International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 10 | Oct - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

Why Cybersecurity is a Corporate Priority in the Automotive Industry

Suresh Sureddi
ssureddi@gmail.com

Abstract: The automotive industry is going through a rapid transformation due to technological advancements like connected cars (V2X technologies), artificial intelligence, autonomous driving, 5G, and cloud computing. These changes provide opportunities and numerous challenges to OEMs, suppliers, and other stakeholders. This review paper first lists the various threats encountered by the industry on different vehicle attack surfaces. It highlights the adoption of different technologies in modern cars and the potential threats they may bring. It finally justifies why cybersecurity has become a corporate priority for stakeholders in the automotive industry.

Keywords: Connected Vehicles, Cybersecurity, Connectivity, CAN (Controller Area Network), Autonomous, V2X(Vehicle-to-Everything), Artificial Intelligence.

1. Introduction:

Autonomous driving, connected cars, electric vehicles, and shared mobility (ACES) have dominated the technical advancements in the automotive industry **[1]**. These innovations and massive data handling and sharing turn modern cars into computers on wheels. The in-vehicle technology enabled modern intelligent vehicles consisting of millions of lines of complex code to provide various real-time information to vehicle occupants. These advanced technologies offer comfortable services to people and ensure the safety of drivers and passengers. However, as these modern cars become more connected (to the cloud, to wireless networks(V2N), and with each other(V2V), and with infrastructure(V2I), they become vulnerable to cyber-attacks. The complexity of the system and the increase of external communication interfaces make the connected cars more exposed to network attacks. As per the functional security of automotive cyber-physical systems (ACP), an attack on the vehicle network will not only cause personal privacy disclosure and economic loss but also endanger people's life safety and even become a national public security problem. The U.S. Department of Transportation (USDOT) **[2]** understands the threat to the nation's cyberinfrastructure and has prioritized cybersecurity. This paper first lists several attacks encountered by various manufacturers in the industry and then provides the details of different technologies being deployed by OEMs and suppliers that could be vulnerable to multiple attacks. This background information justifies why cybersecurity has become a corporate priority.

Here are some real-world cyber security incidents that occurred during the last decade.

Two cybersecurity experts hacked a 2015 Jeep Cherokee remotely over 10 miles away through an internet connection. The vulnerability of the feature allowed the hacker to access the IP address. The hackers then gained access to drive-by-wire systems and could toggle the ignition, lower the engine speed, abruptly engage brakes, or disable the brakes.

In 2016, PenTestPartners exploited the vulnerability of the Mitsubishi Outlander. This model initially used a Wi-Fi access point instead of a GSM module for connected services. PenTestPartners took advantage of this vulnerability **[3]** by cracking the Wi-Fi Pre-Shared Key and only required access to the vehicle while it was connected to an authorized phone. This provides access to turn off the alarm and even unlock the car. Once they knew a vehicle's SSID (Service Set Identifier), any car of the same make and model could be found and connected to a mobile device to determine its geolocation.

A similar incident happened with a 2016 Nissan Leaf **[4]**. In this case, Nissan's "NissanConnect" software required the user to enter the vehicle identification number (VIN) into an app to connect to the vehicle. The VIN was often stamped on the windscreen for easy access. This connection can be established remotely, and once connected, a hacker can determine the vehicle's geolocation and control all heating and cooling units (air, seat, steering wheel).

In 2018, three of BMW's models were proven to have vulnerabilities through OBD connection, allowing the hacker to shut off the vehicle by overloading the system with erroneous messages **[5].** In 2017, a Tesla fleet was hacked by exploiting a bug in the fleet's central server. The hacker gained access to control any car in the fleet, being able to pass Tesla commands, such as drive home remotely **[6].**

Vulnerabilities were exploited in the infotainment system of the 2020 Volkswagen Polo, where a hacker gained access to toggle the traction control and review the driver's personal data. Context Information Security was also used to perform a "man in the middle" attack on the Ford Focus, intercepting messages from the TPMS (Tire Pressure Monitoring System).**[7]**

In 2019, an OEM's automotive cloud was hacked via third-party services and a tier-1 supplier network.**[1]**

Keyless entry issues were an intuitive entry point for automotive security since this technology can unlock the door to a car or start the engine without physically inserting a key. In 2021, Lennert Wouters **[8]** discovered a series of vulnerabilities in the Tesla Model X's keys, including an OTA function that did not implement security mechanisms and a faulty pairing protocol. The protocol allowed him to build a chain of attacks by brushing malicious firmware onto the same chip as the key fob and triggering a rekeying process that allowed the attacker to directly (and without contact) mass produce the keys to the target vehicle.

A cloud API is the main character of the whole network architecture, providing variable functions. This API's access control depends on an access token. In early 2022, a hacker remotely controlled a fleet of Tesla cars in an experiment, exposing the importance of API tokens to vehicle security and presenting a glimpse of what could happen if API tokens become lost or stolen.**[9]**

In the case of Electric vehicles (EVs), many charging station-related vulnerabilities were reported in 2021-2022. In 2022, researchers investigated charging piles and discovered a vulnerability in the plug-and-charge feature, enabling them to get free charging after exploiting the vulnerability.**[9]**

In another incident, a popular automotive vendor suspended operations for two days after a cyberattack hit a supplier. Malicious actors usually steal data and threaten to publish sensitive company data. **[10]**

2. Different technologies contributing to increased Cybersecurity risks in automotive and their countermeasures:

2.1. In-vehicle infotainment systems (IVI):

The user can interact with In-Vehicle infotainment via Bluetooth, USB, Wi-Fi, SD card, touch screen, and GPS. IVI connects with other Electronic Control Units (ECUs) in the car via the CAN bus, ethernet, or MOST, effectively serving as a possible gateway for an attacker. Essentially, IVI has features that make it more convenient and user-

friendly but also give the attacker more options to access the car. The attacker can modify IVI firmware, making the attack persistent and allowing the injection of malicious frames into internal vehicle network connections. **[9]**

2.2. Telematics:

The car's Telematics Control Unit (TCU) provides connectivity to the external world over cellular networks. The Internet of Things (IoT) technology is developing rapidly, and the Internet of Vehicles (IoV) is the typical application of IoT technology in the automotive industry. IoV typically involves Vehicle-to-Vehicle(V2V) communication, Vehicle-to-cloud communication(V2N) and Vehicle-to-Infrastructure(V2I).

OTA (Over-The-Air Updates)

In the past, when new car owners drove vehicles out of the dealership, they would be stuck with the same technology until they either revisited the dealership or bought new cars. This isn't the case anymore. Cloud services allow remote vehicle updating (OTA) of firmware and software quickly without requiring a visit to the dealer. In this case, TCU (Telematics Control Unit) is the gateway module that updates the car's other ECU (Electronic Control Unit) software. In typical OTA architecture, the OEM backend pushes the data through the OTA manager, which is the leading software component in the TCU and is responsible for flashing the software on all other ECUs. MQTT is used for command and control, and HTTP is used for data transfer. OEMs realize remote vehicle updating services (OTA) improve the relationship between the car owner and manufacturer. However, at the same time, this connectivity feature increases the vulnerability to cyber-attacks, particularly related to authenticity and integrity.

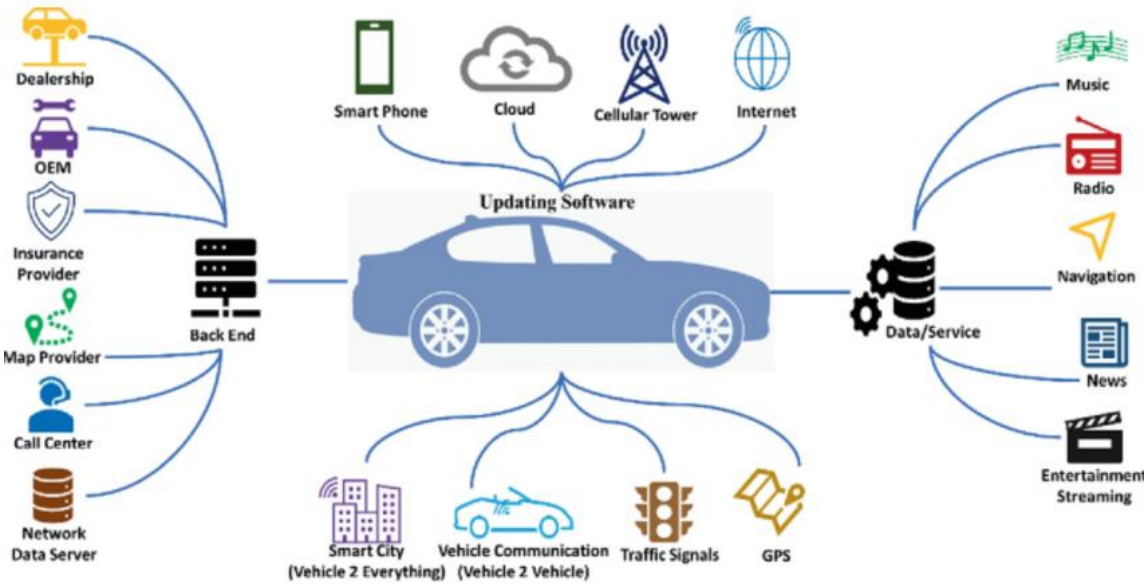

Figure 1: Overview of Connected Vehicle Technologies [Pic source: [10]

2.3. ICV (Intelligent Connected Vehicles)/CAV (Connected and Autonomous)

Connected vehicles are equipped with sensors such as cameras, LiDAR, RADAR, and GPS receivers that capture the status of the vehicle environment to help in automatic decision-making. This collected data is processed and communicated to other vehicles, in-vehicle applications, mobile devices, third-party service providers, and external

infrastructure. This V2X (vehicle-to-everything) communication involves communication between Vehicle-to-Vehicle(V2V), Vehicle-to-Infrastructure(V2I), Vehicle-to-Pedestrian(V2P), and V2R (vehicle-to-roadside units). It is facilitated by VANET technology (Vehicular ad hoc networks). This data exchange can be vulnerable to cyber attacks ranging from unauthorized accessing of the steering wheel, unintentional braking, and location and identity manipulation. Attacks in CAV (Connected and Autonomous Vehicles) include Eavesdropping, Man-in-the-middle, replay, false injection, Denial of service (DoS), jamming, spoofing, masquerading, and repudiation attacks.

2.4. RVI (Remote Vehicle Interactions)

RVI functionalities include locking/Unlocking the door, remote start/stop, and climate control settings. In this case, the User's phone connects to the vehicle's TCU (Telematics Control Unit) box through a cloud server. Cloud APIs exchange messages between the car and the smartphone, which is vulnerable to cyberattacks.

2.5. Sensors and In-vehicle networks:

Various ECUs (Electronic Control Units) in a car are connected through In-vehicle networks such as CAN, MOST, Ethernet, and LIN. These network protocols lack the design of an information security mechanism at the beginning of their design, which makes them vulnerable to cyber-attacks such as sniffing, jamming, replay, or forgery of messages.

2.6. Remote Keyless Entry Systems:

Since RF waves are easily accessible within range, this technology must include thorough safety and security measures to prevent exploitation.
Initially, most RKE key fob designs include fixed codes, which are stored in the flash memory for use as a compare and match. But this design was subject to replay attacks. In this case, the attacker records the user’s remote-control signal and sends it directly to the vehicle to achieve the same function. This replay attack could be prevented by using a rolling code mechanism. Here, whenever a successful command is accepted by a vehicle, the key, and the vehicle will discard the current key, so this design effectively limits the occurrence of replay Attacks. However, the rolling code mechanism had its limitations. It needs a set of cryptographic tables.
By abandoning the traditional RKE design, Tesla used Bluetooth Low Energy (BLE) with
a data layer/application layer authentication and encryption design to produce key fobs. As the cost of BLE devices decreased, more car manufacturers followed up with this design in their advanced vehicles. However, this design has been repeatedly defeated by cost issues. Additionally, due to the flexibility of the BLE key fob used by Tesla on latency, the relay attack became feasible and was successfully used on the 2022 Model 3. One study **[9]** proposes countermeasures such as (1) using a rolling code and avoiding excessive cost cutdowns. (2) Separate the door control and engine unlock functions to avoid the problem of simply opening the door to drive the vehicle away.

2.7. EV Charging stations:

Compared to a traditional car, an EV has more sensors and communication protocols between the vehicle and a charging station, which leads to multiple security issues. Here are the top three attack surfaces as per one study **[9]**

- **CAN bus-based communication between an EV and a charging station:**

CAN bus-based protocols are often used on EV and charging station communications, and data is always transferred by plain text. This allows hackers to hijack the sessions to deploy Man-In-The-Middle (MITM) attacks. They could also transfer malicious code to the EV or charging station.

- **2. App/Cloud services for EV charging stations**

EV charging stations are usually connected to the cloud for transactions and billing procedures. Some EVs provide apps to give users a more convenient experience. In the context of cybersecurity, this is one of the attack surfaces. An attacker could gain privileges to gather user information from mobile devices or penetrate the cloud server.

- **3. Radio communications**

Radio communications, RFID, Bluetooth, and customized radio signals are frequently used on EV charging systems. These could become remote attack surfaces that attackers use to access the EV components. For example, hackers could remotely open the charging port or transfer malicious code to the EV or charging station to gain control.

2.8. Supply chain Security:

The automotive supply chain involves multiple stakeholders, including manufacturers, suppliers, and service providers. Cybersecurity applications include ensuring that all vehicle components and software are secure and free from vulnerabilities. This involves rigorous testing, secure coding practices, and regular security audits.

3. Conclusion:

This article explores several security breaches in the automotive industry over the past decade. It also explores advanced technologies that are being integrated, which could be vulnerable to various types of cyber-attacks. Cyber-attacks can happen at any interface of the vehicle architecture, anywhere between the vehicle communication bus protocol level and the application level, including integrated interfaces to the cloud, communication with other vehicles, and external infrastructure.

Considering the vulnerabilities that the above technologies can bring in and the safety concerns that they can cause, like unauthorized access to critical functions, which can lead to accidents, it has become essential for corporations to give high importance to the implementation of cybersecurity. Also, governments and regulatory bodies have defined standards for the auto industry. Compliance with standards such as ISO/SAE 21434 has become mandatory for corporations to ensure vehicle safety and security. Consumers are increasingly aware that autonomous and connected vehicles can bring in the same level of cyber risks as IoT (Internet of Things) as cars are becoming computers on wheels. Hence, consumers need to gain trust that their vehicles are secure. A breach can damage automakers' reputations. Also, the financial implications are very high for corporations in case of a breach. Hence, it is essential for corporates to proactively take necessary cybersecurity measures by investing upfront during the product development life cycle. Design, implementation, and testing of Security methods should be an active part of the regular SDLC (product Development Lifecycle). It shall run in parallel with the software development lifecycle instead of emphasizing security at the later stage of the development cycle. Cybersecurity is a critical priority for the automotive industry. By proactively addressing cybersecurity, automotive companies can comply with regulations, protect their customers, and safeguard their financial and reputational interests. As the industry continues to evolve, corporations need to maintain robust cybersecurity measures to ensure modern vehicles' safe and secure operation.

References

[1] McKinsey & Company, June 22, 2020, Cybersecurity in automotive: Mastering the challenge.
[2] Brecht, B.; Therriault, D.; Weimerskirch, A.; Whyte, W.; Kumar, V.; Hehn, T.; Goudy, R. A security credential management system for V2X communications. IEEE Trans. Intell. Transp. Syst. **2018**, 19, 3850–3871.
[3] D. Lodge, "Hacking the Mitsubishi Outland PHEV hybrid," PenTestPartners, 05 06 2016. [Online]. Available: https://www.pentestpartners.com/security-blog/hacking-the-mitsubishi-outlander-phev-hybrid-suv/. [Accessed 10 05 2020].
[4] R. Hull, "Nissan disables Leaf electric car app after revelation that hackers can switch on the heater to drain the battery," This is Money.co.uk, 26 Feb 2016. [Online]. Available: https://www.thisismoney.co.uk/money/cars/article-3465459/Nissan-disables-Leaf-electric-car-app-hacker-revelation.html. [Accessed 17 06 2021].
[5] "New Vehicle Security Research by KeenLab: Experimental Security Assessment of BMW Cars," Keen Security Lab, 22 05 2018. [Online]. Available: https://keenlab.tencent.com/en/2018/05/22/New-CarHacking-Research-by-KeenLab-Experimental-Security-Assessment-of-BMW-Cars/. [Accessed 15 06 2021].
[6] F. Lambert, "The Big Tesla Hack: A hacker gained control over the entire fleet, but fortunately he's a good guy," Electrek, 27 08 2020. [Online]. Available: https://electrek.co/2020/08/27/tesla-hack-control-over-entire-fleet/. [Accessed 10 06 2021].
[7] L. Barber, "Popular connected cars from Ford and Volkswagen could put your security, privacy and safety at risk, Which? finds," Which? 09 04 2020. [Online]. Available: https://press.which.co.uk/whichpressreleases/popular-connected-cars-from-ford-and-volkswagen-could-put-your-security-privacy-and-safety-at-risk-which-finds/.
[8] Lennert Wouters, Benedikt Gierlichs, and Bart Preneel. (Aug. 11, 2021). Ruhr-Universität Bochum. "My other car is your car:
compromising the Tesla Model X keyless entry system." Accessed on Nov. 14, 2022, at https://tches.iacr.org/index.php/TCHES/
article/view/9063.
[9] https://vicone.com/files/rpt-automotive-cybersecurity-in-2022.pdf VicOne, Automotive Cybersecurity in 2022
[10] Madhusudan Singh, 19-May-2021, Cybersecurity in Automotive Technology.