130] ■ Secure architecture [157], [193], [199] ■ Multi-factor authentication [148] ■ Blockchain technology [154], [174] ■ CAN bus firewalls [179], [180] ■ Secure boot [181]–[183] ■ Quantum cryptography [181], [182] ■ Hardware security [184]–[187], [206] ■ Honeypots [188]–[190] ■ Vehicle Security Operations Center [191] ■ Memory protection [192], [206]
RD4	**Vehicle Security Issues** ► Autonomous vehicle security [120]–[122], [124]–[128], [130], [132]–[137] ► Adversarial attacks [118]–[121], [124]–[127], [129], [132], [134] ► Agentic vehicles (AgVs) security [223], [224] ► Perception attacks [119]–[121], [124]–[128], [130] ► Attacks on ADAS sensors [120]–[122], [124]–[128], [132], [136], [137] ► GPS and LiDAR spoofing in AVs [122], [123], [128], [130], [132] ► Road/Traffic object spoofing [124]–[127], [132] ► Object patching (camouflage) [129], [132] **Attack Category (Stallings'):** ⧫ Interception attacks [39], [132] ⧫ Fabrication attacks [118]–[122], [124]–[126], [128], [129], [131], [132] ⧫ Modification attacks [124]–[126], [128], [129], [132] ⧫ Interruption attacks [124]–[126], [129], [132], [136], [137]	■ Electronic road sign [16] ■ Robust classification methods [119], [124]–[126], [129], [132] ■ Artificial Intelligence [118]–[129], [132], [134] ■ GPS and LiDAR resilience methods [122], [123], [125], [128], [131], [132] ■ GhostBuster (detects phantom projected objects) [124] ■ DSDA (detects displayed, projected, printed objects) [125] ■ PercepGuard (detects object inconsistency, patches) [126] ■ Contextual plausibility checking [126] ■ Multi-Sensor Fusion [124]–[126] ■ Vehicle-to-Everything (V2X) Communication [71]–[80] ■ Anomaly detection in AV [135] ■ Hardware security [184]–[187], [206] and Secure boot [181]–[183] ■ Sensor redundancy [136], [137] ■ Vehicle Security Operations Center [191] ■ Datasets to train perception models [127], [138]–[143]

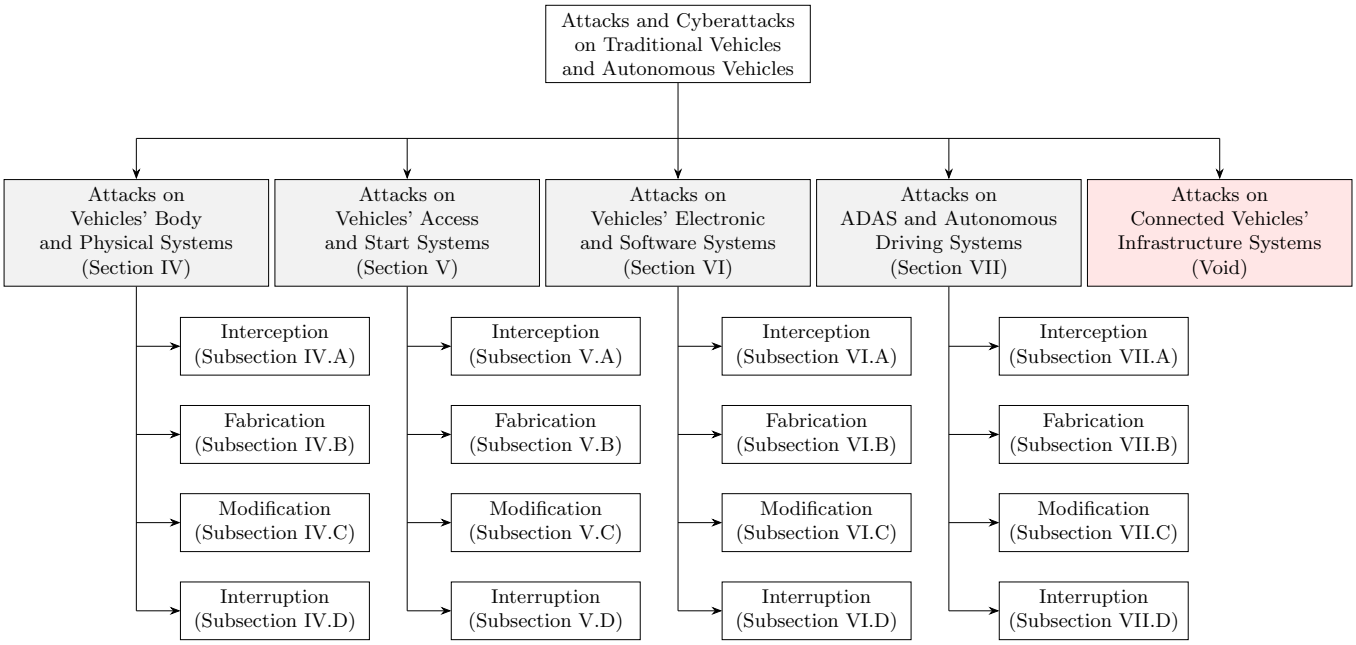

Fig. 2. The comprehensive and orthogonal taxonomy of attacks and cyberattacks on passenger vehicles (traditional and autonomous vehicles). There are five classes (four shown in gray rectangles, and one in a red rectangle). The fifth class is not covered in this paper. Under each class, there are categories of attack scenarios based on which fundamental security service is compromised, i.e., Interception (Confidentiality), Fabrication (Authentication), Modification (Integrity), and Interruption (Availability).

—**Class 2:** Referred to as "Attacks on Vehicles' Access and Start Systems", and it covers the different forms of attack scenarios where a malicous individual aims to bypass any authentication and authorization system of the vehicle to gain access and control over the physical and logical part of the vehicle. . This class alings with research direction **RD2**.

—**Class 3:** Called "Attacks on Vehicles' Electronic and Software Systems". It groups the deversefied types of attack scenarios where a malicous individual aims to hack into the electronic and software part of a vehicle, including the CAN network, the infotaiment system, and any external network interface. . This class alings with research direction **RD3**.

—**Class 4:** This class is entiteled "Attacks on ADAS and Autonomous Driving Systems", and it covers the various types of attacks and cyberattacks where a malicous individual aims to cause harm to the artificial intelligent module of the vehicle that uses various sensors and sensor fusion techniques to process the perceived environmental data and make driving decisions. The goal of the attack is to cause the system to run into misclassifications that lead to serious consequences. . This class alings with research direction **RD4**.

Under each attack class (viz., the gray rectangles in Fig. 2), there are categories of attack scenarios based on which fundamental security service is being compromised, i.e., Interception (Confidentiality), Fabrication (Authentication), Modification (Integrity), and Interruption (Availability)—this is also known as Stallings' attack categorization [200].

The fifth class "Attacks on Connected Vehicles' Infrastrcuture Systems" (viz., the red rectangle in Fig. 2) is not covered in this paper, and is considered outside the main scope of this work (**RD5**). A recent example of such attack category occurred in 2025 in San Francisco, where a tech prankster coordinated 50 concurrent Waymo ride requests to a single residential cul-de-sac. As dozens of Waymo Jaguar I-PACE robotaxis converged on the narrow street simultaneously, their safety sub-routines were triggered; the vehicles' line-of-sight sensors and blind-spot algorithms detected the surrounding fleet as immediate hazards, causing the cars to lock up while attempting turning maneuvers. The resulting self-inflicted spatial paralysis completely blocked access to the street until Waymo was forced to manually geofence and disable service requests within a two-block radius [68]. By exploiting logic flaws in fleet dispatch algorithms rather than hacking onboard vehicle controls, the attack effectively turned legitimate business functionality into a physical weapon of traffic disruption (i.e., a distributed denial of service —DDoS). Fig. 3 illustrates the post which went live on October 12, 2025, claiming that 50 individuals ordered Waymos to the San Francisco's longest dead-end street.

Among other attacks in this direction (i.e., **RD5**), the 2025 Jaguar Land Rover breach [225], likely the most costly cyberattack in British history (an estimated £1.9 billion in economic damage), which compromised enterprise IT systems via social engineering and shut down global production for over a month starting August 31, 2025, with continuing financial fallout for related businesses like dealership group Vertu Motors.



Fig. 3. The post, which went live on October 12, 2025, claims that 50 individuals ordered Waymos to the San Francisco's longest dead-end street [68].

Also, the Q1 2026 telematics provider compromise [226], in which attackers breached the backend systems controlling remote vehicle access and left car owners locked out of their vehicles via the mobile app for up to two weeks. Moreover, the suspected attacks on Russian satellite-enabled immobilizer and alarm-service backends, which left thousands of cars unable to start, pointing to a growing trend of attackers remotely disabling vehicles for ransom [227].

In general, vehicles are subject to two types of security threats, namely, accidental threats and intentional threats. Accidental threats represent the set of threats which are not expected and not involving any intentional parties. It principally targets the physical security of the vehicles, the software technology used within the vehicles, and/or the perceptual and intelligent capabilities in the case of self-driving and autonomous vehicles. It includes software bugs (e.g., misconfiguration, infinite loops, crush bugs, etc), hardware failure (e.g., HDD crash, RAM fails, battery dies, etc), natural hazards (e.g., fires, floods, explosions, etc), and semantic hazards in the case of autonomous vehicles (e.g., A pedestrian wearing a stop-sign-imprinted garment, rear-facing towed vehicle, etc). Intentional threats however, also known as attacks, assume the involvement of an intended party, known as attacker, who undertakes a set of illegal actions to cause harm to the vehicle, or vehicle's passengers. In this paper, we focus on outsider[2] intentional security threats, i.e., attacks and cyberattacks.

[2]Attacks can be classified either as insider or outsider attacks. Insider attacks are generated by a trusted and authorized party within the network (e.g., dishonest employee), whereas outsider attacks are generated by an unauthorized party from outside the network (e.g., a hacker).

For consistency, we use the term "attack" to refer to any deliberate action conducted by a malicious individual (generally, a person) to cause harm to a vehicle (or vehicles) or its owner using classical hardware tools. When the attacker uses information technology resources (e.g., software, SDR, computer, etc) to conduct the attack, we call it a cyberattack.

Additionally, to justify the adoption of Stallings' security service-based classification [200] in this survey, we briefly review the most common attack taxonomies proposed in the literature. Existing fundamental classifications based on attack activity (active/passive) [201], attacker location (internal/external) [202], or protocol layers [203] are often either too broad or tightly coupled to specific technologies or aspect, making them difficult to apply consistently across the diverse automotive ecosystem. By contrast, Stallings' classification organizes attacks according to the compromised fundamental security service, providing a technology-independent and systematic framework that remains applicable across physical, software, communication, and ADAS-related attacks. This makes it particularly well suited to the unified taxonomy proposed in this work.

Moreover, although additional security services have been proposed in the literature—including accountability, non-repudiation, authorization, auditability, trust, trustworthiness, traceability, and anonymity—many of these overlap conceptually with the fundamental security objectives. Incorporating all of them would lead to a taxonomy with significant overlap and limited orthogonality. Therefore, this survey classifies attacks according to the four fundamental security services: authentication, confidentiality, integrity, and availability, as they provide a comprehensive and technology-independent foundation while naturally encompassing many of the remaining security properties.

In the following sections, we present each attack class in detail by reviewing the different attack and cyberattack scenarios while considering their categorization (i.e., based on Fig. 2), and discussing the possible countermeasures and security mechanisms that can be used to mitigtate the attacks or limit the risk and damages caused by some attacks.

IV. Attacks on Vehicles' Body and Physical Systems

In this section, we review the different attacks on vehicles' body and physical systems. We also discuss the possible countermeasures to mitigate or limit the risk of each attack. Also, throughout the paper, all paragraphs that discuss countermeasures for each attack will start by the ■ symbole.

A. Interception Attack and Cyberattack Scenarios

In this category of attacks, we review different attack scenarios where an attacker undertakes actions against the body part of a vehicle and any physical system with an aim to maliciously intercept voice, video footage, biometric elements, or personal belongings, of vehicle owners or passengers.

Hidden Voice Recorder Attack. This attack targets the confidentiality and privacy of vehicle occupants by covertly captur-



Fig. 4. Multi Use RF Camera & Bug Detector from Spycenter Security.

ing conversations inside the cabin without their knowledge or consent (e.g., president, minister, CEO vehicles). To that end, an attacker may discreetly place a miniature recording device under a seat, inside the dashboard, within a door panel, or in other concealed compartments. The device may be installed by a dishonest mechanic during vehicle servicing, an employee at a car wash or detailing center, a trusted acquaintance with temporary access to the vehicle, or simply tossed into the cabin through an open window, open sunroof, or unlocked door. Modern digital voice recorders can operate for days or even weeks on a single battery charge and often feature voice-activated recording to maximize storage and battery life. The records could also be transmitted to the attacker in real-time through the cellular network. The recorded conversations may reveal sensitive personal, financial, or business information, posing significant privacy and security risks to the vehicle's occupants and their resources (e.g., company).

■ Protecting against this attack requires both preventive measures and periodic inspections. Vehicle owners should minimize unauthorized access to their vehicles by using trusted repair facilities, supervising maintenance whenever possible, and locking the vehicle when unattended. Regular inspections of the cabin, including under seats, inside storage compartments, and around dashboard panels, can help detect unfamiliar electronic devices. For high-value targets or organizations handling confidential information, periodic electronic sweeps using RF (Radio Frequency) detectors or specialized bug detection equipment (viz., Detector[3] in Fig. 4) may identify wireless recording or transmitting devices, although offline recorders require thorough physical inspection. Furthermore, tamper-evident seals on interior panels, in-cabin surveillance systems, and access logging during servicing can further reduce the likelihood of covert device installation. Employee background checks and security policies are also important for fleet operators and organizations managing sensitive vehicles.

Hidden Visual Recording Attack. This aims to secretly capture images or videos of vehicle occupants and their activities without their knowledge or consent. An attacker may conceal a miniature camera inside the cabin by integrating it into air vents, decorative panels, USB chargers, tissue boxes, dashboard accessories, or other inconspicuous objects (viz., Fig. 5-left). The device may be deliberately placed inside the vehicle while it is unattended. Modern spy cameras are compact, battery powered, and may record continuously or activate automatically upon detecting motion. The captured footage can reveal the occupants' identities, conversations through lip reading, personal belongings, confidential documents, security credentials, or travel habits. Such information may subsequently be exploited for blackmail, corporate espionage, identity theft, targeted surveillance, or planning future criminal activities.

■ Similar to the previous attack, physical access to the vehicle must be restricted to only authorized and trusted individuals along with regular inspections of the passenger compartment. Vehicle owners should use trusted maintenance providers, supervise servicing whenever practical, and verify that no unfamiliar electronic accessories or objects have been introduced into the cabin. Routine inspections should focus on common concealment locations, including air vents, dashboard panels, USB adapters, charging devices, rear-view mirrors, and decorative accessories. For individuals handling sensitive information, periodic technical surveillance countermeasure (TSCM) inspections or electronic sweeps using optical lens detectors and RF detection equipment (e.g., device shown in Fig. 4) may help identify covert cameras that actively transmit data. Parking in secure, monitored locations and removing confidential documents or sensitive materials from the vehicle further reduce the value of any unauthorized visual recording. Together, these measures significantly reduce the risk of covert visual surveillance and the unauthorized disclosure of private, condifential, secret, or top-secret information.

Hidden GPS Tracker Attack. This attack aims to monitor a vehicle's movements continuously and determine the real-time or historical locations visited by the driver and passengers. An attacker may secretly attach a compact GPS (Global Positioning System) tracking device underneath the vehicle (viz., Fig. 5-middle), inside the bumper, within a wheel well, under a seat, or in another concealed location. The tracker can be installed by a dishonest mechanic, an employee at a car wash or parking facility, a former partner, a stalker, or any individual who gains temporary physical access to the vehicle. Many modern trackers use cellular networks to transmit location data remotely, allowing the attacker to observe routes, parking locations, travel schedules, and frequently visited places from a smartphone or computer. Such information can be exploited for stalking, burglary planning when the owner is away from home, corporate espionage, or other malicious activities. Because these devices are small, battery powered, and often magnetically attached, they may remain undetected for extended periods.

■ Preventing this attack equires controlling physical access to the vehicle and conducting periodic inspections. Vehicle owners should lock the vehicle when unattended and use reputable maintenance and parking services to reduce opportunities for covert device installation. Regular visual and tactile

[3]Spycenter Security Multi-Use RF Bug Detector: https://spycentre.com



Fig. 5. From left to right: A hidden camera in a tissue holder car visor, a GPS tracker sticked under the vehicle, and a tailgating attack where malicious individuals follow a target vehicle to steal the vehicle, or learn information about the passengers .

inspections of the undercarriage, wheel wells, bumpers, and interior compartments can help identify unfamiliar objects or magnetic attachments. For individuals at elevated risk, specialized GPS bug detectors or RF scanners (e.g., device shown in Fig. 4) may assist in detecting active transmitting devices. In some sensitive situations, they could operate GPS spoofing device to broadcast fake random locations around, fooling the tracker to deliver incorrect locations. Also, they could use GPS jammers to disrupt the attacker's GPS tracker if there were any. Moreover, secure parking areas with surveillance cameras can deter unauthorized access.

Vehicle Tailgating Attack. This attack occurs when an adversary physically follows a target vehicle—either closely (viz., Fig. 5-right) or via a coordinated multi-vehicle surveillance team—to perform intelligence gathering or prepare for a secondary physical attack. Unlike digital or network-based attacks, this physical vector leverages visual tracking, license plate reader systems, or temporary covert GPS trackers placed on the chassis. The attacker follows the target to map daily routines, determine high-value destinations (such as home residences, workplaces, or family locations), or stage a physical ambush. In high-threat scenarios, tailgating enables opportunists or coordinated threat actors to execute follow-home robberies, carjackings at isolated choke points (e.g., residential driveways or parking garages), or targeted vehicle/component theft (e.g., catalytic converters or specialized ECU modules). It is worth noting that vehicle tailgating could also happen from the front. The attacker may follow the target vehicle by observing the turn signals and driving directions.

■ Mitigating this attack requires integrating active situational awareness, surveillance detection routes (SDRs), and physical access control boundaries. Drivers employ anti-surveillance driving techniques—such as altering daily commute routes, changing lanes unpredictably, or making a series of four consecutive turns—to confirm if a suspicious trailing vehicle is actively tracking them. If trailing surveillance is confirmed, targets avoid driving to private residences or isolated areas, instead redirecting toward secure, well-lit public zones or law enforcement facilities while contacting emergency services. On an infrastructure level, residential gated communities and corporate parking garages deploy automatic license plate recognition (ALPR) cameras, anti-tailgating vehicle barriers (such as fast-acting speed gates or bollards), and CCTV (Closed-Circuit Television) monitoring to prevent unauthorized vehicles from slipping through perimeter checkpoints. Additionally, periodic physical vehicle sweeps for unauthorized tracking hardware help counter passive, long-term vehicular surveillance.

Forensic Evidence Collection Attack. This targets the physical traces unintentionally left by vehicle occupants to obtain sensitive personal information or facilitate subsequent malicious activities. An attacker with temporary access to the vehicle may deliberately collect latent fingerprints from door handles, windows, the steering wheel, or interior surfaces using fingerprint lifting techniques. Biological evidence, including hair strands, skin cells, saliva on beverage containers, cigarette butts, or used tissues, may also be gathered to obtain DNA samples. In addition, personal belongings such as receipts, parking tickets, handwritten notes, business cards, USB flash drives, access badges, or discarded packaging can reveal valuable information about the owner's identity, routines, workplace, financial activities, or social relationships. These artifacts may be exploited for identity theft, social engineering, targeted surveillance, unauthorized access to secure facilities, or forensic impersonation. As no visible damage is inflicted on the vehicle, the attack often remains unnoticed while compromising the occupants' privacy and security.

■ To fend of this attack, we can start by limiting unauthorized physical access to the vehicle and reducing the exposure of sensitive personal information. Vehicle owners should remove personal belongings, confidential documents, and electronic storage devices whenever the vehicle is left unattended or delivered for servicing. Interior surfaces should be periodically cleaned to minimize recoverable fingerprints and biological traces, while disposable items such as tissues, beverage containers, and receipts should be removed promptly. Choosing reputable service providers, restricting access to trusted individuals, and locking the vehicle when unattended reduce opportunities for evidence collection. Organizations operating fleets (e.g., Taxi company) or transporting sensitive personnel

(e.g., Global Guardian, Pinkerton, and Solace Global) may further employ secure parking facilities, surveillance cameras, and documented chain-of-custody procedures during maintenance. These measures collectively reduce the likelihood that physical evidence can be covertly collected.

B. Fabrication Attack and Cyberattack Scenarios

In this category of attacks, we review attack scenarios where an attacker tries to bypass any authentication and authorization mechanism of a vehicle to either gain access to it, or manage to start the engine and take full control of the vehicle.

License Plate Cloning. In this identity-spoofing attack, the attacker identifies a target vehicle that shares the exact make, model, color, and trim level of their own secondary vehicle. The attacker physically steals or duplicate (clone) the legitimate license plates from the target vehicle and attach them to their vehicle. Operating under the stolen identity, the criminals commit illegal acts—such as armed robberies, toll evasion, or drive-by shootings—intending to trigger automated surveillance cameras. As most automated systems identify vehicles strictly by license plate registration, law enforcement investigators, e,g., the local police, initially frame the innocent owner as the prime suspect. The victim remains unaware of the attack until police execute an investigation or issue warrants, while the true attacker evades identification and leave a false forensic trail.

■ Stopping this attack requires tamper-evident physical hardware[4], advanced automated surveillance, and multi-factor physical identification. From a hardware perspective, states and manufacturers can mandate tamper-proof security screws or RFID-embedded digital license plates (e-plates [16]) that cryptographically broadcast a unique vehicle identification number (VIN) paired directly with the vehicle's internal ECU telemetry. From a surveillance and law enforcement perspective, modern Automated License Plate Recognition (ALPR) systems [45]–[49] utilize AI-driven vehicle feature matching to compare captured license plates against specific visual attributes (e.g., bumper dent patterns, unique stickers, headlight geometry, or micro-body variations) and temporal attributes [9]. Furthermore, cross-referencing multi-camera ALPR networks enables "impossible travel" anomaly detection, i.e., if the same license plate is recorded at two geographically distant locations within a time frame that is physically impossible to cover, the system flags a "Plating Clone Alert" immediately exonerating the innocent owner and alerting law enforcement to an active clone in transit. For consolidation, if the vehicle owner notice that their license placte were removed or switched, they should let the local police know about that as soons as possible.

Private Sale Identity Spoofing. Here an attacker lists a stolen, salvage-titled, or heavily defective vehicle for private sale online. To fabricate a clean vehicle history, the scammer attaches stolen or cloned license plates taken from a legitimate, clean-titled vehicle of identical make, model, year, and color. During the transaction, the scammer provides forged ownership documents matching the cloned plate and encourages the buyer to document the vehicle and plates as proof of sale. After accepting cash payment and handing over the keys, the scammer vanishes. Once the transaction completes or the vehicle subsequently breaks down, the buyer attempts to verify ownership or pursue legal recourse using the recorded license plate details. Consequently, law enforcement and legal authorities are directed entirely to the innocent third-party owner of the original plates, while the actual fraudster escapes without a paper trail.

■ Mitigating this attack requires multi-point physical verification protocols, public registry cryptographic cross-checks (yet requires electronic places [16]), and digital ownership transfer mechanisms [50]–[52]. From a buyer and operational verification perspective, buyers must perform a mandatory physical cross-matching process: comparing the license plate registration against the physical Vehicle Identification Number (VIN) stamped on the dashboard, driver door-jamb, and engine block, as well as the VIN logged digitally within the onboard computer via an OBD-II diagnostic reader. If the physical or digital VIN does not match the paper title or license plate registration, the transaction is flagged immediately as fraudulent. From an administrative and technical perspective, department of motor vehicles (or ministry of transportation in some countries) registries can mandate real-time digital title transfers via secure government mobile applications. By requiring both buyer and seller to complete multi-factor cryptographic authentication and biometric identification before exchange of funds, the system links the physical vehicle's digital VIN directly to the seller's verified government identity, rendering stolen plate substitution ineffective. Another protection consists of having both parties walk to a mechanic shop (that the buyer chooses) to run diagnostic check and physical inspection on the vehicle. If the vehicle was claimed to be healthy and turns out to be faulty, trust is broken, and the sale is cancelled. The frauder should also be reported.

Police Impersonation Hijacking. This tactic relies on deceptive authority to compromise a driver's safety. Operating under the cover of night, attackers equip an unmarked car with illegal blue flashing lights and tail a target on isolated roads. Believing they are being pulled over by legitimate law enforcement, the unsuspecting victim signals, slows down, and stops on the shoulder. Once the target comes to a complete halt, the attacker rapidly exit their vehicle and approach under the guise of an official inspection. They suddenly overwhelm and assault the vulnerable driver, physically ejecting them from the cabin before driving away with the stolen car.

■ Police impersonation hijacking can be mitigated through a combination of public awareness, emergency response procedures, and law enforcement verification mechanisms. Drivers confronted by an unmarked vehicle displaying emergency

[4]A type of hardware that accepts that physical access might happen, but guarantees that it cannot be hidden.



Fig. 6. Different, but common, act of vehicle external and internal component stripping and part theft conducted on various types of cars— from top-left to bottom-right: Stripped wheels, headlights, doors, catalytic converter, stereo, and side mirrors.

lights on isolated roads should avoid stopping immediately and instead acknowledge the signal by reducing speed and activating the vehicle's hazard lights. The vehicle should then proceed at a safe speed toward a well-lit, populated location or the nearest police station while contacting emergency services through a hands-free system to verify the legitimacy of the traffic stop. Throughout the encounter, vehicle doors should remain locked and windows closed until the identity of the officer has been confirmed. Public education campaigns promoting these practices, together with rapid police verification services and increased deployment of clearly identifiable law enforcement vehicles, can significantly reduce the effectiveness of police impersonation attacks and enhance driver safety.

C. Modification Attack and Cyberattack Scenarios

In this subsection, we review various forms of attacks and cyberattacks that compromise data and vehicle integrity, and discussed possible security countermeasures that can be applied by vehicle owners or vehicle manufacturers to protect and secure the vehicles and their passengers.

External Component Stripping and Part Theft. Rather than stealing the entire vehicle, attackers target high-value external or undercarriage components—such as catalytic converters, alloy wheels, doors, hoods, battery (especially, in trucks), headlights, and tailgates—which can be harvested quickly without gaining access to the cabin or engine computer. Attackers utilize portable power tools (e.g., cordless reciprocating saws, angle grinders, and hydraulic jacks) to cut catalytic converters directly out of the exhaust system in under two minutes to harvest precious metals like platinum, palladium, and rhodium. Similarly, thieves jack up parked vehicles to remove wheels using impact wrenches, or unbolt outer body panels (such as tailgates or aluminum doors) to resell on the illicit auto-parts secondary market. Because these physical attacks bypass onboard immobilizers and ignition security entirely, thieves operate silently or quickly in dimly lit parking structures, leaving behind a heavily damaged, non-operational vehicle. In Fig. 6, we illustrate some froms of this attack.

■ To stop this form of attack, it requires investing in physical hardening accessories, structural serial etching, and advanced tilt and sound sensor integration. From a physical security standpoint, owners and manufacturers can deploy protective hardware, such as steel skid plates, catalytic converter locking shields, stainless-steel security cables, and specialized wheel-lock lug nuts with unique key patterns. Furthermore, permanently laser-etching the Vehicle Identification Number (VIN) directly onto body panels, catalytic converter housings, and alloy rims deters illicit resale by making stolen parts easily traceably by law enforcement during scrap metal audits [15]. From a vehicle telemetry standpoint, manufacturers can integrate multi-axis accelerometer sensors (tilt detection for jacking) and acoustic glass-break/ultrasonic vibration sensors into the vehicle security system. Detecting unauthorized vehicle elevation or high-frequency cutting vibrations triggers the security horn, sends immediate real-time push alerts to the owner's mobile application [12], and activates exterior surround-view cameras [25] to capture forensic video evidence.

Convertible Top Slashing Attack. A convertible top slashing attack is a form of physical vehicle vandalism in which an attacker intentionally cuts or tears the fabric or vinyl roof



Fig. 7. From left to right: Manual fuel siphoning attack where a malicious individual uses thier mouth or a hand pump to extract fuel from other people's vehicles, smash-and-grab theft where an attacke smashes the window of a vehicle to steal valuable items, and check engine light obfuscation where the attacker uses tape to cover the light component of the MIL light to make the vehicle's engine look in good condition.

of a convertible to gain unauthorized access to the passenger compartment or to inflict costly damage. Unlike conventional break-in methods that target windows or door locks, slashing the soft top allows rapid entry while bypassing many factory-installed locking mechanisms and alarms. Once inside, attackers may steal valuables, access the glove compartment or trunk, or connect unauthorized devices to exposed vehicle interfaces such as the OBD-II port. Even when no theft occurs, the attack often results in expensive repairs because convertible roof assemblies typically require complete replacement rather than localized patching. Consequently, this attack is particularly attractive to opportunistic criminals due to its speed, low complexity, and high financial impact on vehicle owners.

■ The mitigation of this attack requires combining physical security with intrusion detection and preventive parking practices. Owners should avoid leaving valuables visible inside the vehicle and, whenever possible, park in secure, well-lit areas monitored by surveillance cameras. Modern alarm systems equipped with interior motion sensors, cabin intrusion detectors, and glass-break or vibration sensors can rapidly detect unauthorized entry and alert the owner through connected telematics services. Additional deterrents, such as steering wheel locks or protected OBD-II ports, can limit the consequences even if the passenger compartment is breached. Regular inspection of the convertible roof and prompt repair of minor damage also help prevent further deterioration and reduce opportunities for repeated attacks. Together, these measures decrease both the likelihood and impact of unauthorized access through the convertible top.

Fuel Siphoning Attack. Fuel siphoning is a physical theft attack in which an adversary illegally extracts fuel (gasoline or diesel) from a vehicle's fuel tank for personal use or resale (viz., Fig. 7-left). Attackers typically exploit unsecured fuel filler necks, puncture the fuel tank, or tamper with fuel lines to rapidly drain fuel without requiring access to the vehicle's electronic systems. Although the primary objective is fuel theft, the attack may also damage the fuel delivery system, contaminate the tank (e.g., by putting water or bleach), or leave the vehicle immobilized due to insufficient fuel. Fuel siphoning is particularly prevalent in commercial fleets, trucks, buses, construction equipment, and agricultural vehicles, where large fuel capacities offer substantial financial incentives [53]. Since the theft often occurs while the vehicle is parked and unattended, victims may remain unaware until the vehicle fails to start or exhibits fuel-related warnings.

■ Mitigating fuel siphoning attacks requires a combination of physical security measures and continuous fuel monitoring. Anti-siphon fuel filler devices, lockable fuel caps, reinforced fuel tanks, and protected fuel lines significantly increase the difficulty of unauthorized fuel extraction. Modern fleet management systems can continuously monitor fuel levels and detect abnormal fuel loss when the engine is off, automatically generating alerts for vehicle owners or fleet operators. Fuel tank intrusion sensors, surveillance cameras, secure parking facilities, and adequate lighting further deter opportunistic theft. Additionally, integrating fuel level data with GPS and telematics systems enables operators to correlate unexpected fuel loss with vehicle location and time, facilitating rapid investigation and reducing the likelihood of repeated attacks.

Smash-and-Grab Theft. In this rapid physical intrusion attack, the attackers target visible, valuable items (such as laptops, bags, smartphones, or purses) left exposed inside a parked vehicle's cabin. Relying on speed and force rather than technical bypass tools, the attacker uses heavy or specialized impact implements—such as automatic center punches, tempered glass breaker tools, ceramic spark plug fragments ("ninja rocks"), or hammers—to instantly shatter a side window with minimal noise or effort (viz., Fig. 7-middle). Within seconds, the thief reaches through the broken window frame or unlatches the door, snatches the targeted items, and flees the scene before bystanders, security patrols, or perimeter alarms can intervene. Beyond the immediate loss of personal property, this attack inflicts structural physical damage on the vehicle frame, exposes the interior to environmental elements, and provides the attacker with physical cabin access to reach the diagnostic OBD-II port, glove compartment documents, or internal trunk release controls.

■ The mitigation of this attack requires a combination of behavioral deterrents, physical window hardening, and active

acoustic/vibration sensing. From an operational and behavioral security perspective, drivers must enforce "clean cabin" protocols: removing all visible personal items, electronics, and bags from plain view or locking them securely inside the trunk prior to arriving at a parking destination. From a physical hardware perspective, owners and manufacturers can apply shatter-resistant security window films or deploy laminated side glass, which holds shattered glass fragments together and resists high-impact blows, significantly delaying physical breach attempts. From a vehicle electronic security perspective, modern security systems incorporate ultrasonic acoustic glass-breakage sensors and high-frequency piezoelectric vibration detectors. Upon sensing the distinctive frequency of shattering tempered glass, the Body Control Module (BCM) immediately activates the vehicle horn, flashes exterior hazard lighting, logs real-time event telemetry to the owner's mobile application [25], and triggers vehicle cameras [12] to capture forensic video footage of the perpetrator.

Instrument Cluster Odometer Rollback. In this fraud scheme, an attacker manipulates the digital mileage value displayed on the Instrument Panel Cluster (IPC) to artificially increase the market value of a high-mileage vehicle. The perpetrator gains access to the IPC memory either by connecting an OBD-II programmer to write a lower value to the cluster's microchip, or by removing the physical dashboard to flash the EEPROM chip directly using a EEPROM programmer (viz., Fig. 8-top-left). Because the attacker only alters the local memory registers of the instrument cluster module, the vehicle's independent control units—such as the Engine Control Module (ECM), Transmission Control Module (TCM), and ABS/ESP module—continue logging the actual, higher cumulative distance traveled. Consequently, a discrepancy is created between the altered dashboard display and the true operational history recorded deep within the vehicle's secondary ECUs.

■ Defending against odometer rollback fraud relies on diagnostic cross-module verification, secure non-volatile memory access controls, and centralized telemetry auditing. From a diagnostic inspection perspective, buyers and technicians can use multi-system OBD-II diagnostic tools to perform cross-ECU mileage audits, comparing the IPC's reported distance against non-volatile memory logs in the ECM, ABS controller, and transmission unit. From an architectural perspective, vehicle manufacturers implement cryptographic access controls and hardware-level write protection on cluster EEPROM chips, requiring cryptographic challenge-response authentication before allowing memory modifications. Nevertheless, an attacker may bypass these technical security controls by leveraging a human insider—such as an authorized technician or engineer (a relative) working at the manufacturer's official dealership network, to perform the memory overwriting. To mitigate this insider trust threat, modern connected vehicles periodically sync encrypted total distance metrics to secure manufacturer cloud registries during routine servicing, allowing automated history platforms to flag downward mileage discrepancies during vehicle resale or title transfers [54].

Malfunction Indicator Light (MIL) Physical Obfuscation. In this deceptive fraud tactic, a seller attempts to conceal active Diagnostic Trouble Codes (DTCs) and severe engine defects by physically disabling or obscuring the Malfunction Indicator Light (MIL)—commonly known as the check engine light (illuminated as on vehicles' instrumental cluster panel—IPC). The attacker disassembles the IPC and places opaque material, such as black electrical tape, behind the gauge face directly over the MIL LED, or physically cuts the LED circuit path on the printed circuit board. Consequently, when critical engine, transmission, or emissions faults occur, the warning light is unable to illuminate on the dashboard. Unaware of the hidden mechanical issues, an unsuspecting buyer relies on the visually clean instrument cluster, purchases the vehicle under the impression that it is in good health, and subsequently suffers severe engine failure or costly repairs shortly after driving the vehicle (viz., Fig. 7-right).

■ Mitigating MIL physical obfuscation requires a combination of buyer inspection protocols, onboard diagnostic verification, and redundant architecture design. From an operational verification standpoint, buyers and inspectors must verify the instrument cluster bulb check: when turning the ignition to the "ON" position (without starting the engine), all status lights, including the MIL, must illuminate briefly to confirm bulb integrity. Furthermore, connecting a generic OBD-II scanner to read active and pending DTCs directly from the Engine Control Module (ECM) bypasses physical cluster tampering entirely. From an architectural design perspective, vehicle manufacturers can implement digital cluster integrity checks that monitor LED circuit resistance and alert the driver via secondary displays (e.g., central infotainment or driver information screen) if an IPC tally light fails or is disconnected. Modern fully digital software-driven clusters also reduce this physical attack surface, as warning indicators are rendered via software graphics on liquid crystal displays rather than individual physical light-emitting diodes behind plastic masks.

Mileage Blocking. In this situation, a dishonest person buys a vehicle with the intention of driving it for some time (which could be for a couple of years) and selling it later with a lower mileage. To that end, the dishonest person connects an obdometer blocking device to the vehicle's odometer module. This device blocks the odometer from adding up when the vehicle is being driven. After driving many miles for year, the attacker unplugs the malicious device to sell the vehicle with the mileage it had at the time the device was plugged.

■ By running a physical inspection of the vehicle's engine modules, a specialized mechanic can detect the malicious device. However, the dishonest person could remove the device before selling the vehicle, which makes it impossible for the buyer to know that the displayed mileage of the vehicle was incorrect. The countermeaure to this threat comes back to the design phase. Vehicle manufacturers have to implement cryptographic authentication and cross-ECU redundant logging. Modern vehicles do not store mileage in a single isolated odometer unit; instead, the reading is tracked

across multiple Electronic Control Units (ECUs), such as the Transmission Control Module (TCM), Engine Control Unit (ECU), and ABS module. By encrypting the Controller Area Network (CAN bus) communication between these modules and requiring cryptographic signatures for odometer updates, manufacturers can prevent unauthorized blocking devices from intercepting or manipulating the signals. Furthermore, if a physical blocker attempts to disconnect or freeze the primary cluster module, the secondary ECUs continue logging operating hours and wheel revolutions. When the vehicle detects a mismatch between these independent sensor readings or notices missing heartbeat signals from the dashboard, it can for example permanently record a non-clearable "Odometer Tamper" Diagnostic Trouble Code (DTC) in secure, write-once flash memory (EEPROM) and display a tamper warning on the Instrument Panel Cluster (IPC). Furthermore, the person interested in buying a vehicle can search for oil change and maintenance stickers on windows or door frames, in the glove box or under the hood, and check that the numbers on the odometer gauge are consistent. They could also examine the tires, i.e., if the odometer shows is low mileage, the vehicle should have the original tires on.

D. Interruption Attack and Cyberattack Scenarios

In this category of attacks, we review various attack scenarios where an attacker undertakes malicious actions against the physical part of a vehicle with an aim to cause harm to the vehicle, the vehicle owner, the passengers, or any future owner of the vehicle (e.g., buyer, vehicle dealer, etc).

Armed Carjacking and Rideshare Exploitation. In this direct violent attack, the attacker leverage physical force, deadly weapons (such as firearms or blades), or platform exploitation to coerce the driver into surrendering the vehicle (viz., Fig. 8-top-middle). While traditional armed carjacking relies on ambush tactics—such as surrounding a vehicle stopped at a red light or in a dark parking lot—rideshare-targeted carjackings exploit mobile hailing applications (e.g., Uber, Lyft, inDrive, Nro7o, Yassir, etc) to lure drivers to secluded destinations. In today's world, attackers often request rides using stolen credit cards, anonymous prepaid accounts, or fraudulent burner profiles. Once inside the vehicle or upon arrival at a dimly lit drop-off location, the attacker threatens the driver from the rear passenger seat, forcing them out of the vehicle under duress and taking control of the running car along with the driver's personal belongings.

■ To mitigate carjacking attacks, several measures could be taken: A combination of platform-level identity verification (this may require coordination with the ministry of justice for background check), telemetry-driven emergency response, and remote vehicle immobilization. From a software platform perspective, rideshare applications can mitigate fraudulent hailings by enforcing mandatory multi-factor biometric identity verification (such as real-time facial scanning or government-issued ID validation) for passenger accounts, particularly when using prepaid payment methods. From a hardware and vehicle security perspective, vehicles integrated with rideshare fleet management systems can feature covert emergency panic triggers mounted discretely near the steering wheel or seat base. Activating the trigger silently initiates live interior audio/video streaming to emergency dispatchers, logs real-time cellular telemetry, flash an external back emergency light (still used by some taxi companies) and activates delayed remote engine shutoff. Once the vehicle comes to a complete stop, the vehicle's computer can disable the accelerator pedal, engage secondary hazard lighting, and lock out ignition restarts, neutralizing the stolen vehicle's mobility while ensuring the victim's immediate physical safety.

Staged Rear-End Collision ("Bump and Rob"). Attackers intentionally tap or bump the rear bumper of a target vehicle at low speeds, often selecting vulnerable moments at late-night stoplights, secluded intersections, or poorly lit parking lots where traffic is sparse and visual surveillance (such as security cameras or eyewitnesses) is absent. The minor impact is designed to mimic an accidental fender-bender without disabling the target vehicle. Prompted by the jarring sound and assuming a routine traffic incident, the victim naturally steps out of the vehicle to inspect the bumper and exchange insurance details. Relying on the driver's immediate distraction and the urgency of the moment, the perpetrators anticipate that the victim will leave the engine running or the keys in the ignition. While the primary driver from the striking vehicle engages the victim in conversation to keep their attention focused away from the cabin, a hidden accomplice swiftly slips into the target vehicle's driver seat and speeds off with the car, often followed closely by the accomplice's vehicle.

■ Defending against staged collision carjackings involves both situational awareness protocols and automated safety systems. From a operational security standpoint, drivers who experience a minor rear-end collision in secluded or suspicious environments should remain inside the vehicle with doors locked, keep the engine running, and call emergency services before stepping out to inspect damage or engage the other driver. If the situation appears hostile, the driver should signal the other vehicle and drive directly to a well-lit public area or nearest police station. From a technical design perspective, vehicle manufacturers can mitigate this risk by integrating telematics and surround-view camera systems (e.g., 360-degree ADAS camera). When built-in inertial sensors detect a low-speed collision, the infotainment module can automatically initiate a emergency recording, log external video feeds to non-volatile local memory and cloud backup, and auto-lock all doors to protect occupants while evaluating the situation. Additionally, telematics modules can automatically prompt the driver via screen touch or voice to verify safety, immediately alerting emergency dispatch with real-time GPS coordinates if an unconfirmed departure or forced cabin access is detected. Furthermore, the use of dashcam is also interesting as it may capture the collision scenario for further investigations and to protect against collision insurance frauds.



Fig. 8. From top to bottom, left to right: Mileage overwrite using OBD-II interface to show low mileage when selling the vehicle, firewarm carjacking, exaust distraction carjacking using soda can, driveway snatch-and-run, t-bone ramming using a stolen transport truck, and vehicle theft using tow-truck.

Exhaust Distraction Carjacking. Here, the attacker attaches a metallic object, such as a compressed aluminum can (viz., Fig. 8-top-right), to the interior or rim of the vehicle's exhaust tailpipe while the vehicle is parked. When the victim starts the engine and begins driving, the rapid flow of exhaust gases and engine vibrations cause the metallic object to continuously strike the exhaust tubing, generating a loud, alarming knocking or rattling noise. Prompted by the sudden disturbance and assuming a severe mechanical failure, the driver typically pulls over and exits the vehicle to inspect the tailpipe. Relying on the driver's urge to quickly check the noise, the attacker anticipates that the victim will leave the engine running or leave the keys in the ignition. Once the driver steps away from the cabin, the opportunistic thief quickly enters the running vehicle and drives away.

Feigned Incapacitation Hijacking. In this social engineering-based scenario, a primary attacker intentionally enters a roadway to feign acute intoxication or severe medical distress, forcing a target vehicle into a full emergency stop. Exploiting the operator's altruistic emergency response bias, the driver dismounts from the vehicle to render aid, inadvertently leaving the propulsion system active and the cabin physically unmonitored. Upon the driver's egress, a concealed secondary attacker rapidly infiltrates the driver compartment, engages the drive controls, and exfiltrates with the vehicle. Concurrently, the primary attacker terminates the simulated incapacitation state and flees on foot along a secondary egress route, achieving complete asset compromise while mitigating immediate physical capture.

■ The countermeasures for the two previous exploit rely primarily on driver awareness, operational security, and vehicle auto-lock features. Drivers must adhere to strict key-custody protocols, i.e., the engine should always be turned off, the transmission placed in Park, and the key or keyfob taken with the driver whenever exiting the vehicle, regardless of how brief the inspection may be. From a technical design standpoint, vehicle manufacturers can implement proximity-based automatic engine cut-offs that shut down the ignition if the smart key leaves the cabin while the vehicle is idling. Furthermore, anti-carjacking security systems can automatically lock all doors and sound an alarm if a weight sensor detects the driver's seat becoming unoccupied while the vehicle remains running.

Driveway Snatch-and-Run. In this highly opportunistic attack, generally, a group of attackers monitors residential driveways or gated entrances waiting for target vehicles to return home. When the driver stops at their gate or garage, they routinely exit the cabin while leaving the engine idling, key in the ignition, and doors unlocked to quickly open a gate, move a trash receptacle, or reposition another parked vehicle (viz., Fig. 8-bottom-left). Exploiting this brief window of vulnerability, an attacker positioned nearby rapidly approaches the running vehicle, jumps into the driver's seat, and speeds off within seconds (the other members watch the scene, ready to shellack up the driver in case of resistance). Because the vehicle is already running and unlocked, the attackers bypass all immobilizer and entry security mechanisms without needing physical tools or signal manipulation.

■ Mitigating driveway snatch-and-run attacks requires operational security habits alongside modern proximity and occupancy sensing features. From an operational perspective,

drivers must enforce strict key-custody protocols by switching off the ignition and taking the key or fob whenever exiting the vehicle, even for momentary tasks outside the cabin (as this is a matter of awareness). From a vehicle design perspective, modern Passive Keyless Entry and Start (PKES) systems can implement automated anti-carjacking logic, i.e., if the vehicle detects that the driver's seat-occupancy sensor shows an unoccupied seat and the driver's door opens and closes while the smart key fob is still within the cabin, the vehicle can automatically lock the doors. If the keyfob is detected to be away, the vehicle turns off. Furthermore, if the system senses an attempt to shift out of "Park" without the smart key present inside the cabin interior, the ECU can immediately kill the ignition, engage the electronic parking brake, and sound the horn to alert the surroundings.

T-Bone Ramming Attack Using a Stolen Box Truck. This attack scenario involves deliberately driving a large commercial vehicle into the side of a target vehicle (and sometimes on a crowd of people) to maximize impact forces and cause severe structural damage (viz., Fig. 8-bottom-middle). Owing to their high mass and rigid construction, box trucks can generate significantly greater collision energy than passenger vehicles, making them capable of overcoming side-impact protection and disabling the target vehicle. Stolen trucks are often used to hinder forensic tracing and complicate post-incident investigations. Such attacks may be motivated by criminal intent, targeted violence, or attempts to disable or stop a vehicle before theft or other offenses. Beyond the intended target, these incidents present a substantial risk to pedestrians, nearby motorists, and surrounding infrastructure, often resulting in extensive property damage and serious injuries.

■ To fend off this attack, the countermeasure must combine vehicle safety technologies, infrastructure protection, and operational security measures. Modern vehicles equipped with side-impact protection, reinforced occupant compartments, and advanced restraint systems can reduce occupant injury during severe collisions. Intelligent transportation systems, roadside surveillance, and automatic incident detection can accelerate emergency response and support post-event investigation. For commercial fleets, rapid reporting of stolen vehicles, GPS-based fleet tracking, and collaboration with law enforcement improve the chances of recovering stolen trucks before they are used in criminal activities. Together, these measures enhance resilience against intentional ramming attacks while reducing their potential consequences.

Structural Immobilization Attack. Here the attacker targets a vehicle's mechanical and structural components to render it inoperable or significantly degrade its safe operation. These attacks include loosening or removing wheel lug nuts, cutting brake lines, removing steering rack mounting bolts, damaging suspension springs, introducing frame rail notches, damaging the fuel line, blocking the exhaust pipe, contaminating the engine bay fluid, slashing tires, intentionally cracking the windshield, and other forms of physical vandalism [26], [37]. Unlike cyberattacks, these actions directly compromise the vehicle's structural integrity and often require only simple hand tools, leaving little or no digital evidence. Depending on the targeted component, the consequences range from gradual performance degradation to sudden loss of steering, braking, or wheel retention, posing severe safety risks to occupants and other road users. Such attacks are particularly difficult to detect before operation, making them attractive for malicious sabotage, theft facilitation, or intentional disruption.

■ Mitigating structural immobilization attacks requires a layered approach combining physical protection, routine inspections, and condition monitoring. Critical fasteners, such as wheel lug nuts and steering rack bolts, should employ tamper-resistant hardware or tamper-evident markings to reveal unauthorized access. Regular maintenance should include inspection of brake lines, suspension components, frame rails, and windshield integrity to identify signs of damage, wear, or deliberate modification before vehicle operation. Modern vehicles can further enhance protection through wheel vibration monitoring, brake pressure sensing, and chassis diagnostic systems capable of detecting abnormal mechanical behavior. Physical security measures, including secure parking, surveillance cameras, intrusion alarms, and impact sensors, can deter acts of vandalism and provide evidence in the event of an attack. Collectively, these preventive and monitoring measures improve the likelihood of early detection while significantly reducing the risk of successful structural sabotage.

Tow-Truck Vehicle Theft Attack. In this attack scenario, the attacker targets a vehicle by loading or towing it away using a tow truck or flatbed, thereby bypassing many of the vehicle's electronic anti-theft and immobilization systems (viz., Fig. 8-bottom-right). As the attack does not require starting the engine or defeating onboard security mechanisms, it is effective even against vehicles equipped with advanced keyless entry protection and engine immobilizers. Attackers may impersonate legitimate roadside assistance or recovery services to avoid suspicion, enabling them to remove the vehicle quickly from parking lots, residential areas, or public streets. Also, the speed and low visibility of this attack make it a significant challenge for both private vehicle owners and fleet operators. Once transported to another location, the vehicle can be dismantled for parts, reprogrammed (then left in some place), or subjected to exportation [43].

■ To reduce the risk of such attack, different measures should be taken, such as integrating physical deterrents, real-time monitoring, and location-based security mechanisms. Mechanical devices such as wheel clamps or parking locks increase the effort and time required to tow a vehicle, while secure parking areas with surveillance cameras and controlled access reduce opportunities for unauthorized removal. Modern telematics systems equipped with GPS, inertial sensors, and tilt or towing detection can recognize abnormal vehicle movement while the ignition is off and immediately notify the owner or fleet operator. Geofencing and remote tracking



Fig. 9. From left to right, some radio frequency hardware tools used for radio interception of vehicle entry and start signals: Fliperzero, a multi-purpose radio sniffer and signal replay/generator tool, HackRF One from Great Scott Gadgets, an SDR used to intercept and transmit arbitrary signals, Ettus USRP (Universal Software Radio Peripheral) B210, a high-performance SDR equipment frequently utilized in university and industrial lab research to evaluate precise latency thresholds in RF communications, and the HackKEY from UnicornTeam, used for relay attacks.

further improve the chances of rapid vehicle recovery by providing continuous location updates following unauthorized movement. For commercial fleets, centralized monitoring platforms can automatically flag unexpected towing events and initiate predefined incident response procedures, significantly improving the likelihood of recovering the vehicle before it reaches a secondary location.

V. Attacks on Vehicles' Access and Start System

In this section, we review the various attacks on vehicles access (entry) and start systems. We also discuss the possible countermeasures to mitigate each attack. These attacks mainly aim for compromising the authentication mechanism that is implemented to protect the access to the inside of the vehicle, and also to start the engine and drive the vehicle.

A. Interception Attack and Cyberattack Scenarios

In this subsection, we review different attack scenarios where an attacker targets the vehicles entry and start system by running various interception attacks with an aim to capture signals, codes, and credentials, that may allow the attacker to bypass the authentication system later on. In Fig. 9, we illustrate some of the most used radio frequency hardware models to conduct these cyberattacks. Of course, vehicle theives use customized, non-publishable, radio frequency equipment that is based on the hardware similar to the one shown in Fig. 9.

Keyfob Signal Capture. This attack targets the wireless communication between the vehicle and its remote keyfob by intercepting radio-frequency transmissions during legitimate user interactions. Using a software-defined radio (SDR) or specialized RF receiver (viz., Fig. 9), an attacker records signals transmitted when the owner remotely locks, unlocks, or starts the vehicle. Although modern rolling-code systems generally prevent direct replay, the captured transmissions may still reveal protocol characteristics or be combined with other attacks such as RollJam or cryptographic analysis. Older vehicles and aftermarket access systems that rely on fixed-code transmissions remain particularly vulnerable to this attack. By collecting these wireless signals, attackers gather authentication data that may later be exploited to gain unauthorized access to the vehicle.

■ Vehicle manufacturers should employ encrypted rolling-code, challenge-response authentication protocols that generate a unique cryptographic response for every transaction, or apply frequency hopping techniques (e.g., FHSS) on higher frequency bands to harden signal interception [105]. Also, replay protection, message authentication codes (MACs), and strong cryptographic algorithms prevent previously recorded signals from being reused successfully. Radio communication should also include nonce values or timestamps to ensure freshness [102]. Users should avoid using aftermarket access systems based on fixed RF codes and keep vehicle firmware updated to address newly discovered protocol vulnerabilities.

Rolling-Code Interception Attack. This attack, a.k.a., the RollJam attack, is a sophisticated dual-radio exploitation technique designed to bypass rolling-code defenses [55]. The attacker deploys a custom transceiver device (viz., Rolljammer in Fig. 11) near the target vehicle. When the victim presses the key fob button to unlock the car, Radio 1 broadcasts broadband jamming noise to block the vehicle from receiving the signal, while Radio 2 simultaneously captures and records the unspent rolling code (Code 1). Confused when the vehicle fails to unlock, the victim presses the key fob button a second time. Radio 1 jams the vehicle again while Radio 2 captures the second rolling code (Code 2). Instantly, the attacker's device retransmits Code 1 to unlock the vehicle, satisfying the driver. The attacker is left holding a valid, unspent rolling code (Code 2) in memory, which can be retransmitted later at any time to gain unauthorized entry into the vehicle.

■ Defending against RollJam attacks requires enforcing time-sensitive rolling-code windows and cryptographic timestamps. Modern RKE systems implement tight code-expiration windows where rolling codes expire if not received within a strict timestamp threshold relative to the vehicle's internal clock. Furthermore, bi-directional challenge-response protocols allow the vehicle to verify key state dynamically rather than relying

on unidirectional rolling-code streams. Vehicles can also log consecutive signal interference anomalies; if the BCM detects RF jamming accompanied by repeated out-of-sequence code attempts, it can trigger visual warnings on the dashboard or require physical key insertion to reset the authentication counter. Last but not least, if the vehicle owner suspects such an attack after several attempts to unlock/lock their car, they could press the unlock/lock button again on their keyfob to invalidate all the codes that were intercepted by the attacker.

Code Grabbing Attack. This involves passively intercepting the digital authentication code transmitted by a wireless keyfob during normal operation. Early remote keyless entry systems often transmitted a static code that could be recorded using inexpensive radio receivers, e.g., HackRF One and Flipper Zero, and replayed later to unlock the vehicle. Although modern systems largely employ rolling codes (i.e., send a different code each time), many legacy vehicles and low-cost aftermarket security systems continue to use fixed-code protocols that remain vulnerable.

■ Static authentication codes should be replaced with cryptographically secure rolling-code or challenge-response protocols that generate unique authentication messages for every transaction. Strong encryption, mutual authentication, and hardware security modules (e.g., the use of PUFs—Physical Unclonable Functions [19]) for key storage further reduce the risk of credential interception. Manufacturers should also phase out legacy fixed-code systems and encourage owners to replace insecure aftermarket access devices.

RFID Credential Cloning Attack. Many vehicle owners install aftermarket RFID-based access and ignition systems to improve convenience or replace damaged factory immobilizers. These systems often rely on inexpensive 125 kHz RFID tags (e.g., EM4100 or T5577-compatible tags) or older 13.56 MHz MIFARE Classic cards that offer weak or no cryptographic protection. An attacker can capture the RFID credential using commercially available devices such as the Proxmark3 (viz., 4th item in Fig. 11) during a brief interaction with the legitimate tag or card. Once the credential is extracted, it can be duplicated onto a blank RFID tag, producing a functional clone that is accepted by the vehicle's authentication system. The cloned credential enables unauthorized unlocking and, in some installations, ignition of the vehicle without leaving obvious signs of forced entry.

■ Vehicle access systems should employ RFID technologies that provide strong cryptographic authentication rather than static identifiers. Secure smart cards implementing mutual authentication and encrypted challenge-response protocols, such as DESFire EV2/EV3, iClass, or equivalent secure elements, significantly reduce the risk of credential cloning. Secret keys should be generated uniquely for each vehicle and stored within tamper-resistant hardware rather than in application software. Additionally, the RFID authentication should be integrated with a secure immobilizer that verifies multiple security conditions before enabling the ignition. Regular firmware updates, anti-tamper mechanisms, and event logging can further strengthen the overall security of aftermarket access systems

B. Fabrication Attack and Cyberattack Scenarios

In this subsection, we present attack and cyberattack scenarios that an attacker may undertake to bypass the authentication and authorization systems of the vehicles. The pattern of the attacks is to impersonate the real owner holding the genuine key or keyfob and get illegal access to the vehicle. The attacker may also start the engine and drive the vehicle away.

Jaws-of-Life Reverse Attack. Here, the attacker exploits hydraulic rescue tools, or similar high-force spreading equipment, to forcibly pry open vehicle doors, hoods, or trunks without relying on conventional lock bypass techniques (viz., Fig. 10-left). Originally designed for emergency extrication, these tools can rapidly overcome reinforced door frames and locking mechanisms, enabling attackers to gain access even when electronic security systems remain active. Once inside the vehicle, attackers may steal valuables (e.g., vehicle documents, laptop, etc), remove electronic control modules, or connect a malicious OBD-II device to the diagnostic port to perform unauthorized operations such as key programming, ECU manipulation, or installation of persistent attack hardware. Compared with traditional break-in methods, this technique causes extensive structural damage while minimizing the time required to gain entry, making it particularly attractive for organized vehicle theft and targeted attacks.

■ Defending against Jaws-of-Life reverse attacks requires combining physical hardening with rapid intrusion detection and access control. Reinforced door structures, protected OBD-II ports, and lockable diagnostic port covers can delay unauthorized access and prevent immediate connection of rogue diagnostic devices. Intrusion detection systems equipped with door deformation, vibration, or glass-break sensors can trigger audible alarms, activate vehicle immobilization functions where safe, and immediately notify the owner or fleet operator through telematics services. Secure parking facilities, surveillance cameras, and adequate lighting further reduce opportunities for such attacks. Additionally, implementing cryptographic authentication for OBD-II diagnostic sessions and restricting security-critical functions, such as key programming or ECU reconfiguration, to authenticated service tools can significantly limit the impact even if attackers succeed in physically accessing the vehicle.

Mechanical Lock Picking and Ignition Bypass. Prior to the widespread adoption of electronic immobilizer systems, vehicles relied entirely on mechanical key cylinders for entry and ignition authentication. In this classic attack, attackers use physical lock-picking tools—such as tension wrenches and feeler picks, or brute-force "jiggler" keys (viz., 3rd item in Fig. 11)—to manipulate the wafer tumblers inside the door lock cylinder. Once inside the cabin, the attacker targets the steering column ignition assembly (viz., Fig. 10-middle and right). Using either covert picking techniques or destructive



Fig. 10. From left to right: Jaws-of-Life reverse attack where a malicious individual uses the fire fighters jaws-of-life to hydraulically force open a vehicle door, picklocking a vehicle door lock, picklocking a vehicle ignition system using a falt screwdriver.

brute force (such as driving a flathead screwdriver or slide-hammer directly into the ignition lock cylinder), the thief forces the lock plug to rotate. Because early vehicles lacked electronic transponder verification between the key and the engine computer, turning the ignition switch mechanically completed the high-current electrical circuits for the starter motor, fuel pump, and ignition coil, enabling the thief to start the engine and drive away within minutes.

■ Mitigating purely mechanical vehicle theft involved physical hardware defenses, mechanical locking accessories, and ultimately the architectural shift to electronic verification. From a physical hardware perspective, manufacturers introduced high-security lock designs, such as sidewinder (laser-cut) keys, hardened steel housing plates around the steering column, and shear-bolt mountings for ignition switch housings to resist brute-force torque attacks. Owners frequently relied on secondary physical deterrents, such as heavy-duty steering wheel locks (e.g., "The Club"), brake pedal clamps, or hidden aftermarket ignition kill switches wired directly to the starter relay or fuel pump circuit. From an architectural design perspective, the ultimate countermeasure was the introduction of cryptographic Engine Immobilizer systems in the mid-1990s. By embedding a passive RFID transponder chip inside the key head that must exchange an encrypted challenge-response handshake with the immobilizer ECU, manufacturers rendered mechanical picking and forced cylinder rotation completely ineffective at starting the engine without the legitimate cryptographic key.

Physical Key Decoding and Mechanical Duplication. In this physical entry attack, an attacker obtains mechanical access to the vehicle by physically decoding or duplicating the mechanical key blade without needing the original keyfob's electronic transponder. Attackers or dishonest service attendants (e.g., valets, mechanics) can quickly impression the key or scan its mechanical bitting profile using portable locksmith optical decoders or specialized picking/decoding devices (such as Lishi tools—viz., 2nd item in Fig. 11) directly through the door lock cylinder. Once the mechanical key code or wafer depths are decoded, the attacker uses a high-precision key-cutting machine or locksmith key duplicator to cut a physical replica of the master blade. Although this mechanical copy lacks the cryptographic transponder chip required to bypass the engine immobilizer on modern vehicles, it grants full unauthorized access to the cabin, glove box, and trunk, enabling thieves to steal internal valuables, place spying devices, spend the night in the vehicle (squatting), access the physical OBD-II/J1939 diagnostic port to program a new transponder, or release the mechanical parking brake.

■ The mitigation of this attack requires advanced cylinder design, mechanical key-masking, and physical access locks. Vehicle manufacturers deploy high-security sidewinder (laser-cut) locks featuring complex inner track profiles and dual-sidebar lock cylinders that resist manual impressioning, optical decoding, and standard wafer picking tools. From an operational perspective, key heads can feature physical key covers to prevent quick optical photography/scanning, and drivers should exercise strict key-custody controls during third-party servicing. To protect the interior when the mechanical door is breached, vehicle architectures isolate physical cabin access from engine execution by burying the OBD-II port behind locked internal trim panels, implementing physical OBD-II/J1939 port locks, and requiring dual-factor electronic authentication (transponder verification) before disengaging the electronic steering lock (ESL) or alarm system, rendering a purely mechanical key copy incapable of operating or moving the vehicle.

Replay Attack. In a basic Radio Frequency (RF) replay attack targeting legacy static-code key fobs, an attacker uses a Software Defined Radio (SDR) or RF sniffer to eavesdrop on the wireless signal broadcast when the driver presses the key fob button. Because legacy entry systems transmit the exact same unencrypted or static code string during every transmission, the recorded signal remains permanently valid. The attacker later retransmits (replays) the captured signal on the same frequency (e.g., 315 MHz or 433.92 MHz), tricking the vehicle's Body Control Module (BCM) into unlocking the doors without requiring physical possession of the key fob. The same security vulnerability and attack pattern can be used on automatic garage gates, where vehicles could be parked.

■ Defending against basic replay attacks requires transitioning



Fig. 11. From left to right: Rolljammer by S. Kamkar [55], Lishi 2-in-one lockpick, jiggler keys, and the Proxmark RFID cloner.

from static codes to dynamic cryptographic authentication protocols. Modern remote keyless entry (RKE) systems implement rolling-code algorithms (such as KeeLoq) or challenge-response cryptographic handshakes using symmetric block ciphers (e.g., AES-128). Under a rolling-code scheme, each button press generates a unique pseudo-random code synchronized between the keyfob and the vehicle's receiver. Once a code is received and verified, the vehicle invalidates that specific sequence number, rendering any captured RF transmissions completely useless for future retransmission attempts.

Key Cloning Attack. In this cryptographic replication attack, an attacker targets the physical transponder chip embedded inside the keyfob or mechanical key head. Using a portable RFID/transponder cloning tool in close physical proximity (e.g., Proxmark 3 in Fig. 11) to the target key (such as during valet parking, car washing, or brief servicing), the attacker reads and extracts the key's unique secret key seed and identifier (ID). If the transponder relies on weak or legacy proprietary encryption ciphers (e.g., Megamos Crypto or Hitag 2 [98]), the cloner brute-forces or decrypts the master key within seconds, writing the copied cryptographic identity onto a blank transponder chip. The attacker then uses this cloned key to bypass both door entry and immobilizer checks without triggering any unauthorized access alerts.

■ To stop this attack, the countermeasure should rely on updating transponder cryptographic standards and enforcing strict physical key custody. Vehicle manufacturers must deploy modern transponder hardware utilizing strong, public-domain cryptographic algorithms (such as AES-128 or High-Security Mutual Authentication) that incorporate hardware-level anti-cloning and write-protected memory blocks to prevent unauthorized seed readout over air interfaces. Furthermore, the use of physical unclonable functions (PUFs) technology [57]–[59] proved to be very promising against object cloning, in general, and keyless entry systems, in particlar. Operational measures include educating drivers on key custody during third-party servicing and utilizing Faraday shielding pouches to prevent unauthorized close-range RFID reading.

Relay Attack. Targeting Passive Keyless Entry and Start (PKES) systems, a relay attack employs two attackers equipped with high-gain RF transceiver pairs. While the victim's smart key rests indoors (e.g., near a house front door), Attacker A stands near the targeted parked vehicle and initiates a door-handle activation. The vehicle broadcasts a low-frequency (125 kHz) challenge signal, which Attacker A's device captures and relays over a high-frequency (e.g., 2.4 GHz) cellular or radio link to Attacker B, who is standing near the victim's house. Attacker B's device re-transmits the challenge to the legitimate key fob inside the house, receives the key's valid ultra-high-frequency (UHF) response, and relays it back to Attacker A at the vehicle. The vehicle verifies the valid response and unlocks the doors or starts the engine, deceived into believing the legitimate key fob is standing right next to the vehicle. This attack is illustrated in Fig. 12, where it took less than a minute for the theives to steal a brand new 2020 Mercedes-Benz GLC in the UK.

■ Defending against relay attacks requires accurate signal propagation distance verification rather than relying solely on cryptographic validity. Vehicle manufacturers implement Ultra-Wideband (UWB) IEEE 802.15.4z transceiver chips that measure the precise Time-of-Flight (ToF) of radio signals between the keyfob and the vehicle with picosecond precision. As relay devices inherently introduce signal propagation delay over the extended distance, the UWB system detects the round-trip latency discrepancy and denies access. However, this theoritical specification turns out to be not working in practice, probably due to classical implementation issues. Supplementary countermeasures include motion-sensing smart keys that enter a sleep mode after remaining stationary for several minutes, Faraday-shielded key pouches, and user-configurable key fob sleep buttons. The adoption of frequency hopping techniques (e.g., FHSS) on higher frequency bands was also proposed to harden signal interception and make the relay impossible [105]. Last but not the least, the use of artificial intelligence for fingerprinting the radio signals between the genuine keyfob and the vehicle turned out to be efficient against this attack.

CAN Injection to Unlock Doors. A CAN injection attack targets a vehicle's internal Controller Area Network (CAN) by injecting forged CAN frames that imitate legitimate messages exchanged between Electronic Control Units (ECUs). After gaining physical access to the CAN bus through exposed wiring, lighting harnesses, diagnostic connectors, or compromised ECUs, an attacker can transmit malicious commands to



Fig. 12. From top to bottom, left to right: The complete process of a relay attack. Two malicious individuals (Men In The Middle) stand between the high-end vehicle and the keyfob (inside a house or commercial facility) and relay the signals between the two genuine parties, fooling the vehicle to believe that the keyfob is in close proximity.

the Body Control Module (BCM) to unlock the doors without possessing a valid key. This attack was demonstrated in [56] as RollCAN. Since the traditional CAN protocol lacks message authentication and source verification, receiving ECUs cannot distinguish legitimate commands from maliciously injected ones. This weakness has been exploited in several real-world vehicle thefts, where attackers accessed external CAN wiring, injected door-unlock messages, and subsequently started the vehicle using additional attack techniques. The simplicity and speed of CAN injection make it a highly effective method for bypassing conventional remote access protections while leaving minimal evidence of forced entry.

■ The mitigation of this attack requires strengthening both the in-vehicle communication architecture and intrusion detection capabilities. Implementing CAN message authentication using cryptographic Message Authentication Codes (MACs) or migrating security-critical communications to authenticated protocols such as CAN-FD with security extensions enables ECUs to verify the authenticity of received commands before execution. Additionally, In-Vehicle Intrusion Detection Systems (IDSs) can continuously monitor CAN traffic for abnormal message frequencies, unexpected command sequences, unauthorized transmitters, or deviations from normal communication patterns, allowing malicious injections to be detected in real time. Gateway ECUs (i.e., the internal router between different sub-networks within the vehicle) should isolate externally accessible networks from safety-critical domains and enforce message filtering and access control policies. Finally, securing physical access to CAN wiring and diagnostic interfaces further reduces opportunities for attackers to inject unauthorized CAN frames.

Window Breaking Attack. In this physical attack, an attacker shatters a vehicle's side or rear window to gain rapid access to the passenger compartment (viz., Fig. 13-left). The attack is typically performed using specialized glass-breaking tools, spring-loaded center punches, ceramic fragments, or blunt objects that can fracture tempered automotive glass with minimal effort. Unlike lock-picking or electronic attacks, breaking a window bypasses all door locking mechanisms and allows immediate access to valuables, the OBD-II port, or interior door release handles. In many cases, attackers exploit the brief time required to smash the window, retrieve valuables, or unlock the vehicle from the inside before attracting attention. Although simple to execute, this attack often results in significant repair costs and may serve as the first step in more advanced vehicle theft techniques.

■ Mitigating window breaking attacks requires combining reinforced glazing with rapid intrusion detection and physical deterrence. Glass-break sensors integrated into the vehicle alarm system can detect the characteristic acoustic signature or vibration associated with shattering glass and immediately activate audible alarms while notifying the owner through connected telematics services. Laminated security glass or impact-resistant window films increase the effort required to penetrate the vehicle and can delay unauthorized entry even after the glass has fractured. Parking in well-lit, monitored locations, avoiding visible valuables inside the cabin, and employing surveillance cameras further discourage opportunistic

attacks. Together, these measures significantly reduce both the likelihood of successful window-based intrusion and the time available for attackers to access the vehicle.

Slim Jim Attack. This a traditional physical lock-bypass technique in which an attacker inserts a thin metal strip, commonly known as a Slim Jim, between the vehicle window and door frame to manipulate the internal lock linkage or release mechanism (viz., Fig. 13-middle). By engaging the door rods or lock actuators, the attacker can unlock the door without using the vehicle key or damaging the exterior lock cylinder. Although modern vehicles have largely replaced exposed mechanical linkages with electronically controlled locking systems, older vehicles and some models with accessible door mechanisms remain vulnerable. The attack is quick, inexpensive, and leaves little visible evidence of forced entry, making it attractive for opportunistic theft, unauthorized access to valuables inside the vehicle, or to set up malicious devices.

■ The mitigation of this attack requires eliminating or protecting the mechanical linkages that connect the door lock to the interior locking mechanism. Manufacturers can employ shielded lock linkage, reinforced door construction, and enclosed latch assemblies that prevent external tools from reaching critical locking components. Modern electronic locking systems, in which lock actuators are electronically controlled rather than directly connected to exposed rods, significantly reduce susceptibility to mechanical manipulation. Additional protection can be achieved through intrusion alarms, door tamper sensors, laminated side windows, and secure parking practices. Regularly inspecting door panels for signs of tampering and integrating electronic access control with immobilization systems further reduces the likelihood and impact of unauthorized entry using Slim Jim-style tools.

Tailgate Entry Attack. A tailgate entry, also known as piggyback access, exploits the brief period during which a vehicle door remains open or unlocked after being legitimately accessed by the owner. Instead of bypassing the vehicle's locking mechanisms, an attacker takes advantage of the owner's momentary inattention to enter the vehicle, hide inside, or gain access before the doors automatically relock. This attack is commonly observed in parking lots, rideshare environments, and delivery operations where occupants frequently enter and exit the vehicle. Once inside, the attacker may steal valuables, tamper with vehicle electronics, connect a malicious OBD-II device, or wait until the owner leaves the vehicle unattended. Because the entry occurs without forced access or electronic compromise, conventional anti-theft systems may not recognize the intrusion (which is a successfull attack).

■ The countermeasure for this attack requires combining occupant detection with intelligent access control. Interior presence monitoring systems, employing ultrasonic sensors, radar, infrared sensors, or in-cabin cameras, can detect unexpected occupants after the vehicle has been locked and immediately trigger alarms or notify the owner through connected telematics services. Automatic door relocking, configurable lock timeout intervals, and alerts indicating that a door remains open further reduce opportunities for unauthorized entry. In addition, secure parking practices, maintaining situational awareness during vehicle entry and exit, and verifying the cabin before locking the vehicle can significantly reduce the effectiveness of piggyback access attacks. Integrating interior presence monitoring with intrusion detection systems provides an additional layer of protection against unauthorized occupants who enter without forcing access. Last but not the least, as this is form of social-engineering attack, driver awareness is a priority.

PIN Code Brute-Force Attack. Some vehicles, particularly several North American models, provide a factory-installed or aftermarket exterior keypad (viz., Fig. 13-right) that allows users to unlock the doors by entering a numeric personal identification number (PIN). A brute-force attack targets this authentication mechanism by systematically attempting different PIN combinations until the correct code is found. If the keypad lacks restrictions such as attempt limits, increasing lockout delays, or tamper detection, an attacker may eventually discover the valid PIN through repeated trials. The attack becomes more practical when users choose predictable PINs derived from birthdays, telephone numbers, or other easily guessed values. In addition, fingerprints or wear patterns on frequently pressed keypad buttons may reduce the search space by revealing the digits used in the PIN. Another passive mean for this attack is to perform a shoulder-surffing attack, where the attacker eye-sneaks the vehicle owner when the latter is inputting the PIN code. Once the correct code is identified, the attacker can unlock the vehicle without causing visible damage or triggering suspicion, potentially enabling theft or unauthorized access to items stored inside.

■ Effective protection against PIN brute-force attacks requires strengthening both the authentication mechanism and the keypad's resistance to information leakage. The system should enforce a limited number of consecutive failed attempts, followed by progressively longer lockout periods or temporary keypad deactivation to make exhaustive guessing impractical. The vehicle should log repeated authentication failures and optionally notify the owner through the infotainment system or a connected mobile application when suspicious activity is detected. Users should select random, non-predictable PINs and avoid values associated with personal information. To reduce information leakage, manufacturers can employ touch-sensitive keypads with randomized illumination, periodically changing key layouts, or materials that minimize visible wear and fingerprint residue. Finally, combining the PIN with an additional authentication factor, such as proximity verification of the legitimate key fob or smartphone, provides layered protection against unauthorized access even if the PIN is compromised. Driver awareness is also a requirement as this attack could be successfull through shoulder surffing.



Fig. 13. From left to right: vehicle window-smashing attack where malicious individual smash the windows of vehicles using an emergency safety hammer, glass breakers, a rock, or a spark plug ceramic shard. A theif using slim jim attack to unlock the door, and a PIN padlock found on some north american car models, and which can be brute-forced or subject to shoulder surfing attack.

C. Modification Attack and Cyberattack Scenarios

In this category, we present one attack scenario that aims to perform unauthorized modification to the vehicle access and start system bypassing the authentication system.

OBD-II Key Reprogramming Attack. After gaining physical entry into the cabin (e.g., via lock-picking or window breaking), the thief connects an handheld diagnostic programmer directly into the vehicle's On-Board Diagnostics (OBD-II) port (or J1939 port, if it is a truck). Exploiting unauthenticated service modes, legacy diagnostic routines, or weak pin-code extraction vulnerabilities within the Immobilizer ECU or Body Control Module (BCM), the device commands the vehicle to erase existing registered keys and pair a new, blank key fob. Because the process alters the vehicle's internal cryptographic key database directly through official diagnostic channels, the newly programmed key achieves full legitimacy, allowing the thief to start the engine and drive away within minutes.

■ Preventing unauthorized key reprogramming requires securing diagnostic channels and enforcing hardware-level access controls on the OBD-II bus. Modern vehicle architectures deploy Secure On-Board Diagnostics (OBD) security gateways that enforce cryptographic challenge-response authentication (e.g., ISO 21434 compliance) before granting write access to the Immobilizer ECU. Under this architecture, key programming operations require signed authorization tokens from authorized manufacturer cloud servers. Physical countermeasures include aftermarket OBD-II port lock covers, relocated diagnostic ports, and smart ignition lockouts that detect unauthorized diagnostic requests while the vehicle alarm is primed.

D. Interruption Attack and Cyberattack Scenarios

In this category, we present two attack scenarios that aim to prevent legitimate vehicle owners or passengers from normally using the entry and start system of the vehicle.

Radio Frequency Jamming Attack. In a radio jamming attack, an attacker uses a high-power RF transmitter (e.g., HackRF One, or just a set of keyfobs) operating on common automotive frequencies (e.g., 315 MHz or 433.92 MHz) to flood the wireless spectrum with noise while a driver attempts to lock their parked vehicle using a key fob (viz., Fig. 14). The intentional electromagnetic interference prevents the vehicle's receiver from detecting or parsing the key fob's locking signal. Unaware that the transmission was blocked and assuming the car locked automatically or successfully received the signal, the driver walks away. The attacker then simply walks up to the unsecured, unlocked vehicle, opens the door, and steals contents from the cabin or plugs a malicious OBD-II device.

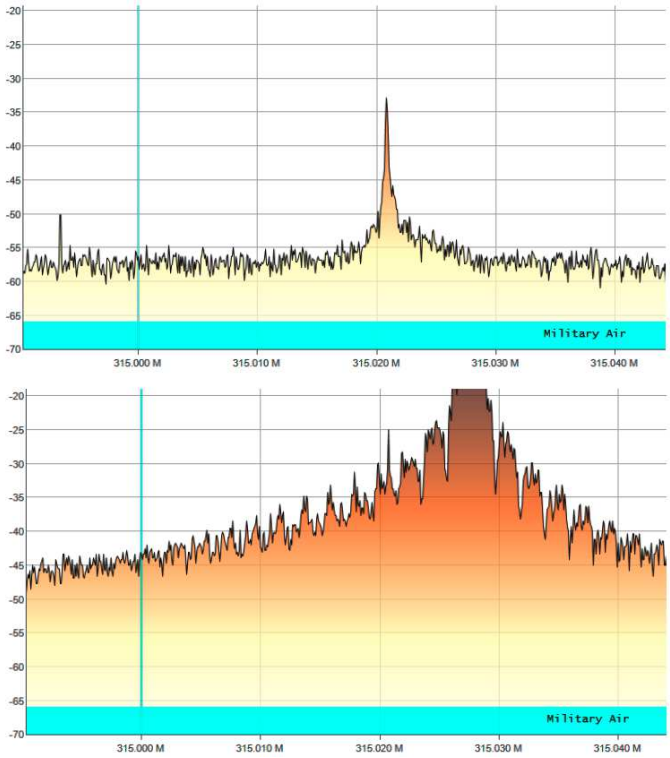

Fig. 14. The locking-signal (captured using HackRF One and displayed on SDR♯ software tool) sent from a 2012 Dodge Grand Caravan's remote controller at 315 MHz (top) and the jammed signal at the same frequency (bottom). The jamming signal was generated by constantly key pressing on another keyfob— these results were obtained in [105].

■ Countermeasures against RF jamming involve multi-channel

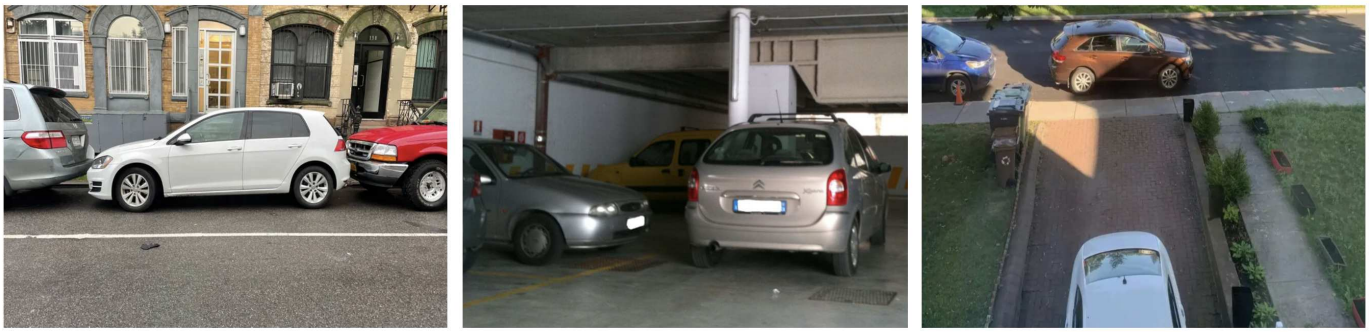

Fig. 15. Different reckless vehicle parking that could be performed by a malicious individual to prevent a person from getting access to their vehicle for personal purposes, e.g., delaying the person from reaching an appointment or a location on time.

frequency hopping and driver notification protocols. Manufacturers can design RKE systems that utilize multi-band frequency hopping (e.g., simultaneously broadcasting across 315 MHz, 433 MHz, and 868 MHz), forcing an attacker to jam wide frequency spectra simultaneously at high power levels. From a vehicle system perspective, Body Control Modules can implement "lock confirmation" feedback loops—such as sounding a distinctive horn chime or flashing exterior indicators only when the door latches physically lock—alerting the driver immediately if the remote lock signal was interrupted by jamming interference.

Vehicle Entry Denial Attack. This attack aims to prevent the legitimate owner from accessing the vehicle by deliberately disabling or obstructing its unlocking mechanisms. One technique involves inserting glue, epoxy resin, chewing gum, metal fragments, or other foreign materials into the mechanical key cylinder, rendering the physical key unusable. Alternatively, an attacker may cut or disconnect the wiring connecting the remote keyless entry (RKE) receiver, damage the antenna, or tamper with the door lock actuator so that pressing the key fob no longer unlocks the doors. Such attacks may be motivated by vandalism, harassment, or to delay the owner while preparing a subsequent theft or robbery. As these actions typically leave little visible evidence beyond a malfunctioning lock or remote entry system, diagnosing the cause may require professional inspection. Another genuine-like scenario could be conducted by a malicious individual by parking another vehicle in such a way so that it immobilizes the vehicle, and prevent or delay target person from reaching an appointment or a location on time (viz., Fig. 15). In severe cases, the owner may be unable to enter the vehicle without specialized tools or emergency roadside assistance.

■ Mitigating vehicle entry denial attacks requires protecting both the mechanical and electronic access mechanisms against physical tampering. Mechanical lock cylinders should incorporate protective shutters and tamper-resistant designs that reduce the likelihood of foreign object insertion, while critical wiring associated with the remote keyless entry system should be routed through protected locations and enclosed within reinforced conduits. Vehicle manufacturers may also implement tamper detection sensors capable of identifying abnormal electrical disconnections or damage to door lock components and notifying the owner through the vehicle's security system or a connected mobile application. Regular inspection of exposed wiring and lock assemblies, particularly after servicing or suspicious incidents, can facilitate early detection of tampering. Finally, providing redundant access methods, such as a concealed emergency mechanical key or authenticated smartphone-based digital key, helps ensure that legitimate users can still access the vehicle if one entry mechanism has been deliberately disabled. Also, vehicle owner should avoid parking their vehicles in parking spots where they can easily be blocked.

VI. Attacks on Vehicles' Electronic and Software System

Logical attacks target the digital components of the vehicle, such as the Electronic Control Units (ECUs), the internal network (CAN bus, LIN bus, etc), or the infotainment software. This generally consists of either injecting malicious messages into the internal vehicle network to override ADAS commands (e.g., forcing an emergency brake in a highway), gaining access via cellular, Wi-Fi, or Bluetooth to modify ADAS settings or disable safety features, or compromising the software update mechanism to push malicious firmware to the perception or planning modules.

A. Interception Attack and Cyberattack Scenarios

In this class of attacks, interception attack scenarios are those in which the attacker passively obtains information from the vehicle's electronic architecture without modifying its behavior. The objective is to steal sensitive information, reverse engineer protocols, prepare for later attacks, or violate vehicle owner, driver, or passengers privacy and confidentiality.

CAN Bus Sniffing. This attack is an active or passive eavesdropping attack where an attacker connects an unauthorized diagnostic tool or malicious hardware implant (such as a rogue dongle hooked to the OBD-II port) directly to the vehicle's Controller Area Network (CAN). Because standard CAN bus architectures broadcast unencrypted messages to every connected Electronic Control Unit (ECU) without message

authentication, an attacker can continuously capture raw traffic frames on the CAN_H and CAN_L lines[5]. By mapping specific CAN IDs to vehicle telemetry—such as steering angles, throttle positions, brake commands, or door-lock states—the attacker can reverse-engineer proprietary ECU protocols to log driver actions or gather the precise payloads required to execute dangerous spoofing and frame-injection attacks later. Fig. 16-left illustrates a configuration for reverse-engineering Android stereo modes using a custom Arduino and MCP2515 CAN bus sniffer to intercept and replay vehicle telemetry.

■ Mitigating CAN bus sniffing requires migrating to modern secure bus architectures, frame-level authentication, and physical diagnostic isolation. Vehicle networks implement SecOC (Secure On-Board Communication) standards—such as AUTOSAR SecOC [204]—which append cryptographic Message Authentication Codes (MACs) and fresh freshness counters to CAN frames, ensuring unauthenticated or intercepted frames cannot be re-injected. At the network architecture level, manufacturers deploy Central Security Gateways that isolate the diagnostic OBD-II port (or the J1939 diagnostic port in trucks) from internal drive-by-wire buses, blocking unauthorized access to safety-critical channels. Furthermore, transition to newer automotive standards like CAN-FD[6] or Automotive Ethernet allows native payload encryption (such as MACsec), ensuring intercepted data frames remain completely unreadable to unauthorized hardware tools.

Diagnostic Data Extraction. In this attack scenario, the attacker gains physical or remote unauthorized access to the vehicle's On-Board Diagnostics port, e.g., OBD-II or J1939, to continuously read, log, and extract sensitive vehicle telemetry using unified diagnostic services (UDS) or standard OBD requests. By connecting a rogue physical hardware dongle, a compromised aftermarket telematics device, or exploiting vulnerabilities in Bluetooth/Wi-Fi OBD/J1939 scanners, the attacker can silently extract real-time vehicle speed, engine parameters (a.k.a., parameters identifiers— PIDs), diagnostic trouble codes (DTCs), VIN details, and historical drive-cycle data. This extracted intelligence exposes driving patterns and vehicle health, while providing the baseline reverse-engineering data necessary to pivot laterally into internal CAN networks or launch secondary firmware flashing attacks against core ECUs. Fig. 16-middle show the use of an OBD-II scanner to read diagnostic data (e.g., DTCs) and engine parameters (PIDs), and to also write data into vehicle ECUs.

■ The mitigation of this attack requires implementing central automotive security gateways with dynamic access control, stateful packet inspection, and diagnostic authentication. Modern vehicle architectures enforce dynamic security access protocols (such as ISO 14229[7] UDS SecurityAccess [205]) that require cryptographic seed-and-key validation or PKI-backed certificate exchanges before non-standard or sensitive diagnostic data streams are released to external devices. Additionally, diagnostic ports are isolated from safety-critical internal buses using hardware-enforced micro-segmentation [206], zero-trust OBD dongle authentication [207], and speed-gated rate limiting—which disables intrusive diagnostic readouts whenever the vehicle is in motion.

ECU Firmware Extraction. Here an attacker recovers the compiled executable binaries and cryptographic keys stored within an Electronic Control Unit's non-volatile memory (such as embedded Flash or EEPROM). By exploiting physical hardware debugging interfaces (like JTAG, SWD, or BDM[8], depending on the microcontroller used within the ECU), extracting external memory chips via chip-off analysis, performing voltage/clock fault injection (glitching) to bypass readout protections, or abusing diagnostic read commands (such as UDS ReadMemoryByAddress) via the CAN bus, the attacker dumps the complete system firmware (viz., Fig. 16-right). Obtaining the raw firmware allows an attacker to reverse-engineer proprietary control algorithms, extract hardcoded secret keys (such as immobilizer or diagnostic seeds), and uncover zero-day software security vulnerabilities to craft persistent malware or unauthorized tuning modifications.

■ Protecting vehicles against ECU firmware extraction requires implementing hardware-enforced memory protections and secure diagnostic access controls. Microcontrollers must permanently disable or cryptographically lock hardware debug interfaces (JTAG/SWD) using production fuses, while utilizing microcontrollers with internal Flash memory encryption to neutralize physical chip-off probing. At the software level, diagnostic protocols must enforce strong authentication (such as ISO 14229 UDS SecurityAccess or PKI certificate validation) before permitting memory read or firmware upload commands. Additionally, hardware fault-injection detection circuits, secure boot routines rooted in Hardware Security Modules (HSMs), and full-chip Flash encryption prevent attacker from leveraging glitching techniques or unauthorized readout routines to dump non-volatile memory.

Automotive Ethernet Packet Sniffing. Here the attacker taps into the high-speed Ethernet links connecting domain controllers, ADAS perception units, and central gateways. By physically bridging the unencrypted differential pair wiring or compromising an edge node on the Ethernet network, the attacker passively captures raw IP/Ethernet frames. Because Automotive Ethernet carries critical data using protocols like SOME/IP (Scalable service-Oriented MiddlewarE over IP), DoIP (Diagnostics over Internet Protocol), and raw AVB/TSN (Audio Video Bridging / Time-Sensitive Networking) video

[5]CAN-High (CAN_H) and CAN-Low (CAN_L) form a differential wire pair in CAN bus networks, transmitting data by altering their relative voltage difference to provide high resistance to electromagnetic interference.

[6]CAN-FD (Controller Area Network Flexible Data-Rate) is an enhanced version of the traditional CAN protocol (ISO 11898-1) designed to meet the high bandwidth demands of modern vehicle systems.

[7]ISO 14229-1:2026 Road vehicles — Unified diagnostic services (UDS) — Part 1: Application layer (https://www.iso.org/standard/87962.html).

[8]JTAG (Joint Test Action Group), SWD (Serial Wire Debug), and BDM (Background Debug Mode) are microcontroller-dependent hardware debug interfaces used for low-level firmware flashing and in-circuit silicon testing.



Fig. 16. From left to right: Reverse-engineering Android stereo modes using a custom Arduino and MCP2515 CAN bus sniffer to intercept and replay vehicle telemetry; the use of an OBD-II scanner to read diagnostic data (e.g., DTCs) and engine component measurments (e.g., PIDs), and to also write data into vehicle ECUs; and a bench mode flashing session using the Magic Motorsport FLEX and FlexBox interface to read firmware from a Magneti Marelli ECU.

streams, sniffing this traffic allows an attacker to reconstruct high-bandwidth camera feeds, sensor point clouds (captured from the vehicle's LiDAR), and control commands, enabling deep protocol reverse-engineering, passenger privacy exposure, and the crafting of targeted network injection attacks.

■ In this situation, vehicle architectures must enforce hardware-accelerated link-layer encryption using MACsec (IEEE 802.1AE), which encrypts Ethernet frames directly at the Physical/Data Link boundary with minimal latency. At the network architecture level, Ethernet switches should implement strict micro-segmentation [206], Virtual Local Area Networks (VLANs), and static MAC address binding to ensure traffic is strictly routed only between authorized endpoints (no ARP poisoning). Furthermore, upper-layer protocols must implement TLS (Transport Layer Security), DTLS (Datagram Transport Layer Security), or QUIC (Quick UDP Internet Connections) for transport security, alongside strict switch-level port security configurations that disable unused ports and flag unauthorized physical connections or promiscuous mode behavior in real time.

Bluetooth Communication Interception. This attack occurs when an attacker eavesdrops on or tampers with the short-range wireless channels connecting smartphones, tire pressure monitoring systems (TPMS), or diagnostic dongles to the vehicle's In-Vehicle Infotainment (IVI) or telematics domain. By using software-defined radios (SDRs) or specialized Bluetooth sniffers to exploit weak pairing protocols (such as legacy Just Works pairing or hardcoded PINs), implementation flaws in Bluetooth Classic/LE stacks, or unencrypted telemetry payloads, the attacker captures transmitted audio, contacts, location logs, and diagnostic diagnostic requests. Beyond severe passenger privacy breaches, intercepting these wireless data channels allows an attacker to execute various attacks to compromise different security services [211].

■ Mitigating Bluetooth interception requires enforcing Secure Connections with Passkey Entry or Out-of-Band (OOB) pairing modes based on Elliptic Curve Diffie-Hellman (ECDH) key exchange to prevent passive eavesdropping and MitM impersonation. At the application layer, all high-privilege traffic—such as mobile key exchanges, diagnostic commands, and telematics telemetry—must be encrypted using end-to-end transport protocols (like TLS over Bluetooth SPP/GATT) backed by Hardware Security Module (HSM) keys. Furthermore, vehicle manufacturers must enforce strict domain isolation to isolate Bluetooth controllers behind central security gateways, employ short pairing time-out windows, and regularly deploy over-the-air (OTA) security patches to resolve protocol stack vulnerabilities.

Wi-Fi Communication Interception. Here an attacker eavesdrops on or tampers with the vehicle's wireless local area network (WLAN) links—such as the vehicle's internal Wi-Fi access point used for passenger infotainment, phone mirroring (like wireless Apple CarPlay and Android Auto), or external drive-thru/home network syncing. By deploying software-defined radios or wireless sniffing interfaces near the vehicle, an attacker can exploit weak access point credentials, outdated security protocols (e.g., WEP, WPA, or WPA2-Personal with weak passwords), or implementation flaws in the Wi-Fi driver stack. Capturing this unencrypted or weakly encrypted traffic allows the attacker to steal sensitive user data, monitor mirrored device screens, intercept location logs, or perform Man-in-the-Middle (MitM) packet injection to pivot from the infotainment Wi-Fi network toward internal telematics and vehicle gateways. An extensive survey of Wi-Fi attacks on different security services can be found in [211].

■ To secure in-vehicle Wi-Fi links against unauthorized interception, vehicle networks must mandate WPA3-Enterprise or WPA3-Personal security standards, leveraging Simultaneous Authentication of Equals (SAE) to protect key exchanges against offline dictionary attacks. Application-layer communications—such as phone-mirroring streams and diagnostic syncs—must employ mandatory end-to-end encryption using for instance TLS 1.3 with Hardware Security Module (HSM)-backed cryptographic certificates. Furthermore, system designers must enforce strict network segmentation and firewall controls on the vehicle gateway to isolate the guest Wi-Fi network entirely from safety-critical CAN and Automotive Ethernet

domains, disabling unauthenticated peer-to-peer connections (like Wi-Fi Direct) when not actively in use.

Cellular Telemetry Interception. In this cyberattack scenario, the attacker passively eavesdrops on or actively intercepts long-range cellular transmissions (such as 4G LTE—Long Term Evolution, or 5G NR—New Radio) flowing between the vehicle's Telematics Control Unit (TCU) and cloud servers [217]. By deploying rogue base stations (IMSI Catchers/stingrays), exploiting weak carrier APN configurations, or taking advantage of unencrypted cellular transport pipes, the attacker captures high-volume telemetry streams including vehicle diagnostic codes, driving history, real-time GPS tracking data, and user profiles. Silently harvesting this cellular data compromises driver privacy on a fleet-wide scale, exposes proprietary OEM (Original Equipment Manufacturer) backend protocols, and provides the necessary transport layer intelligence to mount Man-in-the-Middle (MitM) packet injection or hijack remote over-the-air (OTA) software update channels [148]–[154].

■ The protection against this attack requires enforcing mandatory end-to-end transport encryption—such as TLS 1.3, QUIC, or IPsec tunnels—backed by Hardware Security Modules (HSMs) [67] and embedded SIMs (eSIMs/iSIMs) directly integrated into the TCU. Telematics traffic must be isolated using private Access Point Names (APNs) and encrypted carrier VPNs (Virtual Private Networks)that strictly enforce Mutual TLS (mTLS) authentication with public key infrastructure (PKI) certificates before any telemetry packet is routed. Additionally, cellular baseband modems should enforce strict 5G Standalone (SA) security configurations to resist IMSI catcher downgrades [218]–[220], while cloud infrastructure runs Vehicle Security Operations Center (vSOC) anomaly detection to flag rogue base station connections or unusual telemetry routing in real time.

OTA Firmware Package Interception. This attack occurs when an attacker eavesdrops on or intercepts Over-The-Air (OTA) software update transmissions sent from the manufacturer's backend servers to the vehicle's Telematics Control Unit (TCU). By exploiting unencrypted transport protocols, compromised cellular/Wi-Fi networks, or executing Man-in-the-Middle (MitM) positioning, the attacker captures the binary software payload before it reaches the vehicle's central gateway. Intercepting these raw updates allows an attacker to reverse-engineer proprietary firmware code, extract hardcoded security keys or internal API endpoints, identify unpatched software vulnerabilities, or attempt to modify the binary file to inject malicious logic into safety-critical ECUs.

■ To secure OTA updates against interception and tampering, vehicle manufacturers implement robust end-to-end security architectures based on standards like Uptane. Update packages are individually encrypted and digitally signed at the source using asymmetric public-key cryptography (such as RSA or ECDSA) managed within Hardware Security Modules (HSMs), ensuring the payload remains completely encrypted during transit over TLS 1.3, QUIC, or IPsec cellular connections. Before flashing any update, the receiving ECU verifies the cryptographic signature, checks payload integrity against fresh metadata timestamps, and validates the package against secure boot keys to reject any intercepted, modified, or outdated firmware binaries [148]–[154].

Infotainment Storage Extraction. This occurs when an attacker gains physical access to the In-Vehicle Infotainment (IVI) unit or its removable flash memory chips (such as eMMC or SD cards) to dump stored user data and system binaries. By extracting memory chips using chip-off techniques, connecting directly to board-level test points (such as JTAG or UART[9]), or exploiting bootloader vulnerabilities, the attacker reads the unencrypted file systems directly from hardware. This reveals sensitive personal driver information—including call logs, contact lists, paired Bluetooth keys (thier Bluetooth MAC addresses and user-friendly names), Wi-Fi credentials, location histories, and saved navigation destinations—while exposing proprietary IVI system binaries, reverse-engineerable software stacks, and API (Application Programming Interface) tokens used for backend telematics access.

■ To protect against this attack, IVI architectures must implement full-disk encryption (FDE) or hardware-backed file-based encryption (FBE) integrated directly into the storage controller (e.g., eMMC Inline Encryption). Cryptographic keys must be bound to a Hardware Root of Trust and managed securely by an onboard Hardware Security Module (HSM) or Secure Enclave, ensuring that data cannot be decrypted if the memory chip is removed or read offline. Furthermore, manufacturers should lock down hardware debugging interfaces (permanently disabling JTAG/UART access in production units), enforce Secure Boot to prevent running custom dumping tools, and ensure that sensitive user credentials and tokens are stored in tamper-proof hardware storage.

V2X Message Sniffing. This attack is a passive eavesdropping attack where an attacker monitors unencrypted or publicly broadcasted Vehicle-to-Everything (V2X) wireless communications—such as Cooperative Awareness Messages (CAMs) or Basic Safety Messages (BSMs)—over DSRC (IEEE 802.11p) or C-V2X (Cellular V2X) interfaces. Because these messages continuously transmit rich, real-time spatial data including precise GPS coordinates, velocity, heading, and acceleration, an attacker can for example passively capture these radio packets to track individual vehicles across geographic areas, reconstruct traffic patterns, and build detailed behavioral profiles of drivers without needing to physically follow them or compromise internal vehicle buses.

■ To mitigate tracking while maintaining open safety broadcasting, V2X standards rely on Public Key Infrastructure

[9]UART (Universal Asynchronous Receiver-Transmitter) is a physical serial interface commonly used in hardware reverse engineering to establish a low-level console connection to embedded storage controllers, enabling direct extraction of firmware and raw flash memory chips.

(PKI) with Dynamic Pseudonym Certificates that automatically change a vehicle's temporary identifiers and cryptographic credentials at regular intervals or distance thresholds. This pseudonym cycling, paired with randomized MAC-address updates and spatial-temporal obfuscation (such as micro-delays or noise injected into non-critical telemetry), breaks the linkability of sequential safety messages, making it cryptographically infeasible for an eavesdropper to reconstruct long-term vehicle trajectories or tie broadcasted data back to a permanent vehicle identity.

B. Fabrication Attack and Cyberattack Scenarios

Fabrication attacks are those in which the attacker injects counterfeit information, messages, software, or identities into the vehicle's electronic ecosystem (i.e., CAN bus, LIN bus, Flexray bus, infotainment system, OBD-II, J1939, etc), causing ECUs to process false data as legitimate.

The Jeep Cherokee Remote Takeover. This landmark cyber-physical exploit—popularized by security researchers Charlie Miller and Chris Valasek in [69] where they demonstrated how an unauthenticated network entry point can be pivoted to compromise safety-critical physical systems. The attackers targeted an exposed D-Bus port (TCP Port 6667) within Chrysler's Uconnect infotainment system, accessible wirelessly over Sprint's 3G/LTE cellular network. By exploiting a memory corruption vulnerability in the head unit, they executed remote code execution (RCE) on the radio microchip. From there, the attackers flashed modified firmware onto the vehicle's V850 co-processor, bridging the isolated infotainment network to the critical Controller Area Network (CAN bus). This granted them full read-and-write control over raw CAN frames, enabling them to inject unauthorized commands directly into Electronic Control Units (ECUs) to kill the engine, disable transmission gearing, alter steering inputs, and manipulate active braking while the target vehicle was traveling at highway speeds. This research resulted in a recall of 1.4 million vehicles by Fiat Chrysler and remains one of the defining real-world examples of a cyber-physical supply-chain/network architecture failure.

■ Mitigating cross-domain CAN bus compromises requires enforcing strict structural isolation between telematics/infotainment subsystems and safety-critical powertrain networks. Modern automotive architectures address this by deploying Hardware Security Modules (HSMs) and secure Central Gateway (CGW) modules equipped with deep packet inspection (DPI). These gateways enforce message filtering and rate-limiting rules, instantly dropping unauthorized CAN frames that attempt to bridge non-critical buses (such as infotainment) to safety-critical buses (such as steering or braking). Furthermore, automakers must implement SecOC (Secure Onboard Communication)—which uses Message Authentication Codes (MACs) and freshness counters to cryptographically sign every command sent between ECUs—alongside cellular network firewalls and Cryptographic Firmware Code Signing to prevent unauthorized remote firmware updates over the air.

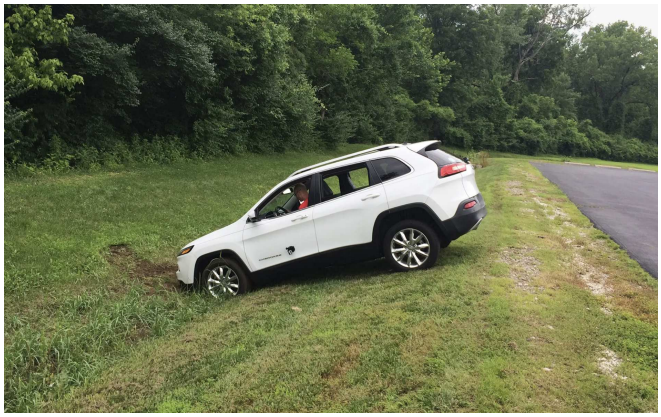

Fig. 17. A white Jeep Cherokee sits stuck in a grassy ditch after cybersecurity researchers remotely hijacked its controls—including cutting the transmission and brakes—to demonstrate critical automotive security vulnerabilities [69].

CAN Message Injection. CAN Message Injection occurs when an attacker transmits unauthorized data frames onto a vehicle's Controller Area Network (CAN) to trigger unintended hardware or software actions. By connecting to physical access points (such as the OBD-II port, exposed headlights/sensor wiring harnesses (viz., Fig. 18), or compromised aftermarket dongles) or by pivoting through a hacked wireless domain like the Infotainment or Telematics unit, the attacker injects forged CAN frames with valid IDs. Because native CAN protocol lacks message source authentication or origin verification, target Electronic Control Units (ECUs) accept these forged commands as legitimate—allowing the attacker to execute critical vehicle functions such as unlocking doors, disabling brakes, disabling airbags, manipulating instrument clusters, or controlling steering and acceleration.

■ To fend off this attack, automotive architectures implement message-level authentication standards like SecOC (Secure On-Board Communication), which appends cryptographic Message Authentication Codes (MACs) and freshness counters to every transmitted frame to reject unauthorized or replayed messages [199]. At the network architecture level, Central Security Gateways (mother ECU [174]) separate diagnostic interfaces (like OBD-II) from critical drive-by-wire buses, enforcing strict firewalls [179], rate limiting, and CAN Bus Intrusion Detection Systems (IDS) [166]–[170] to filter anomalies. Furthermore, modern vehicle designs are transitioning toward CAN-FD (Controller Area Network— Flexible Data-Rate) and Automotive Ethernet, which natively support robust payload encryption and cryptographically verified network segmentation.

Diagnostic Message Injection. Here the attacker transmits unauthorized Unified Diagnostic Services (UDS) or OBD-II diagnostic requests directly onto a vehicle's internal networks (such as CAN, CAN-FD, or DoIP) to manipulate Electronic Control Unit (ECU) behaviors. By exploiting unprotected diagnostic routines or bypassing authorization steps via physical ports (OBD-II, exposed wiring harnesses) or a compromised

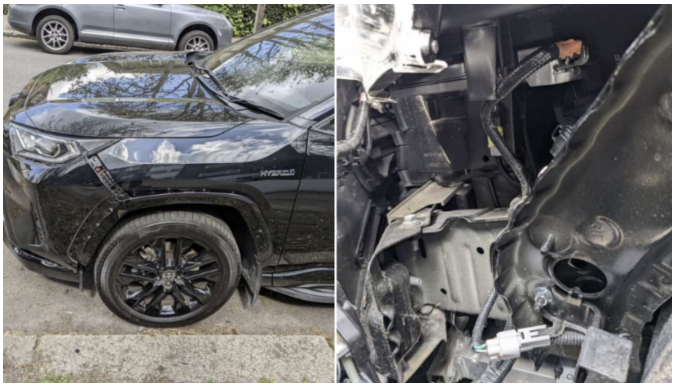

Fig. 18. Stealing a nice car in 2022: beneath the peeled liner of a Toyota RAV4 lies the targeted headlight connector, where thieves plug in CAN injection tools. By tapping straight into the car's network lines, attackers can bypass the immobilizer to unlock and start the vehicle in minutes [221].

wireless gateway, the attacker sends high-privilege diagnostic frames. Because diagnostic protocols can override normal operational logic, these injected messages can force ECUs into bootloader modes, execute actuator tests (e.g., triggering door locks or wiping fault memory), alter calibration parameters, or initiate unauthorized firmware flashing while the vehicle is stationary or in motion.

■ To defend against diagnostic message injection, vehicle architectures mandate strong challenge-response authentication standards (such as ISO 14229[10] UDS SecurityAccess [205]) before permitting sensitive diagnostic services. Central Security Gateways isolate physical diagnostic ports from drive-by-wire networks using stateful packet inspection, strict message filtering [179], and speed-gated rate limiting—blocking intrusive diagnostic routines whenever the vehicle is in motion [166]–[170]. Additionally, diagnostic traffic must incorporate message freshness counters and cryptographic signatures [174], while ECU software enforces strict operational state checks to reject high-risk service requests outside controlled service environments.

ECU Identity Spoofing. ECU Identity Spoofing occurs when a rogue hardware device or a compromised Electronic Control Unit (ECU) impersonates a legitimate ECU on an in-vehicle network (such as CAN, CAN-FD, or Automotive Ethernet) by transmitting messages using the victim ECU's distinct network identifiers or IP/MAC addresses. Because traditional CAN architectures rely solely on arbitration IDs rather than sender authentication, an attacker can transmit forged telemetry or control commands under the guise of a critical system component (e.g., spoofing the Brake Control Module or Gateway). Receiving ECUs accept these forged frames as authentic, allowing the attacker to override safety mechanisms, bypass access control logic, or suppress legitimate safety alerts across the vehicle.

[10]ISO 14229-1:2026 Road vehicles — Unified diagnostic services (UDS) — Part 1: Application layer (https://www.iso.org/standard/87962.html).

■ Mitigating ECU identity spoofing requires implementing frame-level cryptographic authentication and hardware-backed sender validation across the vehicle network [174]. Systems using SecOC (Secure On-Board Communication) append cryptographic Message Authentication Codes (MACs) and unique freshness counters to each frame, ensuring that receiving ECUs reject any message not generated using the legitimate sender's Hardware Security Module (HSM)-protected key [199]. On Ethernet-based networks, switch-level port security—such as static MAC/IP binding, IEEE 802.1X network access control, and link-layer encryption via MACsec—ensures rogue nodes cannot masquerade as authorized ECUs. Additionally, centralized Intrusion Detection Systems (IDS) monitor message frequency, bus electrical characteristics (voltage profiling), and physical port origins to detect and isolate impersonating nodes in real time [166]–[170].

Replay Attack in CAN. Replay Attack in CAN occurs when an attacker captures legitimate data frames previously transmitted across the vehicle's CAN and retransmits them at a later time to trick ECUs into executing unauthorized actions. Because standard CAN protocol messages lack timestamping, freshness counters, or cryptographic sequence validation, an attacker equipped with a simple bus sniffing and injection tool (such as a compromised OBD-II dongle or tapped sensor wire) can record valid commands—such as "unlock doors," "start engine," or "disable traction control"—and replay them verbatim. The target ECUs process these replayed frames as valid operational requests, enabling keyless entry theft, unauthorized vehicle start-up, or dangerous manipulation of driving dynamics without needing to reverse-engineer the payload contents.

■ To neutralize CAN replay attacks, vehicle architectures must enforce message freshness and cryptographic origin validation using standards such as AUTOSAR SecOC (Secure On-Board Communication). SecOC appends a Message Authentication Code (MAC) generated with a secret key and a dynamically incrementing Freshness Value (such as a monotonic counter or synchronized timestamp) to every CAN frame. Receiving ECUs verify both the MAC and the freshness counter; if an incoming frame contains an outdated or previously processed counter, the message is instantly dropped as a replay attempt. Additionally, Central Security Gateways enforce strict rate-limiting, message frequency monitoring, and stateful Intrusion Detection Systems (IDS) to flag and block anomalous frame bursts on the bus [166]–[170].

Fake OTA Update Notification. Fake OTA Update Notification is a social-engineering and spoofing attack where an attacker delivers a fraudulent software update prompt to the vehicle's In-Vehicle Infotainment (IVI) or mobile companion application. By deploying rogue cellular base stations, executing Wi-Fi Man-in-the-Middle (MitM) positioning, or exploiting vulnerabilities in telematics push-notification APIs, the attacker tricks the driver into accepting a malicious "critical system update". When the unsuspecting user approves the

prompt, the vehicle initiates a connection to an attacker-controlled server to download a compromised firmware payload, or the prompt tricks the driver into granting high-privilege access rights to an untrusted application—paving the way for remote arbitrary code execution, ransomware installation, or vehicle control hijacking [69].

■ To protect against fake OTA update notifications, vehicle architectures rely on cryptographic authenticity verification and centralized trust frameworks based on standards like Uptane[11]. Update notification manifests and download links must be digitally signed by the vehicle manufacturer's backend keys using a Hardware Security Module (HSM) and delivered over secure, mutually authenticated TLS 1.3, QUIC, or IPsec channels. The telematics gateway and central update manager cross-check incoming update manifests against signed metadata counters to reject unauthorized, outdated, or altered notification prompts before displaying them on the user interface. Furthermore, critical system updates mandate background cryptographic validation and secure boot checks [181]–[183] before presenting any confirmation prompt to the driver, ensuring users cannot accidentally approve unverified software packages.

C. Modification Attack and Cyberattack Scenarios

Modification attacks are those in which the attacker alters legitimate software, firmware, configuration, or data already stored or transmitted within the vehicle.

ECU Firmware Modification. ECU Firmware Modification occurs when an attacker tampers with or overwrites the compiled binary code executing inside an Electronic Control Unit's (ECU) flash memory to execute unauthorized, persistent logic. By exploiting vulnerabilities in Over-The-Air (OTA) update channels [148]–[154], breaking UDS diagnostic flashing routines (RequestDownload / TransferData), or leveraging physical hardware debug interfaces (such as JTAG or BDM[12]), the attacker replaces legitimate vendor firmware with a modified payload. This allows an adversary to disable safety interlocks, bypass immobilizer anti-theft checks, modify engine timing or torque limits, or install persistent rootkits that can inject arbitrary CAN messages, eavesdrop on vehicle communications, or override driver controls on demand [69].

■ To defeat unauthorized firmware modifications, automotive microcontrollers implement a hardware-anchored Secure Boot [181]–[183] chain rooted in an onboard Hardware Security Module (HSM) or Secure Hardware Extension (SHE) [184]–[187]. During every startup and flashing sequence, the secure bootloader calculates and verifies the digital signature (e.g., ECDSA or RSA[13]) of the firmware image against a immutable public key fused into the hardware during manufacturing; if the signature check fails or integrity is compromised, the ECU refuses to execute the binary (which remains an attack against availability). Furthermore, diagnostic flashing protocols mandate strong challenge-response authentication (such as ISO 14229 UDS SecurityAccess or ISO 21107 PKI certificates), while memory protection units (MPUs) and hardware flash lock bits prevent runtime memory tampering and unauthorized flash write operations.

ECU Parameter Reconfiguration. This attack occurs when an attacker alters non-volatile operational settings, look-up tables (calibration maps), or feature flags stored within an Electronic Control Unit's memory without re-flashing the full firmware binary. By issuing diagnostic service requests over the CAN bus via physical ports or compromised telematics units, the attacker overrides pre-programmed operational bounds. By manipulating critical parameters—such as speed governor limits, engine fuel maps, torque thresholds, sensor calibration offsets, or driver-assistance sensitivity values—the adversary can cause mechanical strain, bypass emissions interlocks, disable safety-critical alerts, or induce unstable driving dynamics under specific conditions.

■ Defending against unauthorized ECU parameter reconfiguration requires strict access controls on calibration memory blocks and message authentication on diagnostic commands. Systems compliant with ISO 14229-1 (UDS SecurityAccess) and ISO 21107 enforce asymmetric PKI certificate exchanges or cryptographic challenge-response protocols before enabling write-access services to configuration identifiers (DIDs). Furthermore, non-volatile memory storing critical calibration variables must be protected using cryptographic Message Authentication Codes (MACs) managed by an onboard Hardware Security Module (HSM). At the network level, central security gateways validate stateful conditions (such as ensuring speed-gated lockouts prevent any parameter modifications while the vehicle is operating) and employ Intrusion Detection Systems (IDS) to flag anomalous configuration requests [166]–[170].

CAN Message Manipulation. This is an on-the-fly frame modification attack, which occurs when an attacker actively intercepts, alters, or suppresses legitimate Controller Area Network (CAN) frames as they travel across the bus. Unlike passive eavesdropping or simple frame injection, this attack typically involves compromised hardware, inline tapping devices, or bridge nodes that perform a "Man-in-the-Middle" (MitM) payload modification—frequently using CAN bus arbitration tricks (such as bit-overwriting or frame-cancellation via error flags). By modifying sensor values or status flags in real time (e.g., changing wheel speed readings, altering battery temperature telemetry, or falsifying driver-input signals), the

[11]Uptane is an open-source, IEEE-standardized security framework (IEEE-ISTO 6100.1.0.0) specifically designed to secure Over-The-Air (OTA) software updates in connected vehicles.

[12]A BDM (Background Debug Mode) interface is an on-chip, low-level hardware debugging and programming interface primarily developed by Motorola (now NXP / Freescale) for its 16-bit and 32-bit microcontroller families (such as the HCS08, HCS12, CPU32, and MPC5xx series).

[13]Standard public-key (asymmetric) cryptosystems that enable secure key exchange and digital signatures; RSA (Rivest Shamir Adelman) relies on the difficulty of factoring large prime products, whereas ECDSA (Elleptic Curve Digital Signature Algorithm) uses elliptic-curve mathematics to offer equivalent security with significantly smaller key sizes.

attacker tricks receiving Electronic Control Units (ECUs) into making dangerous dynamic decisions, such as abruptly triggering emergency braking or ignoring critical safety faults.

■ Mitigating CAN message manipulation requires validating message integrity, freshness, and sender authenticity at the frame level using AUTOSAR SecOC (Secure On-Board Communication). SecOC appends a cryptographic Message Authentication Code (MAC) and dynamic freshness counter to every frame [199], ensuring that any inline modification of the payload renders the MAC invalid and causes the receiving ECU to immediately reject the frame [174]. At the hardware architecture level, modern vehicle networks deploy Central Security Gateways, point-to-point switches, and bus-level Intrusion Detection Systems (IDS) that monitor physical signal voltages, timing jitter, and bus error patterns to isolate and disable tampered lines or compromised ECUs in real time.

Diagnostic Data Modification. Diagnostic Data Modification occurs when an attacker tampers with, alters, or suppresses diagnostic payloads—such as Unified Diagnostic Services (UDS) responses or On-Board Diagnostics (OBD-II) parameter IDs (PIDs)—in transit or within temporary ECU buffers. By placing an inline interception hardware node on the diagnostic bus or compromising a central gateway/OBD dongle, the attacker modifies return values for critical operational parameters, including diagnostic trouble codes (DTCs), sensor readings (e.g., fluid temperatures, brake pad wear, emissions telemetry), or ECU identification data. By falsifying this diagnostic telemetry, the attacker tricks vehicle technicians or automated telematics health monitoring tools into misdiagnosing safety-critical system status, masking underlying hardware failures, bypassing state emissions and safety inspections, or inducing incorrect fail-safe operational modes.

■ To protect diagnostic data from unauthorized modification, automotive architectures implement end-to-end cryptographic integrity and authentication for all diagnostic traffic using standards like ISO 21107 and ISO 14229-1 (UDS). Diagnostic messages transported over DoIP (Diagnostic over IP) or CAN-FD must mandate TLS 1.3 or SecOC (Secure On-Board Communication) payload protection, utilizing Message Authentication Codes (MACs) and freshness counters to instantly detect and reject modified frames. Furthermore, Central Security Gateways enforce strict packet-inspection rules to block invalid response formats, while onboard Hardware Security Modules (HSMs) cryptographically sign critical DTC records and maintenance logs stored in non-volatile memory to prevent local or in-transit alteration.

OTA Firmware Tampering. Here the attacker modifies, injects malicious code into, or corrupts an Over-The-Air (OTA) firmware update package before or during its installation on a vehicle's Electronic Control Unit (ECU). Unlike passive OTA interception, this is an active attack where an attacker alters the binary payload, alters its metadata (e.g., version numbers or flash instructions), or substitutes the vendor's image with a trojanized binary. By exploiting compromised backend cloud build pipelines, weak cryptographic signing implementations, or executing a Man-in-the-Middle (MitM) payload manipulation during wireless transit, the attacker tricks the vehicle's gateway or target ECU into executing malicious code. Successful tampering can permanently brick safety-critical ECUs, disable immobilizers, create persistent remote access backdoors, or dangerously alter physical vehicle behavior during operation.

■ Defending against OTA firmware tampering requires implementing strict, layered compromise-resilient update frameworks such as Uptane (IEEE 2886 standard). Update packages must be signed by multiple isolated offline keys stored within Hardware Security Modules (HSMs) at the manufacturer level [184]–[187], ensuring that a single compromised server cannot produce a validly signed update. Before flashing, the vehicle's primary OTA manager and target ECUs independently verify the update's asymmetric cryptographic signatures (e.g., ECDSA/RSA), validate payload integrity against cryptographic hashes (e.g., SHA-256/SHA-3), and check freshness metadata to block rollback and freeze attacks. Finally, hardware-anchored Secure Boot [181]–[183] on each ECU validates the signature of the newly flashed binary from an immutable root-of-trust before allowing the firmware to execute.

Navigation Map Modification. This attack occurs when an attacker tampers with, alters, or corrupts the spatial database and vector map layers used by In-Vehicle Infotainment (IVI) or Advanced Driver Assistance Systems (ADAS). By exploiting vulnerable Over-The-Air (OTA) map updates, corrupting files on USB/SD media used for manual updates, or executing Man-in-the-Middle (MitM) positioning on live map tile streams, the adversary modifies underlying map data. By altering speed limit attributes, turning restrictions, road geometry, or lane-level topology, the attacker causes the vehicle's navigation engine to calculate dangerous routes. In autonomous or semi-autonomous vehicles, falsified map data tricks localization and sensor fusion algorithms into misinterpreting physical surroundings, triggering unexpected lane changes, improper speed adjustments, or sudden erratic maneuvers.

■ To prevent this form of attack, map providers and automotive OEMs enforce end-to-end cryptographic integrity and authenticity using standards like NDS (Navigation Data Standard) and Uptane-based update frameworks. Map files, tiles, and database patches must be digitally signed by the provider's backend Hardware Security Module (HSM) using asymmetric public-key cryptography (such as ECDSA or RSA). The vehicle's update manager and ADAS domain controller cryptographically verify these signatures, payload hashes, and version timestamps before writing data to system storage. Furthermore, high-definition (HD) map files are stored on encrypted file systems, while perception-based sensor fusion engines continually perform cross-validation—comparing

live camera, radar, and LiDAR sensor inputs against map database features to detect and reject spatial map anomalies in real time.

Cryptographic Key Modification. Here attacker tampers with, overwrites, or substitutes the cryptographic keys or root certificates stored within a vehicle's Electronic Control Units (ECUs), gateway modules, or telematics nodes. By exploiting memory corruption vulnerabilities, leveraging unauthorized hardware access (such as JTAG), or bypassing unprotected flash write operations, the adversary replaces legitimate vendor public keys or secret symmetry keys with attacker-controlled keys. Once compromised, the modified key material causes the vehicle's safety-critical components to trust malicious firmware binaries, validate forged diagnostic commands, accept rogue Over-The-Air (OTA) updates, or accept spoofed CAN/SecOC messages, entirely undermining the vehicle's security architecture.

■ To protect cryptographic keys against unauthorized modification, automotive hardware architectures isolate key material inside dedicated Hardware Security Modules (HSMs) or Secure Hardware Extensions (SHE) equipped with hardware-enforced memory isolation [184]–[187]. Public keys, root certificates, and master keys must be stored in One-Time Programmable (OTP) eFuse arrays or secure flash blocks protected by strict hardware lock bits that prevent overwriting after factory provisioning. Furthermore, any key update operational protocol must mandate a cryptographic key-exchange handshake requiring multi-party authorization or signature verification against an immutable, hardware-anchored Root of Trust (RoT) before updating key storage registers.

Remote ECU Compromise. A remote ECU compromise attack targets vulnerable externally accessible vehicle components, such as infotainment systems, telematics units, Wi-Fi modules, Bluetooth interfaces, or cellular communication gateways, to obtain unauthorized execution privileges within the vehicle's electronic architecture. After exploiting a software vulnerability [69], the attacker establishes persistent code execution and pivots through the in-vehicle network toward safety-critical Electronic Control Units (ECUs). By bypassing network isolation mechanisms, the compromised ECU can transmit unauthorized CAN or Automotive Ethernet messages, reprogram controllers, disable security mechanisms, and manipulate vehicle functions including steering, braking, transmission, and acceleration. Unlike attacks that merely inject isolated messages or disrupt communications, a remote ECU compromise grants persistent administrative control over one or more vehicle subsystems, allowing attackers to execute arbitrary commands while remaining largely invisible to the driver.

■ Defending against remote ECU compromise requires a defense-in-depth architecture that isolates externally exposed components from safety-critical vehicle networks. Infotainment, telematics, Bluetooth, Wi-Fi, and cellular modules should be separated from CAN and Automotive Ethernet domains using secure gateways with strict message filtering and authentication policies. ECUs should implement secure boot, code signing, runtime integrity verification, and hardware security modules (HSMs) to prevent unauthorized software execution. Manufacturers should perform secure software development, continuous vulnerability assessment, and timely over-the-air (OTA) security updates to eliminate exploitable flaws before they can be weaponized. In addition, in-vehicle intrusion detection systems (IDSs) [166]–[170] should monitor abnormal network behavior, lateral movement, and unauthorized CAN message generation, allowing compromised ECUs to be isolated before attackers obtain full control of vehicle functions.

D. Interruption Attack and Cyberattack Scenarios

Interruption attacks aim to disrupt the availability of electronic components, software services, or communications, preventing ECUs, infortaiment systems, CAN bus, OBD-II diagnostic port, and similar subsystems from operating correctly or causing them to enter a degraded or fail-safe state.

Connection Deprivation Attack. This attack occurs when an attacker actively drops or prevents wireless connections between connected vehicular endpoints—such as smartphones, wireless diagnostic OBD-II dongles, or TPMS sensors—and the vehicle's In-Vehicle Infotainment (IVI) or Telematics Control Unit (TCU). Using Software-Defined Radios (SDRs) or specialized wireless chips (e.g., Wi-Fi Alpha cards, Wi-Fi pineapple, Flipper Zero, and Ubertooth One) operating in monitor mode, the attacker exploits management frame vulnerabilities in Wi-Fi (IEEE 802.11) and connection-state flaws in Bluetooth Classic/LE to cause connection deprivation through Wi-Fi deauthentication [211]–[216] and Bluetooth disconnection [208]–[211]. In TABLE II, we illustrate the success and failure of Bluetooth connection deprivation attack on passenger vehicles from different makes and models. These resultes were obtained in [208].

■ Defending against wireless deauthentication and protocol-level disconnections requires validating management traffic, hardening handshake protocols, and enforcing resilient communication boundaries within the vehicle network. To neutralize spoofed teardown requests, vehicular Wi-Fi networks must implement Protected Management Frames (PMF— cf. IEEE 802.11w amandment[14]) to cryptographically sign deauthentication and disassociation frames, while Bluetooth links should utilize Bluetooth LE Secure Connections with Elliptic Curve Diffie-Hellman (ECDH) pairing and Link Layer Encryption (viz., Securiyt Mode 2 and 3 in TABLE II) to block injected session-termination commands. Complementing this cryptographic baseline, internal wireless Intrusion Detection Systems (wIDS) embedded in the Telematics Control Unit should

[14]IEEE 802.11w is a wireless security standard, which through PMF (Protected Management Frames), applies cryptographic integrity and encryption to robust management frames (such as deauthentication, disassociation, and action frames) in WPA2, or preferably WPA3, preventing attackers from executing unauthenticated Wi-Fi disconnection and deauth-flood denial-of-service attacks.

TABLE II
SOME VULNERABLE AND SOME RESILIENT VEHICLES TO BLUETOOTH CONNECTION DEPRIVATION ATTACK [208].

Vehicle Full Name	Bluetooth Version	Bluetooth Security Mode	Attack Success
Dacia Sandero 2018	v2.1+EDR	4	✓
Renault Kadjar 2018	v4.0+LE	4	✓
Volkswagen Tiguan 2017	v3.0+HS	4	✓
Volkswagen Caddy 2017	v2.1+EDR	4	✗
Mini Cooper JCW 2017	v2.0+EDR	3	✗
Peugeot 308 2015	v2.0+EDR	2	✗
Toyota Rav4 2012	v3.0+HS	3	✗
Mercedes-Benz C300 2010	v2.0+EDR	3	✗
Honda Pilot 2011	v1.2+BR	3	✗
Volkswagen Tiguan 2011	v2.0+EDR	3	✗
Lexus ES350 2009	v2.0+EDR	3	✗
Ford Fiesta 2009	v2.0+EDR	3	✗
Kia Sedona 2010	v2.0+EDR	3	✗

actively rate-limit teardown requests and lock connection states upon sensing a deauthentication storm. Furthermore, intelligent IDS have widely been studied, and can be used to distinguish bengin traffic from malicious one.

CAN Bus Denial-of-Service (DoS). In this attack, the attacker floods a Controller Area Network (CAN) bus with high-priority messages or exploits the protocol's non-destructive, bitwise arbitration mechanism to disrupt normal inter-ECU communication. In standard CAN architectures, frames with lower numerical Identifier (ID) values hold higher priority on the bus (e.g., ID `0x000` overrides all other traffic). By connecting a rogue device to an access point (such as the OBD-II port, exposed sensor wiring, or a compromised telematics module) and continuously transmitting high-priority frames with dominant bits (0), the attacker starves legitimate Electronic Control Units (ECUs) from accessing the bus. Advanced variants, such as Bus-Off attacks, trick target ECUs into repeatedly detecting signal errors until they automatically enter a self-isolating "Bus-Off" state, completely silencing safety-critical subsystems like power steering, ABS, airbag, or powertrain controls.

■ Mitigating CAN Bus DoS attacks requires physical access restrictions, hardware-enforced topology separation, and stateful bus monitoring. Central Security Gateways separate public diagnostic interfaces (OBD-II) from critical drive-by-wire buses, enforcing strict message rate-limiting, ID filtering, and firewalling to drop anomalous high-frequency streams. Modern automotive designs are transitioning to point-to-point architectures like CAN-FD with active star couplers or Automotive Ethernet switches that isolate compromised physical lines and prevent single-bus flooding. Furthermore, CAN-bus Intrusion Detection and Prevention Systems (IDPS) monitor message frequencies and electrical signal characteristics (such as voltage profile analysis and bit timing) to instantly detect anomalous dominant-bit transmissions and disconnect malicious nodes via smart transceivers.

Bus-Off Attack. A Bus-Off Attack is a specialized, hardware-level Denial-of-Service (DoS) attack targeting the fault-confinement mechanism built into the Controller Area Network (CAN) protocol. Under normal CAN protocol rules, an Electronic Control Unit (ECU) tracks transmission errors using an internal Transmit Error Counter (TEC). If an ECU accumulates a TEC greater than 255 (due to persistent bus errors), the CAN controller automatically transitions itself into a self-isolating "Bus-Off" state, completely disconnecting the ECU from the network to prevent it from disrupting other nodes. An attacker exploits this mechanism by injecting targeted, single-bit errors onto the bus at the precise moment a victim ECU transmits a frame. By intentionally overwriting a recessive bit (1) with a dominant bit (0) during the victim's transmission, the attacker causes the victim ECU to detect a bit-error, increment its TEC by 8, and retransmit the frame. By repeating this process back-to-back—often within milliseconds—the attacker forces the victim ECU's TEC past the 255 threshold. This tricks the targeted safety-critical ECU (such as the Anti-lock Braking System, Power Steering, or Engine Control Module) into going silent and dropping off the network entirely, without requiring high-privilege access or flood-style packet spamming.

■ Defending against Bus-Off attacks requires a combination of signal-level physical security, smart transceiver hardware, and anomaly detection. Modern Central Security Gateways and intelligent CAN transceivers actively monitor physical bus voltage levels, bit timing jitter, and error-frame frequencies to detect intentional bit-overwriting patterns; when detected, the system can automatically isolate the malicious physical bus segment. Network architects also utilize CAN-FD with isolated star topologies or Automotive Ethernet, which eliminate shared bus topologies where a single rogue tap can corrupt another node's bits. Furthermore, ECU software can be configured with adaptive re-initialization logic and state-aware Intrusion Detection Systems (IDS) [166]–[170] that alert the central domain controller to anomalous TEC increments, allowing fail-safe recovery modes before the module is permanently silenced.

ECU Reset Attack. An ECU Reset Attack occurs when an attacker deliberately forces an Electronic Control Unit (ECU) to reboot or enter a soft-reset state while the vehicle is actively operating. An adversary typically executes this attack by transmitting high-priority diagnostic commands over the Controller Area Network (CAN)—such as Unified Diagnostic Services (UDS) ECUReset (`0x11`) requests, diagnostic session control transitions (`0x10`), or power-mode manipulation requests—via a compromised telematics module, an exposed OBD-II port, or a wireless gateway. Alternatively, an attacker can trigger a hardware reset by inducing severe bus error conditions, exploiting memory corruption vulnerabilities (e.g., buffer overflows causing watchdog timeouts), or manipulating physical voltage levels. During the reboot sequence, the targeted ECU temporarily stops processing sensor data, drops off the network, and halts safety-critical functions (such as power steering assistance, anti-lock braking, or electronic stability

control), potentially causing dynamic vehicle instability or clearing diagnostic fault logs.

■ To mitigate ECU reset attacks, automotive architectures enforce strict stateful access controls and message authentication for all reset and diagnostic services. Systems compliant with ISO 14229-1 (UDS) enforce prerequisite SecurityAccess authentication (0x27) using cryptographic challenge-response handshakes or PKI certificates before executing an ECUReset command. Central Security Gateways validate the vehicle's operational state—such as checking wheel speed and ignition status—and enforce speed-gated lockouts to block all ECU reboot requests while the vehicle is in motion. Furthermore, implementing frame-level authentication via AUTOSAR SecOC ensures that reset frames with missing or invalid Message Authentication Codes (MACs) are immediately rejected [199]. Onboard Hardware Security Modules (HSMs) and software watchdogs also ensure that if an unauthenticated reset attempt occurs, the incident is logged into secure non-volatile memory and reported to an IDS [132].

Diagnostic Session Lock Attack. A Diagnostic Session Lock Attack occurs when an attacker deliberately forces or holds an Electronic Control Unit (ECU) in an elevated diagnostic session state—such as Unified Diagnostic Services (UDS) Extended Diagnostic Session (0x02) or Programming Session (0x03)—to lock out legitimate diagnostic communications or disrupt safety-critical operational routines. By continuously transmitting diagnostic session requests or cyclic keep-alive packets over the CAN bus, an adversary prevents the ECU from returning to its default operational state. While locked in an elevated session, the targeted ECU may suppress normal task scheduling, disable standard error handling, or block diagnostic scans from authorized service tools and central gateways. This allows an attacker to deny vehicle technicians access to fault logs, disable automated telematics health monitoring, or keep safety interlocks suppressed while preparing follow-on exploits.

■ Defending against diagnostic session lock attacks requires implementing state-aware gateway filtering [179], strict session timeouts, and cryptographic command authentication. Systems implementing ISO 14229-1 (UDS) enforce stateful time-to-live session management and mandate cryptographic authentication via UDS SecurityAccess (0x27) or ISO 21107 PKI certificates before transitioning into or maintaining elevated diagnostic modes. Central Security Gateways monitor the vehicle's dynamic operational status—enforcing speed-gated lockouts that instantly force ECUs back to default session states if vehicle movement or engine start is detected. Furthermore, deploying CAN-bus Intrusion Detection Systems (IDS) enables real-time detection and rate-limiting of anomalous message streams, allowing the gateway to block rogue diagnostic traffic and isolate compromised network segments [166]–[170] .

OTA Update Disruption. Here the attacker intentionally interferes with, delays, or aborts the transmission and installation of Over-The-Air (OTA) software updates delivered to a vehicle's telematics unit or central gateway. By leveraging cellular/Wi-Fi signal jammers, executing Man-in-the-Middle (MitM) packet drops on wireless data streams, or flooding the vehicle's internal update manager with malformed, high-frequency payload requests, the attacker prevents critical bug fixes, security patches, or safety recalibrations from reaching target Electronic Control Units (ECUs). In advanced scenarios, an attacker triggers forced network disconnects or simulated power-loss events during active flash-writing procedures to corrupt non-volatile flash memory, effectively "bricking" target ECUs or forcing safety-critical systems into persistent fail-safe modes.

■ Mitigating OTA update disruption requires implementing resilient update architecture frameworks like Uptane alongside dual-bank fail-safe storage strategies. Vehicles deploy dual-bank (A/B) flash memory structures, allowing new firmware to be written and cryptographically validated on a secondary partition in the background while the primary partition safely executes operational code; if a disruption occurs mid-transfer or verification fails, the system seamlessly rolls back to the intact image without interrupting vehicle function. Network-level resilience is maintained using TLS 1.3, QUIC, or IPsec with automatic connection retry logic, resume-on-break download protocols, and integrity checks at every chunk level to resist wireless packet drops. Furthermore, onboard update managers enforce stateful battery/power checks and speed-gated lockouts to ensure updates are only initiated under stable, safe vehicle conditions.

Memory Exhaustion Attack. This attack occurs when an attacker consumes or corrupts an Electronic Control Unit's (ECU) limited dynamic memory (RAM) or non-volatile storage (EEPROM/Flash), degrading operational performance or forcing a system-wide crash. By transmitting high-frequency diagnostic requests, flooding the gateway with fragmented Over-The-Air (OTA) update packets, or triggering unthrottled logging of synthetic diagnostic trouble codes (DTCs), the adversary triggers memory leaks, heap/stack buffer overflows, or storage exhaustion. In real-time embedded systems operating under strict microsecond execution constraints, exhausting available memory causes real-time operating system (RTOS) task scheduling failures, triggers watchdog resets, or forces safety-critical ECUs (e.g., ADAS or braking modules) into unrecoverable fail-safe modes.

■ A system that is resilient against memory exhaustion attacks requires strict memory allocation limits, static analysis, and hardware-enforced isolation. Embedded firmware developers enforce static memory allocation strategies—avoiding dynamic memory allocation functions (e.g., malloc/free) entirely in real-time safety critical tasks to eliminate dynamic heap exhaustion risks. Central Security Gateways (or mother ECU [174]) deploy buffer-limiting rate control and packet reassembly limits to reject oversized or fragmented diagnostic and OTA payloads. At the processor level, microcontrollers

utilize Memory Protection Units (MPUs) and Hardware Security Modules (HSMs) to enforce memory segmentation [206], ensuring that diagnostic buffers cannot overflow into critical application stacks or exhaust flash log partitions.

Malware-Induced Service Disruption. This scenario occurs when malicious software gains execution privileges on an ECU [7], In-Vehicle Infotainment (IVI) system, or Telematics Control Unit (TCU) and actively interferes with real-time embedded operational processes. An attacker typically deploys the malware through compromised Over-The-Air (OTA) updates, malicious third-party diagnostic applications, physical media (USB/OBD-II dongles), or vulnerable cellular and Wi-Fi stack exploits. Once persistent, the malware executes targeted disruption payloads—such as hijacking Real-Time Operating System (RTOS) task scheduling priorities, corrupting volatile shared memory structures, or generating continuous high-priority bus noise. By starving safety-critical processes of processor cycles and network bandwidth, the malware forces key subsystems (e.g., advanced driver-assistance systems, brake modules, airbags deployment, or powertrain controllers) into crash-recovery loops, watchdog resets, or unrecoverable fail-safe modes while the vehicle is in operation.

■ Mitigating malware-induced service disruption requires a hardware-anchored software protection lifecycle spanning secure execution, isolation, and continuous runtime monitoring. Microcontrollers implement hardware-enforced Secure Boot using an immutable Root of Trust (RoT) to cryptographically authenticate all firmware images and operating system kernels before execution [181]–[183]. At runtime, Memory Protection Units (MPUs) and hypervisors enforce strict process-level memory containment and privilege separation, preventing compromised infotainment or telematics applications from accessing safety-critical micro-kernel tasks or shared CAN/Ethernet buffers. Furthermore, onboard Host-based Intrusion Detection Systems (HIDS) [166]–[168] and central Security Gateways continuously monitor CPU execution loads, dynamic memory allocation calls, and task timing constraints, automatically isolating compromised processes or resetting affected nodes into secure operational safe states upon detecting unauthorized execution behavior.

Automotive Ethernet DoS. Automotive Ethernet Denial-of-Service (DoS) occurs when an attacker floods a vehicle's high-speed Ethernet backbone—typically based on IEEE 100BASE-T1 or 1000BASE-T1 standards—with malformed frames, high-bandwidth packet bursts, or protocol-specific request floods. By gaining access via a compromised Telematics Control Unit (TCU), In-Vehicle Infotainment (IVI) node, diagnostic port (DoIP), or exposed physical harness, the adversary targets key Layer-2/Layer-3 protocols like SOME/IP (Scalable service-Oriented MiddleWARe over IP), DoIP (Diagnostic communication over IP), or gPTP (Generalized Precision Time Protocol / IEEE 802.1AS). By exhausting switch buffer memories, overwhelming real-time SOME/IP service registries, or flooding timing-synchronization streams, the attacker starves safety-critical high-bandwidth domains—such as camera/LiDAR ADAS feeds, domain controller communications, or zone gateways—causing frame drops, latency spikes, or complete system desynchronization while the vehicle is operating.

■ The deployment of hardware-enforced traffic shaping, packet filtering, and time-sensitive networking controls constitutes a promising countermeasure to fend off this attack. For example, automotive Ethernet switches enforce IEEE 802.1Qci (Per-Stream Filtering and Policing) to monitor incoming data rates on a per-port, per-stream basis, dropping non-compliant packet bursts before they reach central switch buffers. Network architects employ Virtual Local Area Networks (VLANs) according to IEEE 802.1Q to isolate high-throughput infotainment traffic from critical ADAS and powertrain domains (i.e., reduce the broadcast domain). Furthermore, switch hardware enforces strict ingress rate-limiting for DoIP/SOME/IP ports and utilizes IEEE 802.1Qbv (Time-Aware Shaper) in Time-Sensitive Networking (TSN) environments to guarantee dedicated transmission windows for safety-critical control traffic regardless of background network load.

ECU Power Disruption. An ECU Power Disruption attack occurs when an adversary manipulates or interrupts the electrical power lines, supply voltages, or power management states powering a target Electronic Control Unit (ECU). By transmitting unauthorized power management diagnostic frames (such as UDS ControlDTCSetting or Low-Power Mode commands), exploiting software-driven Power Distribution Units (PDUs) / smart high-side switches, or executing physical fault injection (e.g., rapid power glitching, voltage brownouts, or electromagnetic pulse interference), the attacker forces the ECU to power cycle or shut down unexpectedly. Inducing voltage fluctuations or cutting power during critical processing states causes microcontrollers to execute corrupted instructions, reset repeatedly, or halt active safety functions—such as electric power steering assistance, high-voltage battery management, or automated braking routines—while the vehicle is in motion.

■ To mitigating this attack, the in-system requires integrating resilient hardware power conditioning, fault-tolerant power routing, and stateful power management access controls. Modern automotive ECUs incorporate internal energy storage (such as decoupling capacitors and hold-up circuits) alongside System Basis Chips (SBCs) equipped with Brown-Out Detection (BOD) and Over/Under-Voltage Lockout (UVLO/OVLO) protection circuits that prevent corrupted execution during power dips. Network architectures employ redundant dual-power rails for critical domain controllers and require multi-stage cryptographic authentication (e.g., UDS SecurityAccess or SecOC) before any command modifying power distribution states can be processed. Furthermore, onboard hardware watchdogs and logging systems capture voltage anomaly metrics in secure non-volatile memory, allowing the Central Gateway to isolate compromised power channels and initiate deterministic safety fallbacks.

VII. Attacks on Vehicles' ADAS System

In this section, we review another form of attacks. This type of attacks concernes vehicles equipped with an ADAS (Advanced Driver Assistance Systems) system like autonomous vehicles and self-driving cars. It relies on compromising the vehicles' ADAS sensors, or manipulating the external environment to deceive the sensors of the vehicle rather than "hacking" the vehicle's software.

A. Interception Attack and Cyberattack Scenarios

In this subsection, we review the possible interception cyberattacks that could be undertaken against the different components of a vehicle's ADAS system. This includes, the cameras, GPS (Global Positioning System), RADAR (Radio Detection and Ranging), and LiDAR (Light Detection and Ranging). This would allow the attacker to gain unauthorized access to the signals, messages, and content exchanges within the ADAS system of the vehicle.

Camera Stream Interception. This attack occurs when an attacker taps into the vehicle's internal data buses (such as Automotive Ethernet, MIPI CSI-2[15], or SerDes[16] links) or remote wireless endpoints to secretly capture live video feeds or stored footage from ADAS and cabin cameras. By exploiting unencrypted communications or pivoting laterally from a compromised wireless domain (like Telematics or Infotainment), the attacker can passively monitor passenger activities, log precise driving routes (especially, if the vehicles accesses restricted areas like military bases or other governmental facilities), and capture sensitive surrounding environment data like license plates and facial identities—creating severe privacy violations while establishing a foundation for other forms of attacks.

LiDAR Data Interception. This attack occurs when an attacker wiretaps the high-bandwidth data buses (such as Automotive Ethernet) connecting the LiDAR sensor to the central perception unit, or remote-accesses the feed by compromising connected wireless gateways like Telematics. By sniffing the raw 3D point-cloud data stream, the attacker can reconstruct high-resolution, spatial models of the surrounding environment, track nearby vehicle and pedestrian movements, and precisely infer the target vehicle's real-time trajectory and driving behavior—causing severe driver privacy breaches. This attack can also be used to learn, spy on, and disclose the infrastructure of highly-restricted areas, such as governmental facilities and military bases.

GPS/GNSS Observation. This is a passive surveillance attack where an attacker monitors the output of the vehicle's GNSS (Global Navigation Satellite System) receiver—such as NMEA streams[17]—or taps into internal data buses (e.g., CAN, Automotive Ethernet) to read location coordinates, speed, and heading data. Rather than manipulating positioning signals to divert the vehicle, the attacker passively logs these raw location feeds or intercepts off-board location updates sent via telematics to cloud services. By silently harvesting this spatial telemetry over time, the attacker builds complete, highly accurate travel histories, identifies frequent destinations (like home or workplace), and derives driver routines without triggering any onboard diagnostic alerts or altering vehicle behavior.

■ To defend against camera stream interception, LiDAR data interception, and unauthorized GPS observation, modern vehicle architectures must adopt a unified security strategy built on internal bus isolation, link-layer encryption, and secure telematics. Vehicle networks must enforce strict micro-segmentation and firewall-protected domain gateways to isolate camera feeds, LiDAR point clouds, and GNSS/navigation receivers onto dedicated sensor buses, preventing non-privileged or wireless infotainment systems from accessing safety-critical traffic. To secure high-rate video streams, point-cloud data, and positioning frames in transit with near-zero latency, all internal interfaces (such as Automotive Ethernet) must implement hardware-accelerated link-layer encryption like MACsec (IEEE 802.1AE). Additionally, any vehicle-to-cloud telematics transmission offloading location or sensor data must enforce Mutual TLS (mTLS) with Hardware Security Module (HSM)-backed cryptographic keys, while onboard local caches and video recordings must be secured with encrypted storage at rest. Finally, physical security measures—such as tamper-shielding around sensitive camera wiring harnesses—should be coupled with privacy-enhancing techniques like differential privacy (spatial-temporal noise addition or coordinate rounding) to safeguard raw location coordinates against external tracking [60]–[62].

Radar Signal Monitoring. This attack scenario is an over-the-air passive surveillance attack where an attacker deploys specialized Software-Defined Radios (SDRs) or high-frequency RF receivers to intercept the vehicle's millimetre-wave Frequency Modulated Continuous Wave (FMCW) radar emissions (typically in the 77–79 GHz band). By capturing these continuous frequency chirps and analyzing their slope, Doppler shifts, and timing patterns, the attacker can reverse-engineer the host vehicle's exact velocity and acceleration changes without establishing physical or digital access to internal buses. For example, an attacker could estimate the distance separating the target vehicle and an exposive object (a parked vehicle) to trigger the explosion at the right moment.

■ The protection against this attack requires implementing RF physical-layer security and waveform obfuscation, such as randomizing chirp parameters—varying slope, start frequency,

[15]MIPI CSI-2 (Mobile Industry Processor Interface — Camera Serial Interface 2) is a high-speed standard connecting image sensors to processors, widely adopted across smartphones, automotive ADAS, robotics, and industrial vision systems.

[16]SerDes (Serializer/Deserializer) converts parallel digital data into high-speed serial streams for long-distance transmission, widely used in automotive and high-speed vision links.

[17]NMEA (National Marine Electronics Association) streams are standardized text feeds used by GPS/GNSS receivers to transmit location, speed, and navigation data to embedded and external devices.

sweep duration, and inter-chirp intervals on a frame-by-frame basis—so eavesdroppers cannot reliably lock onto or decode the signal structure [63]–[65]. Manufacturers also employ Low Probability of Intercept/Exploitation (LPI/LPE) techniques [66], such as phase-coded pulse modulation (PCPM) or orthogonal frequency-division multiplexing (OFDM) radar waveforms with pseudo-random code sequences, which blend radar emissions into background thermal noise for unauthorized receivers. Additionally, dynamic power control algorithms dynamically attenuate transmission amplitude to the bare minimum required for target tracking, reducing the spatial radius in which an attacker can do the interception.

AI Model Extraction (or Model Theft). This attack occurs when an attacker exploits physical debugging interfaces (like JTAG[18]), privileged ECU software vulnerabilities, or exposed inference APIs (Application Programming Interfaces) to reverse-engineer or extract trained Deep Neural Network (DNN) weights, hyper-parameters, and model architectures from the ADAS controller. Because autonomous driving models represent core intellectual property (IP) derived from vast training datasets, stealing these proprietary assets enables competitors to clone advanced safety features at a fraction of the development cost. Beyond IP theft, acquiring a exact shadow replica of the victim model allows attackers to calculate offline gradients and craft white-box adversarial attacks—such as imperceptible physical patches on road signs or lane markers—guaranteeing high-confidence misclassifications that cause dangerous driving maneuvers when executed against the real-world vehicle.

■ To safeguard deployed deep-learning models on the edge, hardware architectures must enforce Hardware Root of Trust mechanisms, utilizing Secure Boot [181]–[183], encrypted flash memory, and Hardware Security Modules (HSMs) to keep network weights encrypted in non-volatile storage and decrypt them directly within protected enclave memory (e.g., ARM TrustZone) during runtime execution. Furthermore, developers employ heavy neural network obfuscation and quantization—compiling the model into specialized, fused hardware primitives or adding weight-level obfuscation—to render reverse-engineered binaries unintelligible. At the application layer, system designers restrict diagnostic query access, obscure output confidence scores, and run runtime anomaly monitoring to detect systematic inference-querying patterns, neutralizing both direct binary extraction and black-box distillation attempts.

B. Fabrication Attack and Cyberattack Scenarios

In this subsection, we discuss different cyberattacks where an attacker tries to impersonate legitimate entities to fool the ADAS system into considering fake and incorrect data, or take unwanted actions that could lead to serious consequences.

[18]JTAG (Joint Test Action Group) is an industry standard (IEEE 1149.1) established for testing, debugging, and programming hardware platforms—including microcontrollers, CPUs, FPGAs, and vehicle Electronic Control Units (ECUs)

GPS Spoofing Attack. A GPS spoofing attack deceives the vehicle's Global Navigation Satellite System (GNSS) receiver by transmitting counterfeit satellite signals that closely mimic legitimate GPS transmissions while carrying manipulated navigation data. These forged signals are typically broadcast at a higher power than genuine satellite signals, causing the receiver to lock onto the malicious source and compute an incorrect position, velocity, or time solution. As a result, ADAS and autonomous driving systems relying on GNSS for localization may believe the vehicle is traveling along a different route or occupying an incorrect position. This misinformation can lead to erroneous navigation decisions, improper lane-level localization, incorrect speed estimation, or unsafe path planning, potentially causing the vehicle to deviate from its intended route or violate traffic regulations. GPS spoofing poses a significant threat as the attack can be launched remotely (and efficiently, using high-gain directional antenna) without requiring physical access to the vehicle, making it particularly dangerous for highly automated and autonomous vehicles.

■ Defending against GPS spoofing requires integrating multiple localization sources rather than relying solely on GNSS measurements. Sensor fusion techniques combining GPS data with inertial measurement units (IMUs), wheel odometry, LiDAR, cameras, high-definition maps, and radar enable the vehicle to detect inconsistencies between independent localization estimates. Modern GNSS receivers can also monitor signal characteristics such as received power, signal quality, satellite geometry, and timing consistency to identify anomalous transmissions indicative of spoofing. Cryptographically authenticated navigation signals, such as those available in emerging secure GNSS services, further reduce the feasibility of counterfeit satellite transmissions. Upon detecting suspicious localization discrepancies, the vehicle should disregard compromised GNSS measurements, transition to an alternative localization mode, notify the driver, and limit autonomous functionality until reliable positioning is restored. These layered defenses significantly improve resilience against GPS spoofing attacks while maintaining safe vehicle operation.

LiDAR Spoofing Attack. This is an active physical-layer attack where an attacker fires precisely timed laser pulses at a target vehicle's LiDAR sensor to inject fake 3D point clouds (phantom objects) or blind the sensor entirely. Because LiDAR measures distance by calculating the time-of-flight (ToF) of reflected light, an attacker using synchronized laser diodes can trick the receiver into registering non-existent obstacles, such as ghost pedestrians or fake walls. When the perception software processes these spoofed echoes, the ADAS/Autonomous Driving system interprets them as real hazards, triggering sudden hard braking, erratic swerving, or complete vehicle immobilizations that create severe safety risks for occupants and surrounding traffic.

■ To neutralize physical laser spoofing, LiDAR systems employ multi-layered physical and temporal validation controls,

such as randomizing laser pulse emission intervals (pulse-interval jittering) and using cryptographic phase/frequency modulation [67] on emitted beams so the receiver can discard any pulse that lacks the secret pattern. At the sensor design level, hardware features like spatial filtering, polarized optical lenses, and multi-wavelength firing make it extremely difficult for external lasers to enter the sensor at the correct angle and wavelength. Furthermore, high-level perception pipelines implement sensor fusion anomaly detection, cross-referencing LiDAR point clouds with radar, camera, and ultrasonic data; if LiDAR detects a solid wall that radar and camera feeds confirm is empty space, the fusion engine flags and filters out the spoofed phantom object in real time.

Radar Spoofing Attack. This is an active physical-layer RF attack where an adversary uses specialized signal transmitters—such as Software-Defined Radios (SDRs) or Digital Radio Frequency Memory (DRFM) repeaters—to transmit malicious millimeter-wave signals directly into a vehicle's FMCW radar receiver. By precisely calculating the target radar's chirp timing, center frequency, and slope, the attacker injects artificial reflections that fabricate non-existent objects (phantom vehicles) or hide real obstacles (target masking). When processed by the vehicle's perception module, these false radio echoes manipulate estimated ranges and relative velocities, forcing automated safety systems like Adaptive Cruise Control (ACC) or Automatic Emergency Braking (AEB) to trigger sudden emergency stops or fail to detect stopping vehicles ahead.

■ Defending against active radar spoofing relies on physical-layer signal encryption, waveform randomization, and cross-sensor validation. Modern automotive radars mitigate spoofing by implementing pseudo-random phase coding (PCPM), dynamic chirp-interval jittering, and frequency hopping across radar frames, making it impossible for an attacker's transmitter to predict and synthesize matching beat-frequency signals in real time. At the signal processing level, system architectures evaluate signal-to-noise ratios and spatial angle-of-arrival (AoA) profiles to detect non-standard power spikes or impossible Doppler shifts indicative of synthesized RF injection. Finally, high-level multi-sensor fusion cross-validates radar tracking targets against optical camera feeds and LiDAR point clouds, allowing the perception stack to dismiss unconfirmed phantom radar tracks before taking control actions.

Acoustic Emergency Siren Spoofing. In this cyberattack, the attacker targets the specialized microphone arrays and audio classification pipelines used by Autonomous Vehicles (AVs) to detect approaching emergency responders. An attacker broadcasts simulated emergency siren audio profiles (such as Wail, Yelp, or Hi-Lo patterns) via localized directional speakers or compromised roadside public address systems. When the vehicle's acoustic perception module processes these signals via Convolutional Neural Networks (CNNs) or Mel-Frequency Cepstral Coefficients (MFCC), it falsely identifies a nearby emergency vehicle. Tricked by this fake audio priority signal, the autonomous system triggers evasive yields—such as executing unnecessary emergency stops, pulling off to the road shoulder, or giving up intersection right-of-way—resulting in severe traffic disruptions, collision hazards, or forced immobilizations.

■ Neutralizing fake siren audio requires multimodal spatial validation and visual cross-confirmation. Perception systems must mandate optical verification before taking drastic vehicle maneuvers, cross-referencing acoustic siren alerts with camera/LiDAR detection of active emergency light bars, distinct vehicle markings, or vehicle movement profiles. Additionally, microphone arrays should utilize Time Difference of Arrival (TDOA) algorithms to measure sound propagation vectors and Doppler shifts, discarding static directional speakers or uniform non-moving sound sources as non-legitimate. Finally, V2X priority messaging (such as Emergency Vehicle Alerts over C-V2X) provides a cryptographically signed broadcast path to validate nearby emergency vehicles over the air without relying purely on raw acoustic data.

C. Modification Attack and Cyberattack Scenarios

In this category, an attacker aims to compromise the integrity of the different sensors of the ADAS system, and/or the environment used by the autonomous vehicles introducing fake and incorrect data that could mislead the AI model of the vehicle to run into misclassifications and make unwanted decisions, e.g., sudden stop in a high-traffic highway.

Physical Sensor Tampering Attack. A physical sensor tampering attack targets the integrity of ADAS sensors by deliberately altering their operating conditions or obstructing their ability to accurately perceive the surrounding environment. An attacker with physical access to the vehicle may cover cameras with opaque materials, apply paint or stickers to radar radomes, contaminate LiDAR lenses with dirt or reflective films, or misalign sensors by striking or loosening their mounting brackets. More sophisticated attackers may damage sensor wiring or modify sensor calibration parameters during vehicle maintenance. These actions cause the affected sensors to produce inaccurate or incomplete measurements, degrading the vehicle's perception of lanes, obstacles, pedestrians, or nearby vehicles. Consequently, the ADAS controller may make incorrect decisions, such as failing to detect hazards, performing unnecessary emergency braking, departing from the intended lane, or executing unsafe steering maneuvers that compromise passenger and road-user safety.

■ Protecting ADAS sensors against physical tampering requires a combination of robust hardware design, continuous integrity monitoring, and sensor redundancy. Sensors should be enclosed within tamper-resistant housings and mounted using secure fasteners that discourage unauthorized adjustment or removal. The vehicle should continuously monitor sensor health by verifying calibration parameters, signal quality, and alignment, while periodically performing self-diagnostic routines to detect abnormal behavior. Sensor fusion techniques



Fig. 19. From left to right, some printed object mimicry attacks: A printed stop sign sticked on the back of a vehicle to mislead autonomous vehicles' perception module that a stop sign is in front, making a sudden stop; A truck coming up front printed on the back of a box truck to deceive autonomous vehicles; and an individual wearing a black shirt on which it shows a 80mph speed limit sign, in a school zone (images generated using Google Gemini 1.5 Pro).

can compare observations from multiple independent sensors, allowing inconsistencies caused by a compromised sensor to be identified and isolated. If significant discrepancies or sensor failures are detected, the vehicle should transition to a safe operating mode by disabling the affected ADAS functions, alerting the driver, and recording the event for diagnostic analysis. Regular inspection during maintenance and secure access control for sensor calibration procedures further reduce the likelihood of successful physical tampering.

Sensor Calibration Modification. In this attack scenario, the attacker tampers with or overwrites the zero-point offsets, gain coefficients, or environmental reference tables used by sensors that feed safety-critical systems—such as Advanced Driver Assistance Systems (ADAS), automated driving modules, or stability control units. By issuing unauthorized diagnostic service commands over the CAN bus or tapping directly into local sensor buses, the attacker may alter baseline calibration variables for cameras, radar, LiDAR, wheel speed, or inertial measurement units (IMUs). By introducing subtle skew or dead zones into sensor feedback, the attacker tricks perception algorithms into miscalculating vehicle trajectory, failing to detect obstacles, misinterpreting lane boundaries, or triggering unintended emergency braking and steering maneuvers.

■ To protect sensor calibration parameters from malicious modification, automotive architectures require strict access controls, sensor integrity validation, and runtime plausibility checks. System designers mandate cryptographic challenge-response authentication (such as ISO 14229-1 UDS Security-Access or ISO 21107 PKI certificates) before allowing any calibration routine to execute. Furthermore, critical baseline values stored in sensor EEPROMs or ECU flash must be cryptographically protected with Message Authentication Codes (MACs) managed by an onboard Hardware Security Module (HSM). At the perception layer, cross-sensor sensor fusion algorithms (e.g., comparing camera telemetry against radar and wheel-speed inputs) dynamically detect single-sensor calibration drifts or sudden anomalies, instantly flagging the sensor and falling back to fail-safe operational modes before dangerous driving decisions are executed.

Mimicry using Printed Objects. In this attack scenario, the attacker disturbs the perception model of the ADAS system in autonomous vehicles by maliciously (and sometimes, accidently) introducing a printed object on the driving scene requiring the vehicle to take an unwanted action. For example, a "Stop Sign" could be printed on a paper and sticked on the back of a vehicle to disturb the perception model of nearby autonomous vehicles, making them undertake a sudden stop in a situation that results in serious consequences. Another scenario could be in a school zone, where an individual wears a shirt on which it is printed a highway speed limit sign, making the vehicles speed up in a 15 mph zone (viz., Fig. 19).

■ To fend off this attack, the perception system should be able to distinguish genuine traffic infrastructure from counterfeit visual artifacts. Camera-based detections should be validated using contextual reasoning and multi-sensor fusion, combining information from LiDAR, radar, high-definition maps, and vehicle localization to verify that a detected traffic sign exists at a plausible roadside location. Three-dimensional scene understanding can further identify whether a sign is mounted on permanent roadside infrastructure or merely attached to another vehicle or temporary object. Temporal consistency analysis allows the vehicle to verify that traffic signs remain spatially consistent across consecutive frames, while object tracking can reveal signs that move together with other vehicles, indicating a likely counterfeit. Finally, confidence estimation and anomaly detection techniques should flag unusual detections for additional verification before initiating safety-critical maneuvers, thereby reducing the likelihood that fabricated visual objects influence autonomous driving decisions.

Mimicry using Displayed Objects. In this attack scenario, the attacker wrong the perception model of the ADAS system by displaying, using a large embedded monitor, a display screen, or a digital billboard, objects that could make the vehicle take immediate action if perceived and detected. For example, a vehicle coming up-front could be displayed on a screen placed on the back of a large vehicle (viz., Fig. 20).

■ To thwart this attack, perception system should be ca-



Fig. 20. From left to right, some displayed object mimicry attacks: A law enforcement police car coming up-front, displayed on a display screen located on the side of a truck storage box; a fire truck coming up-front displayed on a digital billboard; and a stop sign displayed on an advertisement display screen (images generated using Google Gemini 1.5 Pro).

pable of distinguishing real physical objects from digitally rendered images. Multi-sensor fusion should be employed to verify camera detections using complementary sensors such as LiDAR and radar, which can determine whether the detected object possesses a corresponding three-dimensional structure and physical presence. Vision algorithms may also analyze display-specific characteristics, including pixel patterns, refresh-rate artifacts, moiré effects, abnormal brightness, and polarization signatures, to identify objects originating from electronic screens. Temporal consistency and motion analysis can further reveal discrepancies between the displayed object's apparent motion and the movement of its supporting vehicle. Additionally, detected objects should be validated against contextual information, such as lane geometry, object size, and expected traffic behavior, before triggering safety-critical maneuvers. By combining robust computer vision techniques with cross-sensor verification and contextual reasoning, autonomous vehicles can significantly reduce the risk of responding to counterfeit objects displayed on electronic screens.

Mimicry using Projected Objects. In this attack scenario, the attacker misleads the perception model of the ADAS system by projecting (using a wireless mobile projector) road-related objects into the driving scene. When the objects are perceived, the vehiles may undertake unwanted driving decisions. For example, a person (a kid) could be projected laying on the highway to froce the vehicles into making a sudden emergency brake and maneuver (viz., Fig. 21).

■ The mitigation of this attack requires the perception system to verify the physical existence of detected objects before initiating safety-critical actions. Camera-based detections should be corroborated using complementary sensors such as LiDAR and radar, which can determine whether the perceived object has a corresponding three-dimensional structure and measurable physical properties. Vision algorithms may further analyze illumination consistency, shadow formation, texture continuity, and optical characteristics to identify objects originating from projected light rather than tangible entities. Temporal consistency and motion analysis can also distinguish stationary projections from real objects by examining their behavior across consecutive frames and under changing viewpoints. When inconsistencies are detected between sensing modalities, the autonomous driving system should reduce confidence in the camera observation, request additional verification, and transition to a safe operating mode rather than executing abrupt maneuvers. This multi-layered validation process significantly improves resilience against projection-based deception attacks while maintaining the safety and reliability of ADAS functions.

Mimicry using Crafted Objects. In this attack scenario, the attacker disturbs the perception model of the ADAS system by introducing real objects that are not supposed to appear on a given driving scene. For example, an attacker could place an 80mph speed limit sign in a school zone, or use black tape to change a 30mph speed limit sign into an 80mph sign. Another scenario could happen when an attacker uses inflatable vehicle-like object (e.g., inflatable military tank) to deceive ADAS systems that the object is a real vehicle (viz., Fig. 22).

■ Mitigating mimicry attacks using crafted objects requires the ADAS perception system to evaluate detected objects within their semantic and geographical context rather than relying solely on visual recognition. Context-aware perception algorithms should verify whether a detected traffic sign or road object is consistent with the surrounding environment, road type, vehicle location, and applicable traffic regulations. For example, a speed limit sign indicating 80 km/h should be considered suspicious if detected within a school zone or a residential area where significantly lower speed limits are expected. High-definition maps, GNSS localization, and digital road infrastructure databases can provide prior knowledge of legitimate traffic sign locations and road attributes, enabling the system to identify inconsistencies between observed and expected conditions. Temporal verification across multiple observations and sensor fusion with LiDAR or radar can further assess whether the object is permanently installed as part of the road infrastructure or has been temporarily introduced. When contextual inconsistencies are detected, the perception system should assign a lower confidence score to the detected object,



Fig. 21. From left to right, some projected object mimicry attacks: A projected person laying on the street, a stop sign projected in a front-side wall, and a running person (as if the individual is crossing) projected on the bridge wall in a highway (images generated using Google Gemini 1.5 Pro).



Fig. 22. From left to right, some crafted object mimicry attacks: A fake stop sign deliberately placed on the side of a highway, a tempered-with school zone speed limit sign, where a malicious individual used balck-tape to modify the 30mph to 80mph, and an inflatable decoy tank that could be used to fool ADAS systems of the presence of a real military tank (images generated using Google Gemini 1.5 Pro— except the rightmost image).

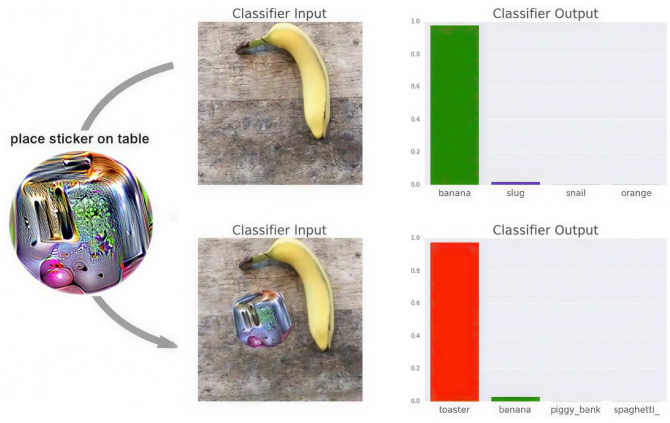

Fig. 23. A camouflage attack: an adversarial patch placed next to a banana causes a deep-learning model to misclassify it as a toaster. The same technique can be applied totraffic signs to induce misclassification [129].

request additional verification, and avoid executing immediate safety-critical actions until the object's legitimacy has been confirmed.

Camouflage of Real Objects. In this attack scenario, the attacker disturbs the perception model of vehicles by placing a specific stickers on a target object. The object will look normal to a human, but will be identified as a different object by the perception model. For example, an attacker could place a specifically engineered small sticker on a "Stop" sign to make it look like a "Speed Limit" sign to the camera. Fig. 23 illustrates an adversarial patch placed next to a banana causes a deep-learning model to misclassify it as a toaster.

■ Defending against camouflage attacks requires enhancing the robustness of the perception system against adversarial perturbations and preventing decisions from relying solely on a single visual cue. Deep learning models should be trained using adversarial examples and physically transformed traffic signs to improve their resilience to stickers, graffiti, occlusions, and other intentional modifications. Multi-sensor fusion enables the vehicle to validate camera-based observations using complementary sensors such as LiDAR, radar, GPS, and high-definition maps, allowing inconsistencies to be detected before safety-critical decisions are made. Temporal consistency checking can further verify whether a detected traffic sign remains consistent across multiple video frames, reducing the impact of transient misclassifications. Confidence estimation and out-of-distribution detection techniques can identify suspicious classifications and trigger additional verification instead of immediately executing the corresponding driving action. Finally, periodic model retraining using newly discovered adversarial samples helps maintain robustness against evolving physical attacks targeting ADAS perception systems.

Agentic Prompt Injection Attack. Future Agentic Vehicles (AgVs) are expected to integrate Large Language Models

(LLMs) capable of reasoning, planning, maintaining memory, and invoking external tools, thereby introducing a new attack surface beyond conventional perception and control systems [223], [224]. In a prompt injection attack, an adversary embeds malicious instructions within trusted information sources, such as Vehicle-to-Everything (V2X) messages, roadside infrastructure, digital signage, passenger voice commands, or cloud services. Rather than exploiting software vulnerabilities or sensor measurements, the attacker manipulates the agent's reasoning process, causing it to misinterpret contextual information or deviate from its intended objectives. Consequently, the compromised agent may alter its route, invoke unauthorized actions (e.g., unlocking doors or modifying navigation), retain poisoned information in memory, or disseminate deceptive information to neighboring autonomous agents, potentially leading to unsafe vehicle behavior or coordinated traffic disruption.

■ Mitigating prompt injection attacks requires securing both the agent's inputs and its reasoning process. External information, including V2X communications, roadside messages, cloud responses, and user interactions, should undergo authentication, trust evaluation, and contextual validation before being incorporated into the agent's prompt. Furthermore, critical actions such as mission modifications, route changes, and safety-sensitive tool invocations should be constrained by immutable safety policies and independently verified prior to execution. Runtime monitoring should continuously detect abnormal reasoning patterns, unauthorized goal changes, and anomalous tool usage, while memory provenance and bounded reasoning mechanisms help prevent memory poisoning and excessive replanning. Together, these measures provide layered protection for the cognitive layer of future Agentic Vehicles.

D. Interruption Attack and Cyberattack Scenarios

In this category, the attacker targets the availability of the ADAS components or system by physically assaulting the components, or using tools to disturb the normal functionning of the sensors, leading to inconsistent or no perceptions.

Sensor Jamming and Blinding Attack. A sensor jamming and blinding attack aims to disrupt the operation of ADAS sensors by overwhelming them with interference or preventing them from receiving legitimate environmental information. Depending on the targeted sensor, an attacker may transmit high-power radio-frequency signals to jam GNSS receivers, emit interfering electromagnetic signals to degrade radar performance, project carefully timed laser pulses to saturate LiDAR receivers, or use high-intensity lights, lasers, or reflective surfaces to blind cameras and create excessive glare. These interference sources reduce the sensor's ability to detect lanes, pedestrians, obstacles, traffic signs, or surrounding vehicles, thereby degrading the accuracy of the perception system. As a result, ADAS functions such as adaptive cruise control, lane keeping assistance, collision avoidance, and autonomous navigation may become unavailable or operate unreliably, potentially increasing the likelihood of unsafe driving behavior or traffic accidents.



Fig. 24. A Waymo's self-driving car (Robotaxi) vandalized by protesters in Los Angeles (USA) in 2025 during the anti-ICE protests.

■ Mitigating sensor jamming and blinding attacks requires a combination of robust sensor design, interference detection, and redundant perception mechanisms. Sensors should continuously monitor signal quality, received power, and operational health to identify abnormal conditions indicative of intentional interference. Multi-sensor fusion enables the vehicle to cross-validate observations from cameras, LiDAR, radar, GNSS, inertial measurement units, and wheel odometry, allowing compromised sensors to be detected and isolated. Camera systems may incorporate high dynamic range imaging, optical filters, and automatic exposure control to reduce susceptibility to intense light sources, while radar and GNSS receivers can employ adaptive filtering, beamforming, and anti-jamming antennas to improve resilience against radio-frequency interference. Upon detecting persistent sensor degradation, the vehicle should disable affected ADAS functions, alert the driver, and transition to a safe operational mode until reliable sensor data are restored. This layered approach enhances the availability and reliability of autonomous perception under hostile conditions.

Physical Vandalism Attack on ADAS Components. This attack targets the hardware components of ADAS with the objective of degrading or completely disabling their sensing capabilities. An attacker may deliberately break or crack camera lenses, damage radar radomes, shatter LiDAR protective covers, disconnect sensor wiring, cut communication cables, or physically remove externally mounted sensors (viz., Fig. 24). Other forms of vandalism include applying paint, adhesives, or corrosive substances to sensor surfaces, striking sensors to alter their alignment, or intentionally damaging mounting brackets during maintenance or while the vehicle is parked. Such actions prevent the affected sensors from accurately perceiving the surrounding environment, causing ADAS functions such as lane keeping assistance, adaptive cruise control, automatic emergency braking, traffic sign recognition, and parking assistance to malfunction or become unavailable. Because

autonomous and highly automated vehicles rely on multiple interconnected sensors, the failure of one or more critical components can significantly reduce situational awareness and compromise driving safety.

■ Protecting ADAS components against physical vandalism requires combining robust hardware protection with continuous system monitoring and fault tolerance. Externally mounted sensors should be enclosed within impact-resistant and tamper-resistant housings capable of withstanding accidental and intentional damage. Critical wiring should be routed through protected channels to minimize exposure to cutting or manipulation, while mounting mechanisms should discourage unauthorized removal or misalignment. The vehicle should continuously monitor sensor health through built-in diagnostics, calibration verification, and signal quality assessment to promptly identify damaged or disconnected components. Sensor fusion algorithms can detect inconsistencies between multiple sensing modalities and isolate malfunctioning sensors while maintaining safe operation whenever possible. If critical sensor failures are detected, the vehicle should automatically disable affected ADAS features, notify the driver through visual and audible warnings, log diagnostic information for maintenance, and transition to a safe degraded operating mode until repairs are completed. This layered defense improves system resilience against deliberate physical attacks and accidental damage alike.

VIII. Discussions and Perspectives

In this section, we analyze the reviewed attacks and countermeasures to identify standing challenges, emerging research trends, and highlight exising gaps and unexplored areas.

A. Discussion on Research Direction 1 (RD1)

In this subsection, we analyze the reviewed attacks and countermeasures related to "Attack on Vehicles' Body and Physical Systems" (i.e., **RD1**) to clarify the current status, pending challenges, and highlight the existing gaps.

The reviewed literature shows that attacks against vehicles' body and physical systems extend well beyond conventional vehicle theft, encompassing threats to confidentiality (e.g., covert surveillance and GPS tracking), integrity (e.g., odometer rollback and license plate cloning), availability (e.g., fuel siphoning, component theft, and structural sabotage), and passengers safety (e.g., carjacking and intentional collisions). This highlights that compromising a vehicle often requires no cyber intrusion, but rather exploits physical access, human behavior, and operational weaknesses.

Existing countermeasures are predominantly preventive, relying on physical hardening, surveillance, secure parking, periodic inspections, tamper-evident mechanisms, and user awareness. Although recent approaches incorporate telematics, onboard sensors, and connected services to improve detection and response, most solutions remain attack-specific and depend heavily on human vigilance, with few unified frameworks capable of addressing multiple physical threats simultaneously.



Fig. 25. K.I.T.T. (Knight 2000): The ultimate AI-powered, autonomous safeguard on four wheels, used in the Knight Rider American action crime drama television series in 1982.

Overall, research on physical attacks remains fragmented compared with software and in-vehicle network security. Limited attention has been devoted to integrated, intelligent monitoring systems capable of fusing information from multiple sensors to detect, reason about, and respond to diverse physical threats in real time. Future research should therefore move toward holistic vehicle protection architectures that continuously monitor both the vehicle's surroundings and internal state, autonomously identifying suspicious activities and initiating appropriate defensive actions. Interestingly, this concept was already envisioned over four decades ago through KITT (Knight Industries Two Thousand), the intelligent vehicle featured in the 1980s television series Knight Rider (viz., Fig. 25). At the time, such a self-aware, passenger-protective vehicle capable of perceiving threats, making decisions, and actively safeguarding its occupants was purely fictional. Today, however, rapid advances in artificial intelligence, multi-modal sensor fusion, connected vehicle technologies, robotics, and edge computing are steadily transforming that vision into a realistic engineering objective. Although significant scientific and technological challenges remain, the gap between science fiction and reality is narrowing rapidly, suggesting that intelligent vehicles capable of autonomously protecting both themselves and their occupants may become a practical reality in the foreseeable future.

B. Discussion on Research Direction 2 (RD2)

In this subsection, we analyze the reviewed attacks and countermeasures related to "Attack on Vehicles' Access and Start Systems" (i.e., **RD2**) to clarify the current status, pending challenges, and highlight the existing gaps.

The reviewed literature indicates that attacks targeting vehicle access and start systems have evolved from simple replay and code-grabbing attacks on legacy Remote Keyless Entry (RKE) systems to highly sophisticated attacks exploiting weaknesses in both wireless protocols and vehicle architectures (we often talk about "mouse jacking"). While rolling-code mechanisms significantly reduced the effectiveness of

classical replay attacks, adversaries rapidly adapted by introducing techniques such as RollJam, relay attacks, CAN injection, and OBD-II key reprogramming. More recently, researchers and security analysts demonstrated that several vehicle models could be unlocked by physically accessing exposed CAN wiring located behind external components, such as headlights or bumpers (viz., Fig. 18) [221], and injecting forged CAN messages into the Body Control Module (BCM), completely bypassing the wireless authentication mechanism. These attacks demonstrate that securing only the RF communication channel is insufficient when alternative physical attack paths remain available.

Current countermeasures rely primarily on stronger cryptography, challenge-response protocols, Ultra-Wideband (UWB) ranging, secure gateways, and intrusion detection systems. Nevertheless, recent developments show that the threat landscape continues to evolve. For example, modified firmware (a.k.a, Unleashed 2.0 or PCFW 2.0) distributed through underground communities for tools such as the Flipper Zero reportedly automates attacks against vulnerable rolling-code implementations, lowering the technical barrier for vehicle theft [222]. Although such tools generally exploit implementation weaknesses rather than breaking modern cryptographic algorithms themselves, they illustrate how offensive capabilities are becoming increasingly accessible. Similarly, practical attacks against some commercial UWB implementations have demonstrated that protocol specifications alone do not guarantee security, emphasizing the need for robust implementations and continuous security validation.

An important research direction lies in exploiting the unique physical characteristics of radio transmissions rather than relying solely on digital cryptography. Recent advances in AI-based Radio Frequency (RF) fingerprinting have shown that every wireless transmitter exhibits subtle hardware imperfections that act as a unique fingerprint. Instead of authenticating only the transmitted cryptographic message, future vehicle access systems could additionally verify whether the received signal originates from the legitimate keyfob associated with that specific vehicle by employing a dedicated machine-learning model for each vehicle-keyfob pair. Such a multi-factor physical-layer authentication mechanism would substantially strengthen defenses against replay, relay, cloning, and signal injection attacks. Combined with secure in-vehicle architectures and authenticated CAN communications, AI-driven RF fingerprinting represents a promising step toward next-generation intelligent vehicle access systems.

C. Discussion on Research Direction 3 (RD3)

In this subsection, we analyze the reviewed attacks and countermeasures related to "Attack on Vehicles' Electronic and Software Systems" (i.e., **RD3**) to clarify the current status, pending challenges, and highlight the existing gaps.

The reviewed literature demonstrates that automotive cyberattacks have evolved from isolated exploits targeting individual ECUs into sophisticated, multi-stage attacks capable of compromising the entire electronic ecosystem. Early attacks primarily relied on physical access through diagnostic ports or direct CAN connections, whereas modern attacks increasingly exploit externally exposed interfaces—including Bluetooth, Wi-Fi, cellular telematics, V2X communications, Automotive Ethernet, and Over-the-Air (OTA) update infrastructures—to obtain remote entry points. Landmark incidents such as the Jeep Cherokee remote takeover [69] illustrated that compromising a seemingly non-critical infotainment system can ultimately provide access to safety-critical vehicle functions, fundamentally changing the automotive industry's perception of cybersecurity. More recently, CAN injection attacks exploiting exposed wiring behind headlights have further demonstrated that attackers continuously discover unexpected pathways into vehicle networks [221], emphasizing that every electronic interface should be considered a potential attack surface rather than relying solely on perimeter defenses.

Existing countermeasures have significantly improved automotive security through technologies such as Secure On-board Communication (SecOC), secure gateways, Hardware Security Modules (HSMs), Secure Boot, Uptane-secured OTA updates, intrusion detection systems, and authenticated diagnostic protocols. Nevertheless, these mechanisms introduce practical deployment challenges that have received relatively little attention. In several regions facing import restrictions, vehicle shortages, or limited availability of manufacturer-authorized service centers, independent repair workshops often lack legitimate access to OEM (Original Equipment Manufacturer) diagnostic platforms and cloud-based Public Key Infrastructure (PKI) authentication required for maintenance operations. Consequently, unofficial tools and modified software—many reportedly distributed through underground marketplaces—are increasingly used to bypass security mechanisms protecting diagnostic and firmware flashing procedures. Although these tools enable maintenance and ECU replacement outside the official ecosystem, they also create opportunities for installing malicious or modified firmware, intentionally or unintentionally. Moreover, the globalization of connected vehicles raises additional supply-chain concerns, where compromised credentials, insider threats within authorized dealerships, or remotely abused diagnostic accounts could allow attackers to perform unauthorized maintenance operations through legitimate manufacturer infrastructures, thereby undermining the trust assumptions on which current security architectures rely.

Future research should therefore move beyond protecting communication channels toward establishing trust throughout the entire vehicle lifecycle, including manufacturing, maintenance, software updates, repair, resale, and decommissioning. Existing security architectures largely assume that firmware updates, diagnostic sessions, and ECU replacements are performed by trusted entities using uncompromised credentials. However, this assumption may not hold in regions where access to official maintenance infrastructure is limited or where unofficial repair ecosystems have become widespread. Consequently, future solutions should support secure and auditable maintenance procedures that remain effective even outside the OEM ecosystem. Promising research directions include remote

attestation of newly flashed firmware, hardware-backed runtime integrity verification, cryptographically verifiable maintenance records, zero-trust diagnostic architectures, and continuous behavioral monitoring capable of detecting compromised ECUs even after they have been legitimately programmed. As software-defined vehicles become increasingly interconnected and frequently cross international borders, cybersecurity must evolve from protecting individual components to establishing an end-to-end chain of trust that spans the vehicle's entire operational lifecycle.

Last but not the least, the use of PUFs (Physical Unclonable Functions) for in-vehicle authentication was showns to be promising. However, PUFs do suffer from different forms of threats, and their use in security protocols has to be carefully handled [144]–[147].

D. Discussion on Research Direction 4 (RD4)

In this subsection, we analyze the reviewed attacks and countermeasures related to "Attack on ADAS and Autonomous Driving Systems" (i.e., **RD4**) to clarify the current status, pending challenges, and highlight the existing gaps.

The security of ADAS-equipped vehicles has become one of the most active research areas in automotive cybersecurity because successful attacks directly threaten passenger safety rather than merely compromising digital assets. Unlike conventional cyberattacks that primarily target software components, many ADAS attacks exploit the physical interaction between the perception system and its surrounding environment. As demonstrated through Section VII, attackers can intercept sensor data, fabricate false observations, modify sensor outputs, or interrupt the sensing process entirely using techniques ranging from GPS spoofing and radar injection to adversarial traffic signs, projected objects, and physical vandalism. As autonomous driving systems increasingly rely on artificial intelligence and multi-sensor perception, the attack surface continues to expand with every additional sensor, communication interface, and machine-learning component integrated into modern vehicles. Consequently, protecting ADAS systems can no longer rely solely on traditional cybersecurity mechanisms, but instead requires securing the complete sensing, perception, decision-making, and actuation pipeline.

Current industrial countermeasures adopt a defense-in-depth strategy combining secure hardware, cryptographic protection, secure boot, authenticated firmware updates, encrypted communications, and multi-sensor fusion. By cross-validating observations from cameras, LiDAR, radar, GNSS, IMUs, and HD maps, sensor fusion has become the primary defense against many physical attacks. Nevertheless, existing solutions remain largely reactive, as coordinated attacks can simultaneously compromise multiple sensing modalities, while deep-learning perception models remain vulnerable to novel adversarial and context-aware attacks. Furthermore, the development of robust ADAS defenses is hindered by the scarcity of comprehensive public datasets. Existing datasets [138]–[143] generally evaluate individual sensing modalities in isolation, with very few providing synchronized multi-modal adversarial data encompassing camera, LiDAR, radar, localization, HD maps, and semantic context. Consequently, current countermeasures improve resilience but are still insufficient to guarantee trustworthy autonomous perception against sophisticated adversaries.

Future research should therefore shift from isolated sensor protection toward holistic and adaptive autonomous driving architectures. A key priority is the development of open, standardized multi-modal adversarial datasets containing synchronized camera, LiDAR, radar, GNSS, IMU, HD maps, and contextual information under realistic attack scenarios. Such datasets would enable reproducible benchmarking and facilitate the development of robust AI-based perception systems. Future ADAS architectures should also integrate AI-driven anomaly detection capable of evaluating cross-sensor consistency, semantic context, and temporal behavior to identify attacks before unsafe decisions are made. Finally, advances in explainable AI, continual learning, and secure cooperative perception through V2V and V2I communications are expected to further improve the resilience of autonomous vehicles against both cyber and physical attacks.

Finally, despite the rapid advancement of Agentic AI and its anticipated integration into future autonomous vehicles, the security of Agentic Vehicles (AgVs) remains largely unexplored in the automotive cybersecurity literature. As discussed earlier, existing research predominantly focuses on securing vehicle communication protocols, in-vehicle networks, Electronic Control Units (ECUs), sensors, and perception models, while largely overlooking threats targeting the reasoning, planning, memory, and tool orchestration capabilities of autonomous agents. As a result, attack vectors such as prompt injection, goal manipulation, memory poisoning, and malicious tool invocation remain insufficiently studied, highlighting a significant research gap. Addressing these emerging threats will be essential to ensuring the security, safety, and trustworthiness of next-generation Agentic Vehicles.

In TABLE III, we provide a superficial summary of the existing countermeasures, their description, along with their disadvantages. We can see that although various countermeasures exist to protect against these threats, they are inherently bound by trade-offs and practical limitations. Technical and hardware mechanisms often introduce operational friction—such as limiting system customization, requiring complex key management, or inflating vehicle costs—while physical barriers can degrade keyless convenience or risk key loss without preventing alternative attack vectors. Furthermore, passive defenses only detect breaches rather than prevent them, and human-focused strategies rely on continuous vigilance against evolving tactics. Ultimately, no single solution offers absolute security without compromising usability, cost, or implementation feasibility.

IX. Conclusion

The automotive industry is undergoing a profound transformation from mechanically dominated vehicles into highly interconnected Software-Defined Vehicles (SDVs) and autonomous Cyber-Physical Systems (CPS). While this evo-

TABLE III
A SUPERFICIAL SUMMARY OF THE EXISTING COUNTERMEASURES, THEIR DESCRIPTION, AND DISADVANTAGES.

RDs	Countermeasure	Description	Disadvantages
RD1	Bug detector	Detect spying devices	▲ Not common in the public domain
	Physical inspection	Detect malicious physical anomalies	▲ Requires a set of physical inspection skills ▲ Not possible as a daily habit
	Public registry cross-checks (Ministry)	Protect during vehicle selling (frauds)	▲ Assumes the existence of a trustworthy agency ▲ Risk of corrupted employees at the public registry
	Trackers for vehicle recovery	Allows stolen vehicle recovery	▲ Requires VHF radio (LoJack) or GPS company ▲ Maybe vulnerable to jammers
RD2	RF fingerprinting (AI-based)	Protect against keyfob cloning and keyfob spoofing (e.g., relay)	▲ Has to become a standard implemented by vehicle manufacturers and a new model requires to be flushed into the vehicle's memory for any replacement keys
RD4	Anti-spoofing mechanisms	Protect against GPS, LiDAR, sound and road object spoofing	▲ Requires the development and embedding of robust AI classification systems
RD1, RD2	Alarm and surveillance systems	Discourage attackers and record the breaches	▲ Does not stop the breach, it only delays or records it
	Secure and safe parking lot	Discourage attackers	▲ Not always available
	Immobilizers and access systems	Discourage attackers	▲ Can be bypassed physically, or using mouse jacking
	Rolling-code access systems	Protect against signal interception and replay	▲ Not reliable. Recent attacks showed that this can be bypassed (Flipper Zero with firmware Unleashed 2.0)
RD2, RD4	RF anti-jamming	Protect against jamming attacks	▲ NONE (but may increase the cost of the vehicle)
RD3, RD4	Secure boot and software authentication	Protect against running corrupted software	▲ Limited kernel customization ▲ Private key management
RD1-RD3	OBD-II port locker	Block access to the OBD-II port	▲ Risk of losing the removal key
	Faraday pouch	Prevent unauthorized communications with vehicle's keyfob	▲ Does not stop other theft methods ▲ Defeats keyless convenience
RD2-RD4	Hardware Security module	Protect against physical attacks Protect against side channel attacks	▲ NONE (may increase the cost of the vehicle)
	Secure in-vehicle network architecture	Protect against attacks that pivot from one network to another	▲ NONE (may increase the cost of the vehicle)
	Cryptographic protocols (encryption, authentication, integrity, non-repudiation)	Protect in-vehicle communicaitons	▲ Has to be a standard that enforces the fundamental goals of security, e.g., SecOC. ▲ Security protocols have to be formally verified.
RD1-RD4	User awareness and vigilance	Be aware of breaches when they happen	▲ Requires social-engineering skills ▲ Be aware of the latest social-engineering tactics
	User authorization	Only authorized and trusted drivers can access the vehicle and drive it	▲ Need to run background check on people ▲ Not scalable (e.g., car rent)
	Tamper-evident hardware	Detect physical breach attempts	▲ It allows detection but not prevention
	Car insurance	Get paid back for any partial or complete vehicle theft	▲ Risk of insurance fraud ▲ Sometimes not feasible due to religious rules
	Artificial Intelligence (as a tool)	Detect and prevent various types of attacks discussed in **RD1**, **RD2**, **RD3**, and **RD4**	▲ Require AI regulations and governance ▲ Consider adverarial models attacks

lution has significantly improved vehicle safety, efficiency, and driving convenience, it has also fundamentally reshaped the automotive threat landscape. Vehicle attacks have progressed far beyond conventional theft and physical vandalism to encompass sophisticated cyberattacks targeting wireless communication interfaces, embedded software, in-vehicle networks, cloud-connected services, and AI-driven perception systems. As a result, modern vehicle security can no longer be viewed solely as a software or networking problem, but rather as a multidisciplinary challenge involving hardware security, cryptography, wireless communications, embedded systems, artificial intelligence, and functional safety.

In this survey, we proposed an orthogonal taxonomy that classifies attacks against modern vehicles into four complementary research directions: attacks on vehicle body and physical systems, attacks on vehicle access and engine-start systems, attacks on electronic and software systems, and attacks on ADAS and autonomous driving systems. For each category, attacks were further organized according to the compromised security service, followed by a systematic review of representative countermeasures and a discussion of current limitations. By organizing the literature according to the primary subsystem under attack, the proposed taxonomy reduces overlaps between existing classifications while providing a unified perspective of the complete automotive attack surface.

The survey demonstrates that although considerable progress has been achieved in strengthening automotive cybersecurity through secure hardware, cryptographic protocols, intrusion detection systems, secure software engineering, sensor fusion, and artificial intelligence, existing defense mechanisms remain largely reactive and domain-specific. Moreover, several important research gaps remain, including the limited availability of realistic multi-modal adversarial datasets for ADAS research, the growing complexity of securing software-defined vehicle ecosystems, the increasing dependence on cloud-based services and over-the-air software updates, and the need for integrated security architectures capable of protecting multiple vehicle subsystems simultaneously. These challenges become even more critical as future vehicles continue to incorporate larger numbers of sensors, software components, wireless interfaces, and autonomous driving capabilities.

Overall, securing next-generation vehicles will require a

transition from isolated security mechanisms toward holistic, adaptive, and continuously evolving security architectures that integrate cyber, physical, and AI-driven protection mechanisms throughout the entire vehicle lifecycle. Future research should emphasize context-aware threat detection, trustworthy artificial intelligence, secure collaborative perception, hardware-assisted security, privacy-preserving cloud services, and standardized benchmarking datasets for evaluating emerging attack and defense techniques. We hope that the taxonomy, analysis, and research directions presented in this survey will provide researchers, automotive manufacturers, and cybersecurity practitioners with a comprehensive reference for understanding the rapidly evolving automotive threat landscape and for developing resilient security solutions for future software-defined and autonomous vehicles.

GENERATIVE AI USE DISCLOSURE

OpenAI ChatGPT (GPT-5.5) and Google Gemini 1.5 Pro were used solely to improve readability, grammar, and language clarity. They were not used to generate scientific content, analyze data, or formulate conclusions; the authors review, verify, and take full responsibility for the accuracy and integrity of the final manuscript.

FUNDING STATEMENT

This research received no specific grant from any fundingagency in the public, commercial, or not-for-profit sectors.

REFERENCES

[1] E. A. Lee, "Cyber physical systems: Design challenges," in Proceedings of the 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing, pp. 363–369, doi: 10.1109/ISORC.2008.25, 2008.

[2] B. Scheneir. "Cybersecurity is Failing at Two Things: Patching & Authentication," in RSA Confernce, 2018.

[3] M. Broy, M. Gleirscher, P. Kluge, W. Krenzer, S. Merenda, and D. Wild. "Automotive Architecture Framework: Towards a Holistic and Standardised System Architecture Description". White Paper of the IBM Corporation and TUM Technical Report, https://mediatum.ub.tum.de/doc/1094456/document.pdf, 2009 (Accessed on August 10th, 2026).

[4] S. A. Bagloee, M. Tavana, M. Asadi, and T. Oliver. "Autonomous Vehicles: Challenges, Opportunities, and Future Implications for Transportation Policies". Journal of Modern Transportation, vol. 24, pp. 284–303, Springer, doi: 10.1007/s40534-016-0117-3, 2016.

[5] A. Eskandarian, Ed., "Handbook of Intelligent Vehicles", Volume 2, Springer, 2012.

[6] D. Elliott, W. Keen, and L. Miao, "Recent Advances in Connected and Automated Vehicles," Journal of Traffic and Transportation Engineering (English Edition), vol. 6, Issue 2, pp. 109-131, doi: 10.1016/j.jtte.2018.09.005, 2019.

[7] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, and S. Savage, "Experimental Security Analysis of a Modern Automobile," in Proceedings of the 2010 IEEE Symposium on Security and Privacy, pp. 447–462, IEEE, doi: 10.1109/SP.2010.34, 2010.

[8] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, and T. Kohno, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," in Proceedings of the 20th USENIX Security Symposium, 2011.

[9] S. M. Shaheen, S. N. Dev, N. P. Somakumar, and S. Vivekanand V, and G. G. Lakshmi. "AI-Powered Surveillance System for Fake Number Plate Identification and Stolen Vehicle Recovery," 2026 International Conference on Computational Robotics, Testing and Engineering Evaluation (ICCRTEE), pp. 1-6, doi: 10.1109/ICCRTEE68719.2026.11566455, 2026.

[10] G. Farrell, A. Tseloni, and N. Tilley, "The Effectiveness of Vehicle Security Devices and their Role in the Crime Drop," Criminology & Criminal Justice, vol. 11, no. 1, pp. 21–35, Sage Journals, 2011.

[11] J. S. Howland, "Vehicle Anti-Theft Security System Design", Final Report, NCJ no. 74475, U.S. Department of Justice, Office of Justice Programs, NCJRS Virtual Library, 1978.

[12] A. D. Babalola and M. S. Olokun. "Design and Construction of Smart Vehicle Security System Using GPS and Spy Cam", Journal of Engineering Research and Reports, 21 (2), pp. 31-47, https://journaljerr.com/index.php/JERR/article/view/553/1107, 2021.

[13] P. Ekblom. "Designing Products against Crime" in R. Wortley and M. Townsley (Eds.), Environmental Criminology and Crime Analysis, 2nd Edition. London: Taylor and Francis, 2017.

[14] C. Patsakis and K. Dellios, "Securing In-Vehicle Communication and Redefining the Role of Automotive Immobilizer," in the proceddings of the International Conference on Security and Cryptography, SciTePress, doi: 10.5220/0004024302210226, 2012.

[15] P. Finn, "Labeling Automobile Parts to Combat Thefts," FBI Law Enforcement Bulletin, vol. 69, no. 4, pp. 10–14, U.S. Department of Justice, Office of Justice Programs, NCJ no. 241089, 2000.

[16] M. Wolf, A. Weimerskirch, and T. Wollinger, "State of the Art: Embedding Security in Vehicles," EURASIP Journal on Embedded Systems, vol. 2007, no. 074706, Springer, 2007.

[17] F. Sommer, J. Dürrwang, and R. Kriesten. "Survey and Classification of Automotive Security Attacks," Information, vol. 10, no. 4, doi: 10.3390/info10040148, MDPI, 2019.

[18] H. Gong, S. Hong, S. Yang, R. Chang, W. Shen, Z. Yuan, C. Yu, and Y. Zhou, "Harness: Transparent and Lightweight Protection of Vehicle Control on Untrusted Android Automotive Operating System," in Proceedings of the 34th USENIX Security Symposium, pp. 4265–4284, no. 220, 2025.

[19] W. Adi and A. Mars, "Physical and Mechatronic Security, Technologies and Future Trends for Vehicular Environment," in Computer Science: Cryptography and Security, ArXiv: 1805.07570, 2018 (Accessed on August 10th, 2026).

[20] J. Sallybanks and R. Brown. "Vehicle Crime Reduction: Turning the Corner", Police Research Series , Paper 119, Policing and Reducing Crime Unit Research, Development and Statistics Directorate, ISBN 1-84082-350-X, 1999.

[21] Y. Mao, D. Shenzhi, D. Jiajun, Z. Wei, W. Can, and Y. Xinyue. "Space–Time Analysis of Vehicle Theft Patterns in Shanghai, China" ISPRS International Journal of Geo-Information, vol. 7, no. 9: 357. doi: 10.3390/ijgi7090357, 2018.

[22] S. Shirota, A. E. Gelfand, and J. Mateu. "Analyzing Car Thefts and Recoveries with Connections to Modeling Origin–Destination Point Patterns," Spatial Statistics, voL. 38, no. 100440, doi: 10.1016/j.spasta.2020.100440, 2020.

[23] G. Farrell. "The Great American Car Crime Decline". Security Journal, vol. 38, no. 10, doi: 10.1057/s41284-024-00452-2, Springer, 2025.

[24] H. M. Marhoon, A. I. Alanssari, and N. Basil, "Design and Implementation of an Intelligent Safety and Security System for Vehicles Based on GSM Communication and IoT Network for Real-Time Tracking", J Robot Control (JRC), vol. 4, no. 5, pp. 708–718, Oct. 2023.

[25] A. Mustafa, H. Jameel, M. Baqar, R. A. Khan, Z. M. Yaqoob, Z. Rahim, and S. Khan "Vehicle Intrusion and Theft Control System Using GSM and GPS—An Advance and Viable Approach," Asian Journal of engineering, sciences, and technology, vol. 2, Issue 2, 2012.

[26] K. B. Kelarestaghi, M. Foruhandeh, K. Heaslip, and R. Gerdes, "Vehicle Security: Risk Assessment in Transportation," in Computer Science: Cryptography and Security, ArXiv (1804.07381), 2018.

[27] W. Rhodes and R. Kling, "Evaluation of the Effectiveness of Automobile Parts Marking and Anti-Theft Devices on Preventing Theft", U.S. Department of Justice, Office of Justice Programs, NCJ no. 208800, 2003.

[28] B. I. Kwak, J. Woo and H. K. Kim, "Know your Master: Driver Profiling-based Anti-Theft Method," in the proceedings of the 14th Annual Conference on Privacy, Security and Trust (PST), pp. 211-218, doi: 10.1109/PST.2016.7906929, IEEE, 2016.

[29] R. V. Clarke and P. M. Harris, "Auto theft and its prevention," In the University of Chicago Press journals, Crime and Justice, vol. 16, pp. 1–54, doi: 10.1086/449203, 1992.

[30] I. Ayres and S. D. Levitt, "Measuring Positive Externalities from Unobservable Victim Precaution: An Empirical Analysis of Lojack,"

in Quarterly Journal of Economics, vol. 113, no. 1, pp. 43–77, doi: 10.1162/003355398555522, 1998.

[31] J. C. van Ours and B. Vollaard, "The Engine Immobiliser: A Non-starter for Car Thieves," The Economic Journal, vol. 126, no. 593, pp. 1264–1291, doi: 10.1111/ecoj.12196, 2016.

[32] H. Copes and M. Cherbonneau, "The key to auto theft: Emerging methods of auto theft from the offenders' perspective," British Journal of Criminology, vol. 46, no. 5, pp. 917–934, doi: 10.1093/bjc/azl001, 2006.

[33] S. Kriven and E. Ziersch, "New car security and shifting vehicle theft patterns in Australia," Security Journal, vol. 20, no. 2, pp. 111–122, Springer, 2007.

[34] M. G. Maxfield and R. V. Clarke, Eds., "Understanding and Preventing Car Theft, Crime Prevention Studies", vol. 17, Monsey, NY: Criminal Justice Press, ISSN: 1065-7029, 2004.

[35] S. Donkin and M. Wellsmith, "Cars Stolen in Burglaries: The Sandwell Experience," Security Journal, vol. 19, no. 1, pp. 22–32, Springer, 2006.

[36] B. Jacobs, V. Topalli, and R. Wright, "Carjacking, streetlife, and offender motivation," British Journal of Criminology, vol. 43, no. 4, pp. 673–688, Oxford University Press, 2003.

[37] J. Van Wilsem. "Criminal Victimization in Cross-National Perspective: An Analysis of Rates of Theft, Violence and Vandalism Across 27 Countries". European Journal of Criminology, vol. 1, no. 1, pp. 89–109, Sage Journals, doi: 10.1177/1477370804038708, 2004.

[38] H. Fu, H. Zhang, G. Zhang; Y. Yang, R. Spolaor, X. Cheng, and P. Hu. "Vehisper: Eavesdropping on In-Vehicle Audio via Secondary Magnetic Leakage," in IEEE Transactions on Mobile Computing, vol. 25, no. 9, pp. 14625-14641, doi: 10.1109/TMC.2026.3684118, 2026.

[39] A. Mishra, S. Lee, D. Kim, and S. Kim. "In-Cabin Monitoring System for Autonomous Vehicles". Sensors 2022, vol. 22, no. 12, doi: 10.3390/s22124360, MDPI, 2022.

[40] S. Kim, A. Cho, and D. H. Lee. "Analysis of Threats and Countermeasures for Odomter Protection", International Journal of Automotive Technology, vol. 21, pages 1271–1281, Springer 2020.

[41] M. H. Rahman and H. C. Chin. "Recovery of Theft Vehicles: Prospects and Barriers to an ITS based Approach", 22nd KKCNN Symposium on Civil Engineering, pp. 549-554, 2009.

[42] P. Dhumal, S. Sawantbhonsale, S. Nandan, and M. Sangewar. "Auto Shield: A Review on Smart Vehicle Theft Detection Strategies," International Journal of Novel Research And Development, vol. 10, no. 4, pp. 337-341, doi: 10.56975/ijnrd.v10i4.306224, 2025.

[43] L. O'Shea, Z. Behalal, and H. Harbottle. "Where Do Stolen Cars and Parts from the UK and EU End Up?", Global Initiative Against Transnational Organized Crime. Switzerland. Retrieved from https://coilink.org/20.500.12592/7yhxpkv on 18 Aug 2026. COI: 20.500.12592/7yhxpkv, 2026.

[44] S. Gupta, A. Buriro, and B. Crispo. "DriverAuth: A risk-based multimodal biometric-based driver authentication scheme for ride-sharing platforms", Computers & Security, vol. 83, pp. 122-139, Elsevier, 2019.

[45] E. Tabarnoust, and Y. Zaz. "Robust Real-Time Recognition of Multilingual Moroccan License Plates for CPU-based Edge Devices". Discover Computing, vol. 29, no. 439, Springer, doi: 10.1007/s10791-026-10332-5, 2026.

[46] R. Garg, R. Wason, P. Arora and M. N. Hoda, "Robust Advanced Number Plate Recognition (ANPR) System from Real-Time Video Footage," in proceedings of the 12th International Conference on Computing for Sustainable Global Development (INDIACom), pp. 1-4, doi: 10.23919/INDIACom66777.2025.11115864, 2025.

[47] A. Tourani, A. Shahbahrami, S. Soroori, S. Khazaee and C. Y. Suen, "A Robust Deep Learning Approach for Automatic Iranian Vehicle License Plate Detection and Recognition for Surveillance Systems," in IEEE Access, vol. 8, pp. 201317-201330, doi: 10.1109/ACCESS.2020.3035992, 2020.

[48] Z. -X. Chen, C. -Y. Liu, F. -L. Chang and G. -Y. Wang, "Automatic License-Plate Location and Recognition Based on Feature Salience," in IEEE Transactions on Vehicular Technology, vol. 58, no. 7, pp. 3781-3785, doi: 10.1109/TVT.2009.2013139, 2009.

[49] Y. Alborzi, T. S. Mehraban, J. Khoramdel and A. N. Ardekany, "Robust Real time Lightweight Automatic License plate Recognition System for Iranian License Plates," in the proceedings of the 7th International Conference on Robotics and Mechatronics (ICRoM), pp. 352-356, doi: 10.1109/ICRoM48714.2019.9071863, 2019.

[50] M. Kiran, B. Ray, J. Hassan, A. Kashyap, V. Y. Chandrappa, "Blockchain-based secure Ownership Transfer Protocol for smart objects in the Internet of Things", Internet of Things, vol. 25, doi: 10.1016/j.iot.2023.101002, Elsevier, 2024.

[51] T. Li, Z. Jin and C. Pang, "Secured Ownership Transfer Scheme for Low-Cost RFID Tags," in the 2010 Third International Conference on Intelligent Networks and Intelligent Systems, pp. 584-587, doi: 10.1109/ICINIS.2010.13, ACM, 2010.

[52] V. Cherneva and J. L. Trahan, "TP-OTP: Two-Party, Ownership Transfer Protocol for RFID Tags Based on Quadratic Residues," in the proceedings of the 2021 IEEE Green Energy and Smart Systems Conference (IGESSC), pp. 1-6, doi: 10.1109/IGESSC53124.2021.9618683, 2021.

[53] L. Urciuoli. "Fuel Theft in Road Freight Transport: Understanding Magnitude and Impacts of Anti-Theft Devices". Journal of Transportation Security, vol. 13, pp. 1–18, doi: 10.1007/s12198-020-00207-1, 2020.

[54] C. Sey, H. Lei, W. Qian, X. Li, L. D. Fiasam, S. L. Kodjiku, I. Adjei-Mensah, I. O. Agyemang. "VBlock: A Blockchain-Based Tamper-Proofing Data Protection Model for Internet of Vehicle Networks". Sensors, vol. 22, no. 20, doi: 10.3390/s22208083, MDPI, 2022.

[55] S. Kamkar. "Drive it like you hacked it: New attacks and tools to wirelessly control gates, garages, and cars", Conference presentation, DEF CON 23, Las Vegas, NV, United States, 2015, https://samy.pl/defcon2015/. (Accessed on August 10th, 2026)

[56] J. Hamborg, T. Lauser, and C. Krauß. "RollCAN – CAN-bus based RollJam-Attack". In Proceedings of the 2nd Cyber Security in CarS Workshop (CSCS '25), no. 4, pp. 1–7, doi: 10.1145/3736130.3762686, ACM, 2025.

[57] R. P. Parameswarath and B. Sikdar, "A PUF-based Lightweight and Secure Mutual Authentication Mechanism for Remote Keyless Entry Systems," In the 2022 IEEE Global Communications Conference (GLOBECOM 2022), pp. 1776-1781, doi: 10.1109/GLOBECOM48099.2022.10001217, IEEE, 2022.

[58] R. P. Parameswarath and B. Sikdar, "A Secure PUF-Based Authentication Protocol for Remote Keyless Entry Systems in Cars," in IEEE Transactions on Vehicular Technology, vol. 73, no. 7, pp. 9825-9838, doi: 10.1109/TVT.2024.3363000, IEEE, 2024.

[59] V. K. V. V. Bathalapalli, S. P. Mohanty, E. Kougianos, V. Iyer and B. Rout, "iTPM: Exploring PUF-based Keyless TPM for Security-by-Design of Smart Electronics," 2023 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), pp. 1-6, doi: 10.1109/ISVLSI59464.2023.10238586, IEEE, 2023.

[60] Y. Zhao, F. Shen, G. Xu, and G. Wang. "A Spatial-Temporal Approach Based on Antenna Array for GNSS Anti-Spoofing". Sensors, vol. 21, no. 3, doi: 10.3390/s21030929, MDPI, 2021.

[61] L. Meng, L. Yang, W. Yang, and L. Zhang. "RETRACTED: A Survey of GNSS Spoofing and Anti-Spoofing Technology". Remote Sensing, vol. 14, no. 19, doi: 10.3390/rs14194826, MDPI, 2022.

[62] K. Hu and Y. Huang. "A Composite Detection Method for Direct GPS Deception Attack". IOP Conference Series: Materials Science and Engineering, vol. 790, no. 1, doi: 10.1088/1757-899X/790/1/012028, 2020.

[63] A. Argyriou, "Obfuscation of Human Micro-Doppler Signatures in Passive Wireless RADAR," in IEEE Access, vol. 11, pp. 40121-40127, doi: 10.1109/ACCESS.2023.3269435, IEEE, 2023.

[64] R. Lo Cigno, G. Gringoli, S. Bartoletti, M. Cominelli, L. Ghiro, and S. Zanini. "Communication and Sensing: Wireless PHY-Layer Threats to Security and Privacy for IoT Systems and Possible Countermeasures". Information, vol. 16, no. 1, doi: 10.3390/info16010031, MDPI, 2025.

[65] M. Ordean and F. D. Garcia. "Millimeter-Wave Automotive Radar Spoofing", Cryptography and Security, arXiv:2205.06567, 2022 (Accessed on August 10th, 2026).

[66] G. Galati, G. Pavan, K. Savci, and C. Wasserzier. "Counter-Interception and Counter-Exploitation Features of Noise Radar Technology". Remote Sensing, vol. 13, no. 22, doi: 10.3390/rs13224509, MDPI, 2021.

[67] M. Rezaei, L. Hussein, and S. Moazeni. "Secure FMCW LiDAR Systems with Frequency Encryption". In Proceedings of the 2022 Workshop on Attacks and Solutions in Hardware Security (ASHES'22), pp. 35–43, doi: 10.1145/3560834.3563829, ACM, 2022.

[68] E. White, "San Francisco Tech Pranksters Create Self-Driving Traffic Jam with 50 Waymos," Road & Track, https://www.roadandtrack.com/news/a69032975/san-francisco-tech-pranksters-waymo-self-driving-car-traffic-jam/, 2025. (Accessed on August 10th, 2026)

[69] A. Greenberg, "Hackers Remotely Kill a Jeep on the Highway—With Me in It," in WIRED Security magazine, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/, 2015. (Accessed on August 10th, 2026)

[70] Y. Guo, "Research on Security Analysis and Protection Measure of Internet of Vehicles Communication Protocol under Physical Layer Attack," 2024 4th Asia-Pacific Conference on Communications Technology and Computer Science (ACCTCS), pp. 375-380, doi: 10.1109/ACCTCS61748.2024.00072, IEEE, 2024.

[71] J. Cui, J. Yu, H. Zhong, L. Wei and L. Liu, "Chaotic Map-Based Authentication Scheme Using Physical Unclonable Function for Internet of Autonomous Vehicle," in IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 3, pp. 3167-3181, doi: 10.1109/TITS.2022.3227949, IEEE, 2023.

[72] J. Ye, L. Guo, B. Yang, F. Li, L. Du, L. Guan, and W. Song. "Cyber–Physical Security of Powertrain Systems in Modern Electric Vehicles: Vulnerabilities, Challenges, and Future Visions," in IEEE Journal of Emerging and Selected Topics in Power Electronics, vol. 9, no. 4, pp. 4639-4657, doi: 10.1109/JESTPE.2020.3045667, IEEE, 2021.

[73] Q. Liu, H. Li, S. Ding and Y. Wang, "Lightweight Secure Data Exchange in Decentralized VANETs with Physical Layer Security," 2020 IEEE 92nd Vehicular Technology Conference (VTC2020-Fall), pp. 1-5, doi: 10.1109/VTC2020-Fall49728.2020.9348470, 2020.

[74] M. S. Alam, S. M. Hossain, J. Oluoch and J. Kim, "A Novel Secure Physical Layer Key Generation Method in Connected and Autonomous Vehicles (CAVs)," 2022 IEEE Conference on Communications and Network Security (CNS), pp. 1-6, doi: 10.1109/CNS56114.2022.9947262, IEEE, 2022.

[75] H. Chen, X. Chen, L. Fan and C. Chen, "Classified security protection evaluation for vehicle information system," 2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), pp. 1-6, doi: 10.1109/SSIC.2015.7245673, IEEE, 2015.

[76] H. Ji, J. Wang, L. Wang, G. Sun, L. Jin and J. Fang, "Data Security Testing Method of Intelligent and Connected Vehicles Based on Typical Scenarios," in the 2023 IEEE 8th International Conference on Intelligent Transportation Engineering (ICITE), pp. 153-159, doi: 10.1109/ICITE59717.2023.10733896, IEEE, 2023.

[77] J. Madden, B. McMillin and A. Sinha, "Environmental Obfuscation of a Cyber Physical System - Vehicle Example," in the 2010 IEEE 34th Annual Computer Software and Applications Conference Workshops, pp. 176-181, doi: 10.1109/COMPSACW.2010.39, IEEE, 2010.

[78] R. Akasheh and A. Badawy, "Group Secret Key Generation for Vehicular Networks Based on Physical Layer Security," in the proceedings of the 2025 International Wireless Communications and Mobile Computing (IWCMC), pp. 1078-1083, doi: 10.1109/IWCMC65282.2025.11059540, IEEE, 2025.

[79] J. Qin and J. Liu, "Multi-Access Edge Offloading Based on Physical Layer Security in C-V2X System," in IEEE Transactions on Vehicular Technology, vol. 71, no. 7, pp. 6912-6923, doi: 10.1109/TVT.2022.3164896, IEEE, 2022.

[80] X. Luo, Y. Liu, H. -H. Chen and Q. Guo, "Physical Layer Security in Intelligently Connected Vehicle Networks," in IEEE Network, vol. 34, no. 5, pp. 232-239, doi: 10.1109/MNET.011.1900628, IEEE, 2020.

[81] Y. Burakova, B. Hass, L. Millar, and A. Weimerskirch, "Truck Hacking: An Experimental Analysis of the SAE J1939 Standard". In: WOOT. 2016, in the 10th USNIX Workshops in Offensive Technologies, 2016.

[82] S. Mukherjee, R. Chatterjee and J. Daily, "TruckSentry: Context Aware Intrusion Detection and Prevention System for J1939 Networks," in IEEE Open Journal of Intelligent Transportation Systems, vol. 6, pp. 294-309, doi: 10.1109/OJITS.2025.3545474, IEEE, 2025.

[83] X. Zeng, F. Wang, B. Wang, C. Wu, K. J. R. Liu and O. C. Au, "In-Vehicle Sensing for Smart Cars," in IEEE Open Journal of Vehicular Technology, vol. 3, pp. 221-242, doi: 10.1109/OJVT.2022.3174546, IEEE, 2022.

[84] R. Verdult, F. D. Garcia, and J. Balasch. "Gone in 360 seconds: Hijacking with Hitag2," In Proceedings of the 21st USENIX Conference on Security Symposium, Security'12, page 37, ACM, 2012.

[85] N. Soltani, K. Sankhe, J. Dy, S. Ioannidis, and K. Chowdhury. "More is Better: Data Augmentation for Channel-Resilient RF-Fingerprinting". IEEE Communications Magazine, vol. 58, no. 10, pp. 66–72, IEEE, 2020.

[86] T. Jian, B. C. Rendon, E. Ojuba, N. Soltani, Z. Wang, K. Sankhe, A. Gritsenko, J. Dy, K. Chowdhury, and S. Ioannidis. "Deep Learning for RF Fingerprinting: A Massive Experimental Study". IEEE Internet of Things Magazine, vol. 3, no. 1, pp. 50–57, IEEE, 2020.

[87] A. Francillon, B. Danev, and S. Capkun. "Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars". IACR CryptologyePrint Archive, 2010/332, https://eprint.iacr.org/2010/332, 2010 (Accessed on August 10th, 2026).

[88] A. I. Alrabady and S. M. Mahmud. "Analysis of Attacks against the Security of Keyless-Entry Systems for Vehicles and Suggestions for Improved Designs". IEEE Transactions on Vehicular Technology, vol. 54, no. 1, pp. 41–50, IEEE, 2005.

[89] K. Ren, Q. Wang, C. Wang, Z. Qin, and X. Lin. "The Security of Autonomous Driving: Threats, Defenses, and Future Directions". in Proceedings of the IEEE, vol. 108, no. 2, pp. 357–372, IEEE, 2020.

[90] T. Bianchi, A. Brighente, and M. Conti. "SoK: Stealing Cars Since Remote Keyless Entry Introduction and How to Defend From It", in Computer Sience: Cryptography and Security, ArXiv: 2505.02713, 2025 (Accessed on Augest 10th, 2026).

[91] A. Kapulica, V. Dakić, Z. Morić, and R. Petrunić. "Key Fob Replay Attacks on Personal Vehicles: Vulnerabilities and Mitigation Strategies". In 2024 International Congress on Human-Computer Interaction,Optimization and Robotic Applications (HORA), pp. 1–5, doi: 10.1109/HORA61326.2024.10550523, 2024.

[92] G. Avoine, I. Boureanu, D. Gérault, G. P. Hancke, P. Lafourcade, and C. Onete. "From Relay Attacks to Distance-Bounding Protocols", Security of Ubiquitous Computing Systens, pp. 113–130, doi: 10.1007/978-3-030-10591-4_7, Springer, 2021.

[93] M. Stocker, B. Großwindhager, C. A. Boano, and K. Römer. "Towards secure and scalable uwb-based positioning systems". In 2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS), pages 247–255, IEEE, 2020.

[94] F. D. Garcia, D. Oswald, T. Kasper, and P. 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), USENIX Association, 2016.

[95] I. Shaikh, V. Sakinal, V. Bhongale, S. Borde, R. Kamathe, and V. Hanchate. "Vulnerability assessment of vehicleaccess system using software-defined radio (SDR): attacks, testing, comparative analysis and future countermeasures". Journal of Transportation Security, vol. 19, no. 11, doi: 10.1007/s12198-026-00336-z, Springer, 2026.

[96] Z. Depp, H. Tulay, and C. Koksal. "Enhanced Vehicular Roll-Jam Attack using a Known Noise Source". Symposium on Vehicle Security and privacy (VehicleSec 2023), doi: 10.14722/vehiclesec.2023.23037, 2023.

[97] L. Csikor, H. W. Lim, J. W. Wong, S. Ramesh, R. P. Parameswarath, and M. C. Chan. "RollBack: A New Time-Agnostic Replay Attack Against the Automotive Remote Keyless Entry Systems". ACM Transactions on Cyber-Physical Systems, vol. 8, no. 1, pp. 1–25, ACM, 2024.

[98] R. Benadjila, M. Renard, J. Lopes-Esteves, and C. Kasmi. "One Car, Two Frames: Attacks on Hitag-2 Remote Keyless Entry Systems Revisited". In 11th USENIX Workshop on Offensive Technologies (WOOT17), USENIX Association, 2017.

[99] Y. J. Tu and S. Piramuthu. "On Addressing RFID/NFC-based Relay Attacks: an Overview". Decision Support Systems, vol. 129, Issue. C, doi: 10.1016/j.dss.2019.11319, ACM, 2020.

[100] S. Malladi J. Alves-Foss, and R. B. Heckendorn. "On preventing replay attacks onsecurity protocols". Proc. International Conference on Security and Management, https://apps.dtic.mil/sti/html/tr/ADA462295/, 2002 (Accessed on August 10th, 2026).

[101] V. Daza and X. Salleras. "LASER: Lightweight And SEcure Remote keyless entry protocol". Computer Science: Cryptography and Security, ArXiv: 1905.05694, 2019 (Accessed on August 10th, 2026).

[102] K. Greene, D. Rodgers, H. Dykhuizen, Q. Niyaz, K. Al Shamaileh, and V. Devabhaktuni. "A Defense Mechanism Against Replay Attack in Remote Keyless Entry Systems Using Timestamping and XOR Logic". IEEE Consumer Electronics Magazine, vol. 10, no. 1, pp. 101–108, IEEE, 2021.

[103] R. P. Parameswarath and B. Sikdar. "An Authentication Mechanism for Remote Keyless Entry Systems in Cars to Prevent Replay and RollJam Attacks". In 2022 IEEE Intelligent Vehicles Symposium (IV), pp. 1725–1730, IEEE, 2022.

[104] W. Choi, M. Seo, and D. Lee. "Sound-Proximity: 2-Factor Authentication against Relay Attack on Passive Keyless Entry and Start System". Journal of Advanced Transportation, vol. 2018, no. 1, doi: 10.1155/2018/1935974, Wiley, 2018.

[105] K. Lounis and M. Zulkernine. "Frequency Hopping Spread Spectrum to Counter Relay Attacks in PKESs". In the Conference on Risks and Security of Internet and Systems (CRiSIS'2020), pp. 49–66, Springer, 2021.

[106] G. Dabosville, H. Maghrebi, A. L. Huillery, T. Le, and J. Bringer. “On the Bright Side of Darkness: Side-Channel Based Authentication Protocol Against Relay Attacks”. In 2019 22nd EuromicroConference on Digital System Design (DSD), pp. 214–221, doi: 10.1109/DSD.2019.00040, IEEE, 2019.

[107] S. Brands and D. Chaum. “Distance-Bounding Protocols”. In Advances in Cryptology — EUROCRYPT’ 93, pp. 344–359, doi: 10.1007/3-540-48285-7_30, Springer, 1993.

[108] Y. Xie, H. J. Kim, S. Y. Chong, and T. L. Song. “Time-based Countermeasures for Relay Attacks on PKES Systems”. In Proceedings of the 16th International Conference on Informatics in Control, Automation and Robotics, vol. 1, pp. 795–801, doi: 10.5220/0007957407950801, SCITEPRESS, 2019.

[109] T. Yang, L. Kong, W. Xin, J. Hu, and Z. Chen. “Resisting Relay Attacks on Vehicular Passive Keyless Entry and Start Systems”. In 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery, pp. 2232–2236, doi: 10.1109/FSKD.2012.6234155, IEEE, 2012.

[110] D. Suresh J. Prashant, and P. Parag. “Mitigating Relay Attacks in Vehicle Access Systems using BLE and UWB”. Engineering, Technology & Applied Science Research, vol. 15, no. 5, pp. 26965–26970, doi: 10.48084/etasr.12581, 2025.

[111] S. Rizvi, J. Imler, L. Ritchey, and M. Tokar. “Securing PKES Against Relay Attacks using Coordinate Tracing and Multi-Factor Authentication”. In 2019 53rd Annual Conference on Information Sciences and Systems (CISS), pp. 1–6, doi: 10.1109/CISS.2019.8692790, IEEE, 2019.

[112] A. Vinith, S. N. Vempalli, A. Kumar, and G. Singh. “Securing Keyless Entry Systems in Modern Cars from Relay and Replay Attacks using Two-Way Authentication”. In Proceedings of the KILBY 100 7th International Conference on Computing Sciences 2023 (ICCS 2023), Available at SSRN: http://dx.doi.org/10.2139/ssrn.4502119, 2023.

[113] J. Wang, K. Lounis, and M. Zulkernine. “CSKES: A Context-based Secure Keyless Entry System”. In 2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), pp. 817–822, IEEE, 2019.

[114] U. Ahmad, H. Song, A. Bilal, M. Alazab, and A. Jolfaei. “Securing Smart Vehicles from Relay Attacks using Machine Learning”, in the Journal of Supercomputing, vol. 76, no. 4, ACM, 2020.

[115] K. Joo, W. Choi, and D. H. Lee. “Hold the Door! Fingerprinting Your Car Key to Prevent Keyless Entry Car Theft”. Computer Science: Cryptography and Security, ArXiv: 2003.13251, 2003 (Accessed on August 10th, 2026).

[116] J. C. M. Quintero, E. P. E. Cuesta, and L. J. R. Lopez. “A New Method for the Detection and Identificationof the Replay Attack on Cars using SDR Technology and Classification Algorithms”. Results in Engineering, vol. 19, no. 101243, doi: 10.1016/j.rineng.2023.101243, Elsevier, 2023.

[117] J. Wang, K. Lounis, and M. Zulkernine. “Identifying Security Features for Proximity Identification”. In the 14th IEEE International Workshop on Security, Trust and Privacy for Software Applications (STPSA’19), pp. 592-597, IEEE, 2019.

[118] K. Eykholt, I. Evtimov, E. Fernandes, B. Li, A. Rahmati, C. Xiao, A. Prakash, T. Kohno, and D. Song. “Robust Physical-World Attacks on Deep Learning Models”. Cryptography and Security, arXiv (1707.08945), 2018 (Accessed on August 10th, 2026).

[119] Y. Li, M. Cheng, C.-J. Hsieh, and T. C. M. Lee. “A Review of Adversarial Attack and Defense for Classification Methods”. Computer Science, Cryptography and Security, ArXiv: 2111.09961, 2021 (Accessed on August 10th, 2026).

[120] A. D. M. Ibrahum, M. Hussain, and J.-E. Hong. “Deep Learning Adversarial Attacks and Defenses in Autonomous Vehicles: A Systematic Literature Review from a Safety Perspective”. Artificial Intelligence Review, vol. 58, no. 1, doi: 10.1007/s10462-024-11014-8 , Springer, 2024.

[121] K. Grosse and A. Alahi. “A Qualitative AI Security Risk Assessment of Autonomous Vehicles”. Transportation Research Part C: Emerging Technologies, vol. 169, no. 104797, doi: 10.1016/j.trc.2024.104797 Elsevier, 2024.

[122] S. Dasgupta, A. Ahmed, M. Rahman, and T. N. Bandi. “Unveiling the Stealthy threat: Analyzing Slow Drift GPS Spoofing Attacks for Autonomous Vehicles in Urban Environments and Enabling the Resilience”. Computer Science: Cryptography and Security, arXiv: 2401.01394, 2024 (Accessed on August 10th, 2026).

[123] J. Tu, M. Ren, S. Manivasagam, M. Liang, B. Yang, R. Du, F. Cheng, and R. Urtasun “Physically Realizable Adversarial Examples for LiDAR Object Detection”. Computer Vision and Pattern Recognition, arXiv: 2004.00543, 2020 (Accessed on August 10th, 2026).

[124] B. Nassi, Y. Mirsky, D. Nassi, R. Ben-Netanel, O. Drokin, and Y. Elovici. “Phantom of the ADAS: Securing Advanced Driver-Assistance Systems from Split-Second Phantom Attacks”. In Proceedings of the 2020 ACM SIGSAC Conferenceon Computer and Communications Security, pp. 293–308, doi: 10.1145/3372297.3423359, ACM, 2020.

[125] M. Safarzadehvahed and M. Zulkernine. “DSADA: Detecting Spoofing Attacks in Driver Assistance Systems using Objects’ Spatial Shapes”. ACM Transactionson Autonomous and Adaptive Systems, doi: 10.1145/3716139, ACM, 2025.

[126] Y. Man, R. Muller, M. Li, Z. B. Celik, and R. Gerdes. “That Person Moves Like a Car: Misclassification Attack Detection for Autonomous Systems using Spatiotemporal Consistency”. In 32nd USENIX Security Symposium (USENIX Security 23), no. 388, pp. 6929–6946, ACM, 2023.

[127] M. Safarzadehvahed, M. Zulkernine, P. R. M. de Araujo, and S. Givigi. “IPRPAS: A Dataset of Physical Adversarial Samples for Assessing Object Detection in Intelligent Vehicles”. IEEE Internet of Things Journal, vol. 12, no. 12, pp. 21255–21263, doi: 10.1109/JIOT.2025.3550048, IEEE, 2025.

[128] A. Guesmi and M. Shafique. “Navigating Threats: A Survey of Physical Adversarial Attacks on LiDAR Perception Systems in Autonomous Vehicles”. Computer Vision and Pattern Recognition, arXiv: 2409.20426, 2024 (Accessed on August 10th, 2026).

[129] T. B. Brown, D. Mané, A. Roy, M. Abadi, and J. Gilmer. “Adversarial patch”. Computer Vision and Pattern Recognition, arXiv: 1712.09665, 2018 (Accessed on August 10th, 2026).

[130] Z. Wang, H. Wei, J. Wang, X. Zeng, and Y. Chang. “Security Issues and Solutions for Connected and Autonomous Vehicles in a Sustainable City: A Survey”. In Sustainability, vol. 14, no. 9, doi: 10.3390/su141912409, MDPI, 2022.

[131] B. Yang, X. Ji, Z. Jin, Y. Cheng, and W. Xu. “Exploring Adversarial Robustness of LiDAR-Camera Fusion Model in Autonomous Driving”. Robotics, arXiv: 2312.01468, 2024 (Accessed on August 10th, 2026).

[132] A. A. Mehta, A. A. Padaria, D. J. Bavisi, V. Ukani, P. Thakkar, R. Geddam . ”Securing the Future: A Comprehensive Review of Security Challenges and Solutions in Advanced Driver Assistance Systems,” in IEEE Access, vol. 12, pp. 643-678, doi: 10.1109/ACCESS.2023.3347200, IEEE, 2024.

[133] J. M. Qurashi, M. J. Ikram, K. Jambi, F. E. Eassa, and M. Khemakhem, “Autonomous Vehicles: Security Challenges and Game theory-based Countermeasures,” in Proceedings of the 1st International Conference on Advanced Innovations in Smart Cities (ICAISC), pp. 1–6, doi: 10.1109/ICAISC56366.2023.10085301, IEEE, 2023.

[134] A. Chernikova, A. Oprea, C. Nita-Rotaru and B. Kim, “Are Self-Driving Cars Secure? Evasion Attacks Against Deep Neural Networks for Steering Angle Prediction,” 2019 IEEE Security and Privacy Workshops (SPW), pp. 132-137, doi: 10.1109/SPW.2019.00033, IEEE, 2019.

[135] D. Bogdoll, M. Nitsche and J. M. Zöllner, “Anomaly Detection in Autonomous Driving: A Survey,” 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), pp. 4487-4498, doi: 10.1109/CVPRW56347.2022.00495, IEEE, 2022.

[136] M. Berk, O. Schubert, H.-M. Kroll, B. Buschardt, and D. Straub, “Exploiting Redundancy for Reliability Analysis of Sensor Perception in Automated Driving Vehicles,” IEEE Transactions on Intelligent Transportation Systems, vol. 21, no. 12, pp. 5073–5085, doi: 10.1109/TITS.2019.2948394, IEEE, 2020.

[137] Y. Wang, Q. Liu, E. Mihankhah, C. Lv, and D. Wang, “Detection and Isolation of Sensor Attacks for Autonomous Vehicles: Framework, Algorithms, and Validation,” IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 7, pp. 8247–8259, doi: 10.1109/TITS.2021.3077015, IEEE, 2022.

[138] A. Geiger, P. Lenz, and R. Urtasun. “Are We Ready for Autonomous Driving? The KITTI Vision Benchmark Suite”. In IEEE Conference on Computer Visionand Pattern Recognition (CVPR), pp. 3354-3361, doi: 10.1109/CVPR.2012.6248074, IEEE, 2012.

[139] F. Yu, H. Chen, X. Wang, W. Xian, Y. Chen, F. Liu, V. Madhavan, and T. Darrell. “BDD100K: A diverse driving dataset for heterogeneous multitask learning”. In IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), pp. 2633-2642, doi: 10.1109/CVPR42600.2020.00271, IEEE, 2020.

[140] H. Caesar, V. Bankiti, A. H. Lang, S. Vora, V. E. Liong, Q. Xu, A. Krishnan,Y. Pan, G. Baldan, and O. Beijbom. “nuScenes: A Multimodal

Dataset for Autonomous Driving". In IEEE/CVF Conference on Computer Vision andPattern Recognition (CVPR), pp. 11618-11628, doi: 10.1109/CVPR42600.2020.01164, IEEE, 2020.

[141] B. Hurl, K. Czarnecki and S. Waslander, "Precise Synthetic Image and LiDAR (PreSIL) Dataset for Autonomous Vehicle Perception," 2019 IEEE Intelligent Vehicles Symposium (IV), pp. 2522-2529, doi: 10.1109/IVS.2019.8813809, IEEE, 2019.

[142] M. Angus, M. ElBalkini, S. Khan, A. Harakeh, O. Andrienko,C. Reading, S. L. Waslander, and K. Czarnecki, "Unlimited Road-Scene Synthetic Annotation (URSA) Dataset". Computer Science: Computer Vision and Pattern Recognition, ArXiv: 1807.06056, 2018 (Accessed on August 10th, 2026).

[143] M. Martinez, C. Sitawarin, K. Finch, L. Meincke, A. Yablonski, and A. L. Kornhauser, "Beyond grand theft auto V for training,testing and enhancing deep learning in self driving cars," Computer Science: Computer Vision and Pattern Recognition, ArXiv: 1712.01397, 2017 (Accessed on August 10th, 2026).

[144] K. Lounis, S. H. H. Ding and M. Zulkernine, "D2D-MAP: A Drone to Drone Authentication Protocol Using Physical Unclonable Functions," in IEEE Transactions on Vehicular Technology, vol. 72, no. 4, pp. 5079-5093, doi: 10.1109/TVT.2022.3224611, IEEE, 2023.

[145] K. Lounis and M. Zulkernine, "T2T-MAP: A PUF-Based Thing-to-Thing Mutual Authentication Protocol for IoT," in IEEE Access, vol. 9, pp. 137384-137405, doi: 10.1109/ACCESS.2021.3117444, IEEE, 2021.

[146] K. Lounis and M. Zulkernine, "Lessons Learned: Analysis of PUF-based Authentication Protocols for IoT" in Digital Threats: Research and Practice, vol. 4, Iss. 2, no. 19, pp. 1 - 33, doi: 10.1145/3487060, ACM, 2022.

[147] K. Lounis. "More Lessons: Analysis of PUF-based Authentication Protocols for IoT", in Cryptology ePrint Archive, 2021/1509, 2021.

[148] H. Kim and S. Jeon, "Multi-Factor Authentication for In-Vehicle Secure OTA Protocol," in IEEE Access, vol. 13, pp. 208626-208641, doi: 10.1109/ACCESS.2025.3641178, IEEE, 2025.

[149] A. Ghosal, S. Halder and M. Conti, "STRIDE: Scalable and Secure Over-The-Air Software Update Scheme for Autonomous Vehicles," ICC 2020 - 2020 IEEE International Conference on Communications (ICC), pp. 1-6, doi: 10.1109/ICC40277.2020.9148649, IEEE, 2020.

[150] S. Halder, A. Ghosal, and M. Conti, "Secure over-the-air software updates in connected vehicles: A survey," Computer Network, vol. 178, no. 107343, doi: 10.1016/j.comnet.2020.107343, Elsevier, 2020.

[151] M. Steger, M. Karner, J. Hillebrand, W. Rom, C. Boano and K. Römer, "Generic framework enabling secure and efficient automotive wireless SW updates," 2016 IEEE 21st International Conference on Emerging Technologies and Factory Automation (ETFA), pp. 1-8, doi: 10.1109/ETFA.2016.7733575, IEEE, 2016.

[152] M. Steger et al., "An Efficient and Secure Automotive Wireless Software Update Framework," in IEEE Transactions on Industrial Informatics, vol. 14, no. 5, pp. 2181-2193, doi: 10.1109/TII.2017.2776250, IEEE, 2018.

[153] D. Mbakoyiannis, O. Tomoutzoglou, and G. Kornaros, "Secure over-the-air firmware updating for automotive electronic control units," in Procceedings of the 34th ACM/SIGAPP Symposium on Applied Computing, pp. 174–181, doi: 10.1145/3297280.329729, ACM, 2019.

[154] S. S. Raghavan, "Blockchain-based framework for secure OTA updates in autonomous vehicles". International Journal of Scientific Research & Engineering Trends, vol. 8, no. 6, pp. 2409-2417, ISSN: 2395-566X, 2022.

[155] D. K. Nilsson, U. E. Larson and E. Jonsson, "Efficient In-Vehicle Delayed Data Authentication Based on Compound Message Authentication Codes," 2008 IEEE 68th Vehicular Technology Conference, pp. 1-5, doi: 10.1109/VETECF.2008.259, IEEE, 2008.

[156] M. L. Chavez, C. H. Rosete and F. R. Henriquez, "Achieving confidentiality security service for CAN," 15th International Conference on Electronics, Communications and Computers (CONIELECOMP'05), pp. 166-170, doi: 10.1109/CONIEL.2005.13, IEEE, 2005.

[157] H. Oguma, A. Yoshioka, M. Nishikawa, R. Shigetomi, A. Otsuka and H. Imai, "New Attestation Based Security Architecture for In-Vehicle Communication," IEEE GLOBECOM 2008 - 2008 IEEE Global Telecommunications Conference, pp. 1-6, doi: 10.1109/GLOCOM.2008.ECP.369, IEEE, 2008.

[158] A. Groll and C. Ruland, "Secure and authentic communication on existing in-vehicle networks," 2009 IEEE Intelligent Vehicles Symposium, pp. 1093-1097, doi: 10.1109/IVS.2009.5164434, IEEE, 2009.

[159] S. Fassak, Y. El Hajjaji El Idrissi, N. Zahid and M. Jedra, "A secure protocol for session keys establishment between ECUs in the CAN bus," 2017 International Conference on Wireless Networks and Mobile Communications (WINCOM), pp. 1-6, doi: 10.1109/WINCOM.2017.8238149, IEEE, 2017.

[160] O. Agbo, M. Hefeida and A. S. El-Wakeel, "Hybrid-CNN Intrusion Detection Framework for CAN Networks in Connected and Autonomous Vehicles," in IEEE Internet of Things Journal, vol. 12, no. 17, pp. 36353-36369, doi: 10.1109/JIOT.2025.3582118, IEEE, 2025.

[161] S. Mirsattarian, M. Kargahi and V. Panahi, "Secure Communication on CAN-Bus Using Sporadic Authenticated Encryption," 2024 5th CPSSI International Symposium on Cyber-Physical Systems (Applications and Theory) (CPSAT), pp. 1-8, doi: 10.1109/CPSAT64082.2024.10745422, IEEE, 2024.

[162] J. Cui et al., "Lightweight Encryption and Authentication for Controller Area Network of Autonomous Vehicles," in IEEE Transactions on Vehicular Technology, vol. 72, no. 11, pp. 14756-14770, doi: 10.1109/TVT.2023.3281276, IEEE, 2023.

[163] F. Páez and H. Kaschel, "A Proposal for Data Authentication, Data Integrity and Replay Attack Rejection for the LIN Bus," 2021 IEEE CHILEAN Conference on Electrical, Electronics Engineering, Information and Communication Technologies (CHILECON), pp. 1-7, doi: 10.1109/CHILECON54041.2021.9702979, IEEE, 2021.

[164] F. Paez and H. Kaschel, "Towards a Robust Computer Security Layer for the LIN Bus," 2021 IEEE International Conference on Automation/XXIV Congress of the Chilean Association of Automatic Control (ICA-ACCA), pp. 1-8, doi: 10.1109/ICAACCA51523.2021.9465340, IEEE, 2021.

[165] N. Bagga, S. Kalra and P. Kaur, "Attacks on Flex-Ray Protocol by Altering the Timestamp Configuration of the Network," 2025 International Conference on Networks and Cryptology (NETCRYPT), pp. 1235-1237, doi: 10.1109/NETCRYPT65877.2025.11102798, IEEE, 2025.

[166] M. J and K. C, "Smart vehicle monitoring for detecting anomalies on CAN bus," 2021 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), pp. 1-6, doi: 10.1109/CONECCT52877.2021.9622628, IEEE, 2021.

[167] Y. S. Santawani and N. B. Chopade, "A Comprehensive Survey of Cyber Attacks & Intrusion Detection Techniques for Securing Automotive Systems," 2026 International Conference on Emerging Technologies and Future Innovations (ETFI), pp. 1-3, doi: 10.1109/ETFI68128.2026.11484102, IEEE, 2026.

[168] K. Agrawal, T. Alladi, A. Agrawal, V. Chamola and A. Benslimane, "NovelADS: A Novel Anomaly Detection System for Intra-Vehicular Networks," in IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 11, pp. 22596-22606, doi: 10.1109/TITS.2022.3146024, IEEE, 2022.

[169] C. Dong, H. Wu and Q. Li, "Multiple Observation HMM-Based CAN Bus Intrusion Detection System for In-Vehicle Network," in IEEE Access, vol. 11, pp. 35639-35648, doi: 10.1109/ACCESS.2023.3265018, IEEE, 2023.

[170] P. Wei, B. Wang, X. Dai, L. Li, and F.He. "A novel intrusion detection model for the CAN bus packet of in-vehicle network based on attention mechanism and autoencoder". Digital Communications and Networks, vol. 9, no. 1, pp. 14-21, doi: 10.1016/j.dcan.2022.04.021, KEAI Publishing ltd, 2023.

[171] A. Castiglione, T. Elia, C. carmine Esposito, and F. Cirillo. "Lightweight Cryptography and Physically Unclonable Functions for Secure In-Vehicle Communications". In Proceedings of the International Conference on Research in Adaptive and Convergent Systems (RACS '25), no 32, pp. 1–8, doi:10.1145/3769002.3769963, ACM, 2025.

[172] E. Aliwa, O. Rana, C. Perera, and P. Burnap. "Cyberattacks and Countermeasures for In-Vehicle Networks". ACM Computing Survey, vol. 54, no. 1, pp. 1–37, doi: 10.1145/343123, ACM, 2021.

[173] K. Iehira, H. Inoue and K. Ishida, "Spoofing attack using bus-off attacks against a specific ECU of the CAN bus," 2018 15th IEEE Annual Consumer Communications & Networking Conference (CCNC), pp. 1-4, doi: 10.1109/CCNC.2018.8319180, IEEE, 2018.

[174] M. S. U. Alam, S. Iqbal, M. Zulkernine and C. Liem, "Securing Vehicle ECU Communications and Stored Data," ICC 2019 - 2019 IEEE International Conference on Communications (ICC), pp. 1-6, doi: 10.1109/ICC.2019.8762043, IEEE, 2019.

[175] X. Hu et al., "A Lightweight and Confidential Communication Scheme for On-Vehicle ECUs," in IEEE Network, vol. 38, no. 3, pp. 34-40,, doi: 10.1109/MNET.2024.3365946, IEEE, 2024.

[176] Y. Zhang, B. Ge, X. Li, B. Shi and B. Li, "Controlling a Car Through OBD Injection," 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud), pp. 26-29, doi: 10.1109/CSCloud.2016.42, IEEE, 2016.

[177] R. Xie, P. Xiang, J. Duan and X. Wang, "A Tamper-Resistant Two-Way Authentication Method for On-Board Diagnostics (OBD) Devices," 2026 5th International Conference on Electronics, Integrated Circuits and Communication Technology (EICCT), pp. 1111-1116, doi: 10.1109/EICCT69950.2026.11564512, IEEE, 2026.

[178] T. U. Kang, H. M. Song, S. Jeong and H. K. Kim, "Automated Reverse Engineering and Attack for CAN Using OBD-II," 2018 IEEE 88th Vehicular Technology Conference (VTC-Fall), pp. 1-7, doi: 10.1109/VTCFall.2018.8690781, IEEE, 2018.

[179] S. Y. P, A. Gotkhindikar and S. K. Tiwari, "Survey on CAN-Bus Packet Filtering Firewall," 2022 International Conference on Edge Computing and Applications (ICECAA), pp. 472-478, doi: 10.1109/ICECAA55415.2022.9936152, IEEE, 2022.

[180] S. Rizvi, J. Willett, D. Perino, T. Vasbinder, and S. Marasco. "Protecting an automobile network using distributed firewall system". In Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing (ICC '17). no. 174, pp. 1–6, doi: 10.1145/3018896.3056791, ACM, 2017.

[181] D. K. Oka and P. Jungklass. "Secure Boot in Automotive Real-Time Systems in Context of Post-Quantum Cryptography". In Proceedings of the 2nd Cyber Security in CarS Workshop (CSCS '25), no. 3, pp. 1–7, doi: 10.1145/3736130.3764513, ACM, 2025.

[182] J. W. Bos, M. Löhr, A. Sadeghi, and M. Winandy. "Post-Quantum Secure Boot on Vehicle Network Processors". IACR: Cryptology ePrint Arive, 2022/635, 2022 (Accessed on August 10th, 2026).

[183] S. Sanwald, L. Kaneti, M. Stöttinger, M. Böhner, "Secure Boot Revisited: Challenges for Secure Implementations in the Automotive Domain". SAE International Journal of Transportation Cybersecurity and Privacy, vol. 2, no. 2, pp. 69-81, doi: 10.4271/11-02-02-0008, 2019.

[184] C. Wang, C. Dong, Y. Li and R. Zhao, "Research on the System of Hardware Security Protection Module of Automobile Chips Based on HSM Vehicle Network," 2024 IEEE 7th International Conference on Automation, Electronics and Electrical Engineering (AUTEEE), pp. 719-724, doi: 10.1109/AUTEEE62881.2024.10869662, IEEE, 2024.

[185] M. El-Said, "ECU Counterfeit Mitigation Using Holistic Approach in Modern Automotive Echo System," 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), pp. 1-2, doi: 10.1109/CCNC46108.2020.9045510, IEEE, 2020.

[186] A. Maruaisap and P. Kumhom, "A hardware-based security scheme for in-vehicle CAN," 2016 International Computer Science and Engineering Conference (ICSEC), pp. 1-5, doi: 10.1109/ICSEC.2016.7859891, IEEE, 2016.

[187] C. Labrado and H. Thapliyal, "Hardware Security Primitives for Vehicles," in IEEE Consumer Electronics Magazine, vol. 8, no. 6, pp. 99-103, doi: 10.1109/MCE.2019.2941392, IEEE, 2019.

[188] N. Ilg, D. Germek, P. Duplys and M. Menth, "Work-in-Progress: Emerging E/E-Architectures as Enabler for Automotive Honeypots," 2024 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), pp. 361-366, doi: 10.1109/EuroSPW61312.2024.00046, IEEE, 2024.

[189] V. Verendel, D. K. Nilsson, U. E. Larson and E. Jonsson, "An Approach to using Honeypots in In-Vehicle Networks," 2008 IEEE 68th Vehicular Technology Conference, pp. 1-5, doi: 10.1109/VETECF.2008.260, IEEE, 2008.

[190] E. Eriksson and L. Fahlbeck, "Investigating the Use of Honeypots in Vehicles," Master's thesis Chalmers University of Technology and University of Gothenburg, 2022.

[191] . Li, P. Liu, Q. Zhang and T. Liu, "How to Better Cope with New Automotive Security Risks: VSOC Empowered by Threat Intelligence," 2024 4th International Conference on Control Theory and Applications (ICoCTA), pp. 310-314, doi: 10.1109/ICoCTA64736.2024.00066, IEEE, 2024.

[192] A. M. Nasser, D. Ma, and P. Muralidharan, "An Approach for Building Security Resilience in AUTOSAR Based Safety Critical Systems", Journal of Cyber Security and Mobility, vol. 6, no. 3, pp. 271–304, doi: 10.13052/2245-1439.633, River Publishers, 2017.

[193] D. Reinhardt and M. Kucera, "Domain Controlled Architecture - A New Approach for Large Scale Software Integrated Automotive Systems," in the International Conference on Pervasive and Embedded Computing and Communication Systems, vol. 13, pp. 221–226, doi: 10.5220/0004340702210226, 2013.

[194] X. Li, N. Zhang, X. Xu, A. -T. Nguyen, K. Al-Haddad and H. Zhang, "Attack-Resilient Event-Triggered Control of Vehicle Speed Tracking System With DoS Attacks: Experimental Results," in IEEE Transactions on Consumer Electronics, vol. 70, no. 3, pp. 5079-5089, doi: 10.1109/TCE.2024.3410536, IEEE, 2024.

[195] A. Tashiro, H. Muraoka, S. Araki, K. Kakizaki and S. Uehara, "A secure protocol consisting of two different security-level message authentications over CAN," 2017 3rd IEEE International Conference on Computer and Communications (ICCC), pp. 1520-1524, doi: 10.1109/CompComm.2017.8322794, IEEE, 2017.

[196] B. Groza, "LiBrA-CAN: Lightweight broadcast authentication for controller area networks", ACM Transactions on Embedded Computing Systems, vol. 16, no. 3, pp. 1–28, doi: 10.1145/305650, ACM, 2017.

[197] B. Groza, L. Popa and P. -S. Murvay, "Highly Efficient Authentication for CAN by Identifier Reallocation With Ordered CMACs," in IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 6129-6140, doi: 10.1109/TVT.2020.2990954, IEEE, 2020.

[198] A. J. Michaels, V. S. S. Palukuru, M. J. Fletcher, C. Henshaw, S. Williams, and T. Krauss. "CAN Bus Message Authentication via Co-Channel RF Watermark," in IEEE Transactions on Vehicular Technology, vol. 71, no. 4, pp. 3670-3686, doi: 10.1109/TVT.2022.3143708, IEEE, 2022.

[199] S. A. A. Hridoy and M. Zulkernine, "LaaCan: A Lightweight Authentication Architecture for Vehicle Controller Area Network" in the Proceedings of the 2020 Security and Privacy in Communication Networks (SecureComm 2020), vol. 336, pp. 215-234, doi: 10.1007/978-3-030-63095-9_12, Springer, 2020.

[200] W. Stallings, "Cryptography and Network Security: Principles and Practice (Instructor's Manual)". Upper Saddle River, NJ, USA: Prentice-Hall, 1998.

[201] S. T. Kent, "Encryption-based Protection for Interactive User/Computer Communication," in Proceedings of the 5th Symposium on Data Communcations (SIGCOMM), vol. 5, pp. 7–13, doi: 10.1145/800103.8033, ACM, 1977.

[202] R. McNamara, "Networks—Where does the real threat lie?" Information Security Technical Report, vol. 3, no. 4, pp. 65–74, DOI: 10.1016/s1363-4127(98)80039-3, 1998.

[203] J. McHugh, "The 1998 Lincoln Laboratory IDS Evaluation," in Recent Advances in Intrusion Detection, vol. 1907, pp. 145–161, doi: 10.1007/3-540-39945-3_10, Springer, 2000.

[204] AUTOSAR. (2024). "Specification of Secure Onboard Communication (SecOC)" Document ID 654. AUTOSAR Classic Platform Specifications. https://www.autosar.org. (Accessed on August 10th, 2026)

[205] Simma Software, Inc.,"UDS Security Access (0x27) vs. Authentication (0x29)", https://simmasoftware.com/uds-security-access-authentication/, 2026. (Accessed on August 10th, 2026)

[206] Cybersecurity and Infrastructure Security Agency (CISA), "Microsegmentation in Zero Trust, Part One: Introduction and Planning," CISA Technical Guidance Ver. 1.0, Jul. 29, 2025. [Online]. Available: https://www.cisa.gov/sites/default/files/2025-07/ZT-Microsegmentation-Guidance-Part-One_508c.pdf (Accessed on August 10th, 2026)

[207] J. B. Kristoffersson, "Zero Trust in Autonomous Vehicle Networks Utilizing Automotive Ethernet," M.S. thesis, Dept. Comput. Sci. Eng., Chalmers Univ. Technol., Gothenburg, Sweden, 2022.

[208] K. Lounis. "Cut It: Deauthentication Attack on Bluetooth,". In the Proceedings of the 14th International Conference on Security of Information and Networks (SIN'21), pp. 1-8, doi: 10.1109/SIN54109.2021.9699265, IEEE, 2021.

[209] K. Lounis and M. Zulkernine. "Bluetooth Low Energy Makes Just Works Not Work". In the 3rd Cyber Security and Networking Conference (CSNet'19), pp. 99-106, doi: 10.1109/CSNet47905.2019.9108931, IEEE, 2019.

[210] K. Lounis and M. Zulkernine. "Connection Dumping Vulnerability Affecting Bluetooth Availability," In the Proceedings of the 13th International Conference on Risks and Security of Internet and Systems (CRiSIS'18), pp. 188-204, doi: 10.1007/978-3-030-12143-3_16, Springer, 2018.

[211] K. Lounis and M. Zulkernine. "Attacks and Defenses in Short-Range Wireless Technologies for IoT". In IEEE Access, vol. 8, pp. 88892 - 88932, doi: 10.1109/ACCESS.2020.2993553, IEEE, 2020.

[212] K. Lounis, S. H. H. Ding, and M. Zulkernine. "Cut It: Deauthentication Attacks on Protected Management Frames in WPA2 and WPA3". In

the 14th International Symposium on the Foundations of Security and Practices (FPS'21), doi: 10.1007/978-3-031-08147-7_16, Springer, 2021.
[213] K. Lounis and M. Zulkernine. "Exploiting Race-Condition for Wi-Fi Denial of Service Attacks". In the 13th International Conference on Security of Information and Networks (SIN'20), no.2, pp. 1-8, 10.1145/3433174.34335, ACM, 2020.
[214] K. Lounis and M. Zulkernine. "Bad-Token: Denial of Service Attacks on WPA3". In the 12th International Conference on Security of Information and Networks (SIN'19), no. 15, pages 1-8, 10.1145/3357613.3357629, ACM, 2019.
[215] K. Lounis and M. Zulkernine. "WPA3 Connection Deprivation Attacks". In the 14th International Conference on Risks and Security of Internet and Systems (CRiSIS'19), pp. 164-176, doi: 10.1007/978-3-030-41568-6_11, Springer, 2019.
[216] K. Lounis. "Wi-Fi Security: Do We Still Have to Look Back?", Cryptology ePrint Archive, 2022/1764, 2022.
[217] M. Lichtman, R. P. Jover, M. Labib, R. Rao, V. Marojevic and J. H. Reed, "LTE/LTE-A jamming, spoofing, and sniffing: threat assessment and mitigation," in IEEE Communications Magazine, vol. 54, no. 4, pp. 54-61, doi: 10.1109/MCOM.2016.7452266, IEEE, 2016.
[218] M. Khan, P. Ginzboorg, K. Järvinen, and V. Niemi. "Defeating the Downgrade Attack on Identity Privacy in 5G," in Security Standardisation Research (SSR 2018), Lecture Notes in Computer Science, vol. 11322, doi: 10.1007/978-3-030-04762-7_6, Springer, 2018.
[219] A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani, and E. Weippl. "IMSI-catch me if you can: IMSI-catcher-catchers". In Proceedings of the 30th Annual Computer Security Applications Conference (ACSAC '14), pp. 246–255, doi: 10.1145/2664243.2664272, ACM, 2014.
[220] I. Palamà, F. Gringoli, G. Bianchi, and N. B. Melazzi. "The Diverse and Variegated Reactions of Different Cellular Devices to IMSI Catching Attacks". In Proceedings of the 14th International Workshop on Wireless Network Testbeds, Experimental evaluation & Characterization (WiNTECH '20), pp. 80–86, doi: 10.1145/3411276.3412191, ACM, 2020.
[221] K. Tindell. "CAN Injection: Keyless Car Theft," in CTO of Canis Automotive Labs, https://kentindell.github.io/2023/04/03/can-injection/, 2022 (Accessed on August 10th, 2026).
[222] RTL-SDR.COM. "Flipper Zero DarkWeb Firmware Bypasses Rolling Code Security", RTL-SDR (RTL2832U) and software defined radio news and projects, https://www.rtl-sdr.com/flipperzero-darkweb-firmware-bypasses-rolling-code-security/, 2025 (Accessed on August 10th, 2026).
[223] A. Eslami and J. Yu. "Security Risks of Agentic Vehicles: A Systematic Analysis of Cognitive and Cross-Layer Threats", Artificial Intelligence, arXiv: 2512.17041, 2025 (Accessed on August 10th, 2026).
[224] A. Polamarasetti, V. Yammanur, N. Ravuri, V. V. R. M. Bokka, and R. Vadisetty, "Agentic ai-driven cybersecurity for cloud-connected automotive systems," in International Conference on IntelligenceBased Transformations of Technology and Business Trends, pp. 697–707, doi: 10.1007/978-3-032-07373-0_53, Springer, 2025.
[225] M. Burgess. "A Cyberattack on Jaguar Land Rover Is Causing a Supply Chain Disaster", https://www.wired.com/story/jlr-jaguar-land-rover-cyberattack-supply-chain-disaster/, Wired, Security section, 2025 (Accessed on August 10th, 2026).
[226] OpenPR. "Automotive Cybersecurity News Q1 2026 - Vehicle Vulnerabilities Double Year-on-Year And Hackers "Brick" Thousands of Cars", in Logistics & Transport, ABNewswire Press release, https://www.openpr.com/news/4540807/automotive-cybersecurity-news-q1-2026-vehicle, 2026 (Accessed on August 10th, 2026).
[227] Uawire. "Anti-drone jammers across Russia are immobilizing BMW and Porsche vehicles, reports say" https://www.uawire.org/anti-drone-jammers-across-russia-are-immobilizing-bmw-and-porsche-vehicles-reports-say, 2026 (Accessed on August 10th, 2026).