**Cybersecurity Risks and Mitigation Strategies for Connected and Autonomous Vehicles: A Business Imperative for the Automotive Sector**

**Executive Summary**

The advent of Connected and Autonomous Vehicles (CAVs) heralds a transformative era for transportation, promising enhanced safety, efficiency, and novel mobility services. However, this evolution is intrinsically linked to an escalating and increasingly complex cybersecurity threat landscape. The heightened connectivity of CAVs—encompassing Vehicle-to-Everything (V2X) communication, cloud services, and sophisticated in-vehicle networks—combined with the millions of lines of code and hundreds of Electronic Control Units (ECUs) that govern their operation, has dramatically expanded the potential attack surface.1 This report provides a comprehensive analysis of these evolving cybersecurity risks, their profound implications for safety and data integrity, and the critical mitigation strategies, standards, and business practices essential for the automotive sector.

The threat landscape is characterized by diverse vulnerabilities across all CAV components, from sensors and ECUs to infotainment systems and the underlying communication infrastructure. Attack vectors range from remote exploits targeting software and APIs to physical intrusions and supply chain compromises, with real-world incidents demonstrating capabilities to control vehicle functions, steal sensitive data, and cause widespread operational disruption.2 The consequences of such breaches are severe, extending beyond direct financial losses—which can run into billions of dollars—to encompass catastrophic safety failures, erosion of consumer trust, significant legal liabilities, and substantial reputational damage.4 In the context of CAVs, cybersecurity is inextricably linked to functional safety; a cyberattack is not merely an IT issue but a direct threat to human lives.

Addressing these challenges necessitates a multi-layered, lifecycle approach to cybersecurity, beginning with "Security-by-Design" principles embedded from the initial concept phase through to vehicle decommissioning.8 Key technical mitigation strategies include robust encryption, comprehensive authentication mechanisms (such as Public Key Infrastructure), network segmentation, advanced Intrusion Detection and Prevention Systems (IDS/IPS) often leveraging Artificial Intelligence (AI), Hardware Security Modules (HSMs), secure software development practices, and rigorously protected Over-the-Air (OTA) update mechanisms.5

The automotive industry is increasingly guided by standards and regulations such as ISO/SAE 21434, UNECE WP.29 R155 (Cybersecurity Management System), and R156 (Software Update Management System), which mandate comprehensive risk management processes and cybersecurity engineering practices.13 However, a critical challenge identified is the "Automotive Cyber Gap"—the disconnect between achieving regulatory compliance and establishing true, adaptive resilience against sophisticated and evolving threats.3 Bridging this gap requires moving beyond a compliance-centric mindset to foster a culture of continuous security improvement, driven by threat intelligence and proactive vulnerability management.

Ultimately, robust cybersecurity is not merely a defensive necessity but a core business imperative and a potential competitive differentiator for the automotive sector.16 Investment in comprehensive cybersecurity strategies protects against financial and reputational losses, ensures regulatory compliance, builds consumer trust crucial for the adoption of new technologies like autonomous driving, and enables the safe deployment of innovative connected services. This report calls for concerted action from all industry stakeholders—OEMs, suppliers, regulators, and technology providers—to collaboratively strengthen the cybersecurity posture of CAVs, thereby safeguarding the future of mobility.

**I. The Evolving Threat Landscape for Connected and Autonomous Vehicles**

The progression towards increasingly connected and autonomous vehicles (CAVs) signifies a paradigm shift in transportation, offering unprecedented advancements in safety, efficiency, and user experience. However, this increased sophistication brings with it a substantially magnified and dynamically evolving cybersecurity threat landscape. The intricate web of technologies underpinning CAVs creates a complex ecosystem ripe for exploitation by malicious actors, demanding a thorough understanding of the inherent vulnerabilities.

**A. The Expanding Attack Surface: Increased Connectivity and Complexity**

The fundamental challenge in securing CAVs lies in their vastly expanded attack surface, a direct consequence of their enhanced connectivity and inherent architectural complexity. Modern vehicles are no longer isolated mechanical systems but are rapidly transforming into sophisticated, software-defined platforms, often described as "IoT ecosystems on wheels".1

1. **CAV Architecture Overview: Key Components (ECUs, Sensors, IVI, In-Vehicle Networks, V2X, Cloud Services)**  
   Connected and Autonomous Vehicles (CAVs) are characterized by their integration of advanced communication and autonomous driving technologies, enabling them to operate with varying degrees of independence from human intervention.17 The architecture of a typical CAV is a complex amalgamation of hardware and software components, each contributing to the vehicle's functionality and, consequently, to its potential vulnerabilities.  
   At the core of a CAV's operation are numerous **Electronic Control Units (ECUs)**. A modern high-end vehicle can contain over 100 ECUs, collectively running on potentially 150 million lines of code, a figure projected to exceed 600 million lines of code by 2025.1 These ECUs govern a wide array of functions, from critical operations like engine management, braking, and steering, to comfort and convenience features. The sheer volume and diversity of these ECUs, often sourced from multiple suppliers, inherently increase the likelihood of software flaws and security loopholes.1 This architectural complexity, driven by the multitude of interconnected ECUs and massive codebases, inherently creates a vast and difficult-to-secure attack surface. Each ECU, communication channel, and line of code represents a potential entry point or a weak link in the security chain, making comprehensive security management an immense challenge.  
   To achieve autonomy, CAVs rely on a sophisticated suite of **sensors** to perceive their environment. These include LiDAR (Light Detection and Ranging), radar, high-resolution cameras, Global Positioning System (GPS), and ultrasonic sensors.1 These sensors generate vast amounts of data, which are processed by advanced data analytics and, increasingly, Artificial Intelligence (AI) and Machine Learning (ML) algorithms to build a dynamic representation of the vehicle's surroundings and inform driving decisions.1  
   **In-Vehicle Infotainment (IVI) systems** provide entertainment, navigation, and connectivity features to occupants. While enhancing user experience, IVI systems often connect to external networks via Wi-Fi, Bluetooth, and cellular modems, and may run third-party applications, making them a significant entry point for cyber threats.17  
   Communication between ECUs occurs over **in-vehicle networks**. The Controller Area Network (CAN) bus is a prevalent standard, but protocols like FlexRay and Automotive Ethernet are also used.21 While designed for reliability and real-time performance, many legacy in-vehicle networking protocols, particularly CAN, lack robust, built-in security features.2  
   A defining characteristic of CAVs is **Vehicle-to-Everything (V2X) communication**. This technology enables vehicles to exchange information with other vehicles (V2V), roadside infrastructure (V2I), pedestrians (V2P), and the wider network/cloud (V2N).10 V2X is crucial for enhancing situational awareness, traffic efficiency, and safety, but it also exposes vehicles to a host of remote threats over wireless channels.1  
   Finally, CAVs are increasingly reliant on **cloud services** for a variety of functions, including Over-the-Air (OTA) software updates, telematics, remote diagnostics, data storage and processing for autonomous driving algorithms, and fleet management.1 This dependency introduces vulnerabilities associated with cloud security, data transmission, and the integrity of software updates.  
   The convergence of these distinct technologies—those enabling connectivity and those enabling autonomy—within a single CAV platform exponentially increases the security challenges.1 Vulnerabilities in connectivity features can be exploited to compromise autonomous driving functions, and vice versa. For example, a breach through an internet-connected IVI system could potentially provide an attacker with a pathway to manipulate critical driving controls if network segmentation is inadequate. This interplay necessitates a holistic security approach that addresses the entire CAV ecosystem, rather than treating connectivity and autonomy in isolation. The security of CAVs is becoming an increasing concern as the technology enabling autonomy and connectivity becomes more complex and intelligent.17
2. **Vulnerabilities by Component:**  
   The expanded attack surface of CAVs translates into a multitude of vulnerabilities distributed across their various components. Each element, from the smallest ECU to the overarching cloud infrastructure, presents potential weaknesses that can be exploited.

* **Electronic Control Units (ECUs) and In-Vehicle Networks (e.g., CAN Bus)**  
  ECUs, the distributed computing nodes of a vehicle, are susceptible to various attacks due to software bugs, firmware vulnerabilities, and insecure development practices.21 Given their interdependence, a compromise in one ECU can potentially cascade and affect the functionality of others. For instance, an attack on an engine control module could lead to the transmission of false data, such as incorrect wheel speed, to the electronic brake control module, potentially causing inappropriate brake activation.21  
  The in-vehicle networks that connect these ECUs, particularly the widely adopted **CAN bus**, represent a significant area of vulnerability. The CAN protocol, in its original design, prioritized reliability and cost-effectiveness over security, resulting in a fundamental lack of built-in authentication and encryption mechanisms.2 This legacy design choice, while understandable for its era, now constitutes a critical vulnerability debt. Attackers who gain access to the CAN bus—whether through physical means like the On-Board Diagnostics (OBD-II) port 2 or remotely by first compromising a connected ECU (e.g., an IVI system or telematics unit)—can exploit these weaknesses. Common attacks on the CAN bus include:
* **Spoofing and Message Injection:** Attackers can transmit counterfeit CAN messages, impersonating legitimate ECUs. Other nodes on the network will accept these forged commands (e.g., "unlock doors," "disable brakes") as genuine because the protocol cannot distinguish fake from real messages.2
* **Eavesdropping (Lack of Confidentiality):** CAN traffic is typically unencrypted, allowing an attacker with access to the bus to intercept and read all data being transmitted, potentially exposing sensitive operational information.2
* **Denial-of-Service (DoS):** A malicious node can flood the bus with high-priority messages, preventing legitimate, lower-priority traffic (which could include safety-critical commands) from getting through. Attackers can also exploit error handling mechanisms to disrupt communication or shut down the bus.2
* **Replay Attacks:** Since CAN messages often lack sequence numbers or freshness checks, an attacker can record legitimate messages (e.g., "brake ON") and replay them later to cause unauthorized or untimely actions.2

Real-world incidents, such as the use of "CAN injection" devices by thieves to bypass security systems and steal vehicles by sending fake authorization messages, underscore the practical implications of these vulnerabilities.2 The proliferation of ECUs in modern CAVs further exacerbates this "weakest link" problem; a vulnerability in a seemingly non-critical ECU, if connected to the CAN bus, can become an entry point to compromise safety-critical vehicle functions.5 While newer network protocols like Automotive Ethernet offer improved security features, the extensive existing deployment of CAN means its vulnerabilities will remain a concern for many years.21

* **Sensors (LiDAR, Radar, Cameras) and Perception Systems**  
  The sensors that enable autonomous driving—LiDAR, radar, cameras, GPS, and ultrasonic sensors—are themselves targets for cyberattacks. These attacks aim to corrupt the vehicle's perception of its environment, leading to flawed decision-making by the autonomous driving system.1 Such sensor attacks represent a unique challenge because they can often bypass traditional network-based cybersecurity defenses by directly manipulating the physical world or the sensor's interpretation of it. Common attack vectors include:
* **Sensor Spoofing:** Attackers can project false data to deceive sensors. For example, infrared light can be used to trick LiDAR systems into detecting non-existent obstacles, or counterfeit GPS signals can be broadcast to misdirect the vehicle.19
* **Sensor Manipulation/Adversarial Attacks:** Physical alterations to the environment, such as placing adversarial stickers on road signs, can confuse camera-based object detection systems, causing misclassification (e.g., a stop sign recognized as a speed limit sign).1 This highlights the vulnerability of AI-based perception systems, where subtle manipulations, sometimes imperceptible to humans, can cause catastrophic failures.
* **Jamming/Denial-of-Service:** Attackers can use radio frequency jamming to disrupt GPS signals or radar, or physically obstruct or blind cameras and LiDAR sensors, effectively creating a denial-of-service condition for the perception system.1
* **Sensor Data Overload:** Flooding sensors with an excessive volume of data or requests can cause them to malfunction or produce inaccurate readings, impairing the vehicle's decision-making capabilities.6

The infamous attack on a Tesla's Mobileye EyeQ3 camera, where manipulated road signage caused the vehicle to misread a speed limit and autonomously accelerate, exemplifies the real-world potential of such attacks.1 Mitigating these threats requires a shift towards sensor fusion (cross-validating data from multiple sensor types) and developing AI models that are robust against adversarial inputs.19

* **In-Vehicle Infotainment (IVI) Systems**  
  IVI systems, with their rich feature sets and extensive connectivity (Wi-Fi, Bluetooth, cellular, USB), often represent a "soft underbelly" for vehicle cybersecurity.17 Prioritized for user experience and third-party application integration, their security measures may be less stringent compared to critical control ECUs, making them attractive initial targets for attackers. Vulnerabilities in IVI systems can lead to:
* **Privacy Invasion:** Attackers can gain access to the vehicle's microphone or GPS data to eavesdrop on conversations or track the vehicle's movements.20
* **Remote Code Execution (RCE):** Flaws in IVI software or connected mobile applications (like Apple CarPlay or Android Auto) can allow attackers to execute arbitrary code on the IVI system.20
* **Pivot to Critical Systems:** If not adequately isolated from other in-vehicle networks, a compromised IVI system can serve as a "stepping stone" for attackers to gain access to more critical vehicle control systems via the CAN bus or other internal networks.5

The "AirBorne" vulnerabilities in Apple CarPlay, stemming from flaws in the AirPlay protocol, demonstrated how buffer overflows could lead to RCE on IVI systems via Wi-Fi or Bluetooth, potentially allowing attackers to manipulate displays, access microphones, or even install persistent malware.20 Similarly, the Subaru Starlink IVI admin panel vulnerability, where publicly accessible scripts and weak authentication allowed researchers to access customer data, view GPS records, and issue remote commands like unlocking doors, highlights the risks associated with the backend infrastructure supporting IVI services.8 The increasing integration of mobile device technologies into IVIs also means that vulnerabilities and attack vectors from the mobile ecosystem are directly imported into the vehicle, significantly expanding the threat landscape.

* **Vehicle-to-Everything (V2X) Communication**  
  V2X communication, encompassing V2V, V2I, V2P, and V2N interactions, is designed to improve road safety and traffic efficiency by enabling real-time information exchange.10 However, this constant communication with external entities introduces significant security challenges due to its distributed, ad-hoc nature and the need for trust between largely unknown parties.23 Key vulnerabilities include:
* **Message Spoofing and False Information:** Attackers can inject false messages (e.g., fake accident warnings, phantom vehicle locations) or manipulate legitimate messages to cause confusion or dangerous actions by other vehicles or infrastructure.10
* **Denial-of-Service (DoS):** V2X communication channels can be flooded with messages or jammed, preventing the transmission of critical safety information.10 Attacks can also target Roadside Units (RSUs) or On-Board Units (OBUs).
* **Data Leakage and Privacy Violations:** Unauthorized access to V2X platforms or weak access controls can lead to the leakage of sensitive data, including location information and personal identifiers.10 Eavesdropping on V2X communications is also a concern.
* **Attacks on Infrastructure:** Compromising RSUs or traffic management centers can allow attackers to manipulate traffic signals or disseminate false information widely.10
* **Sybil Attacks:** An attacker creates multiple fake identities to gain undue influence in the network, spread misinformation, or disrupt consensus mechanisms.21
* **Blackhole/Greyhole Attacks:** Compromised vehicles may selectively drop or refuse to forward V2X messages, hindering the flow of critical information.21

Securing V2X communication heavily relies on robust Public Key Infrastructure (PKI) for authenticating participants and ensuring message integrity and confidentiality through encryption (e.g., using TLS/SSL protocols).10 The potential for compromised V2X communication to have cascading, systemic impacts on traffic flow and safety, affecting multiple vehicles and infrastructure elements simultaneously, makes it a high-value target for large-scale disruption.

* **Automotive Cloud Services and Over-the-Air (OTA) Updates**  
  The reliance of CAVs on cloud services for telematics, data processing, remote operations, and especially OTA software updates introduces another critical attack surface.18 These cloud platforms and the OTA update mechanisms are highly centralized and thus attractive targets for attackers seeking widespread impact across entire vehicle fleets.3 Vulnerabilities include:
* **Cloud Service Compromise:** Attacks on cloud servers can lead to data breaches (theft of vehicle data, user credentials, operational metrics), ransomware locking access to critical fleet management systems, or manipulation of data used by CAVs.3
* **Insecure APIs:** APIs connecting vehicles or companion apps to cloud services can be exploited if not properly secured, allowing unauthorized access to data or vehicle functions.3
* **Malicious OTA Updates:** The OTA update process itself is a critical vulnerability point. Attackers might compromise the manufacturer's update servers or manipulate the update process to deploy malicious firmware or software to vehicles. This could introduce new vulnerabilities, install malware, or cause catastrophic failures.1 Faulty update steps or insecure code within legitimate updates can also inadvertently reduce security.18
* **Supply Chain Attacks:** Vulnerabilities can be introduced into software or firmware by third-party vendors in the supply chain, which are then deployed to vehicles via OTA updates, compromising them long after manufacturing.18

The security of cloud services and OTA updates is intrinsically linked to the security of the entire automotive supply chain. A holistic approach is required, ensuring security from component development by third-party vendors through to the final deployment process.A summary of these component-specific vulnerabilities is presented in Table 1.**Table 1: CAV Component Vulnerability Matrix**

|  |  |  |  |
| --- | --- | --- | --- |
| **Component** | **Common Vulnerabilities** | **Example Attack Vectors** | **Potential Impacts** |
| **ECU (Generic)** | Software bugs, firmware flaws, weak authentication, insecure debugging ports | Malware injection, unauthorized reprogramming, exploiting known CVEs | Loss of specific function, gateway to other systems, unsafe state |
| **CAN Bus** | Lack of authentication, no encryption, broadcast nature, OBD-II port access | Message spoofing/injection, eavesdropping, DoS (bus flooding), replay attacks, CAN injection | Unauthorized control (brakes, steering), vehicle theft, system disruption |
| **Sensors (LiDAR)** | Susceptibility to spoofing/blinding/jamming, data integrity issues | Infrared light projection, physical obstruction, signal replay, data manipulation | Incorrect object detection/ranging, phantom obstacles, sudden braking/acceleration, compromised navigation |
| **Sensors (Radar)** | Susceptibility to jamming/spoofing, signal interference | RF jamming, signal reflection attacks, false target injection | Inaccurate speed/distance measurement, ghost targets, failure to detect real objects, ACC/AEB malfunction |
| **Sensors (Cameras)** | Adversarial attacks, image spoofing/manipulation, blinding, environmental limitations | Adversarial patches/stickers, projecting false images, intense light, physical obstruction | Misclassification of objects/signs, lane departure, incorrect traffic light recognition, impaired ADAS functions |
| **Sensors (GPS)** | Signal spoofing, jamming, replay attacks | Broadcasting fake GPS signals, RF jamming, retransmitting old signals | Incorrect vehicle location, route deviation, navigation system failure, unsafe maneuvers based on false position |
| **IVI System** | OS vulnerabilities, insecure apps, weak Wi-Fi/Bluetooth security, exposed APIs | Exploiting app flaws, malware via USB/apps, Wi-Fi MitM, Bluetooth exploits (e.g., AirBorne) | Data theft (contacts, location), microphone eavesdropping, distraction, pivot to critical systems |
| **V2X Gateway/OBU** | Weak authentication/encryption, protocol flaws, insecure key management, RSU compromise | Message spoofing (false warnings), DoS on communication, MitM, Sybil attacks, data leakage | Misleading safety alerts, traffic disruption, incorrect cooperative maneuvering, privacy loss |
| **Cloud Platform** | Insecure APIs, misconfigurations, data breaches, weak access controls, server-side flaws | API exploitation, credential stuffing, SQL injection, exploiting unpatched server software | Fleet-wide data compromise, unauthorized remote commands, service disruption, ransomware |
| **OTA Mechanism** | Lack of code signing/validation, insecure transmission, compromised update server | Malicious firmware injection, rollback to vulnerable versions, MitM during update | Vehicle bricking, installation of backdoors, fleet-wide compromise, safety system disablement |

**B. Prominent Cyber Threats and Attack Vectors**

The vulnerabilities inherent in CAV components and systems give rise to a diverse range of cyber threats and attack vectors. These threats are not merely theoretical but have been demonstrated in numerous research efforts and real-world incidents, underscoring the urgent need for robust security measures. Attack vectors are diversifying from primarily physical or short-range attacks to sophisticated remote exploits targeting software, APIs, and cloud infrastructure, enabling attacks of a much larger scale and impact.

**Works cited**

1. Security Challenges for Connected and Autonomous ... - BAE Systems, accessed May 16, 2025, <https://www.baesystems.com/sites/Satellite?blobcol=urldata&blobkey=id&blobtable=MungoBlobs&blobwhere=1668612986595&ssbinary=true>
2. Security Concerns in CAN, CANopen, and J1939 Networks ..., accessed May 16, 2025, <https://jcom1939.com/security-concerns-in-can-canopen-and-j1939-networks/>
3. Mind the Cyber Gap: Key Insights from Upstream's 2025 Automotive ..., accessed May 16, 2025, <https://upstream.auto/blog/insights-from-upstreams-2025-automotive-cybersecurity-report/>
4. VicOne Research Estimates Tens of Billions in Automotive ..., accessed May 16, 2025, <https://vicone.com/company/press-releases/vicone-research-estimates-tens-of-billions-in-automotive-cyberattack-losses-plus-rising-vulnerabilities-and-risks>
5. CAN Bus Security → Term - Prism → Sustainability Directory, accessed May 16, 2025, <https://prism.sustainability-directory.com/term/can-bus-security/>
6. www.arxiv.org, accessed May 16, 2025, <https://www.arxiv.org/pdf/2504.20180>
7. How The Reputation Of A Dealership Can Be Shattered In An Instant, accessed May 16, 2025, <https://heliontechnologies.com/2024/09/03/the-real-cost-of-a-cybersecurity-incident-how-it-can-wreck-an-auto-dealerships-reputation/>
8. How Subaru's IVI System Admin Panel Vulnerability Could Have ..., accessed May 16, 2025, <https://vicone.com/blog/how-subarus-ivi-system-admin-panel-vulnerability-could-have-enabled-vehicle-tracking-and-control>
9. Automotive Cybersecurity Compliance - Security Compass, accessed May 16, 2025, <https://www.securitycompass.com/industry/automotive/>
10. The Future of V2X Communication: Cybersecurity Vulnerabilities ..., accessed May 16, 2025, <https://www.hermessol.com/2024/11/08/v2x/>
11. (PDF) CYBERSECURITY IN AUTOMOTIVE NETWORKS ..., accessed May 16, 2025, <https://www.researchgate.net/publication/389128493_CYBERSECURITY_IN_AUTOMOTIVE_NETWORKS_MITIGATING_THREATS_IN_CAN_LIN_AND_AUTOMOTIVE_ETHERNET_SYSTEMS>
12. Securing the Future: DevSecOps in Connected Cars & Smart Factories, accessed May 16, 2025, <https://vlinkinfo.com/blog/devsecops-in-automotive/>
13. New Cyber Security Standard Will Propel Cultural Shift in ..., accessed May 16, 2025, <https://innovationatwork.ieee.org/new-cyber-security-standard-will-propel-cultural-shift-in-automotive-industry/>
    1. 7 Automotive Cybersecurity Best Practices - ISMS Connect, accessed May 16, 2025, <https://isms-connect.com/insights/7-automotive-cybersecurity-best-practices>
    2. NIST finalizes cybersecurity incident response framework profile ..., accessed May 16, 2025, <https://www.hoganlovells.com/en/publications/nist-finalizes-cybersecurity-incident-response-framework-profile-aligned-with-csf-20>