HIGH SCHOOL EDITION
Journal of Student Research
Volume 13 Issue 2 (2024)

The Need for Cybersecurity in Automotive Industry

Anay Prasanth Nair[1], Sarada Prasad Gochhayat[#], Virgel Torremocha[#] and Jothsna Kethar[#]

[#]Advisor

ABSTRACT

This research paper analyzes the importance of cybersecurity in the automotive industry and explains how cybersecurity threats impact the modern world of connected, autonomous, and electrical vehicles. Furthermore, this paper covers in-depth research into the different types of automotive cyber threats such as physical, sensor, software, and network attacks on a vehicle, and various methods to prevent these threats from happening in real-world scenarios. The research paper also helps the reader to gain a broader understanding of cybersecurity in the automotive world. The methodology of this research involved analyzing and collecting information through various external websites, articles, and research papers. Information was collected on automotive cybersecurity incidents from news articles and international cyber security conference presentations. Based on this evidence from various external sources, the research problem was supported by factual data. This paper also talks about all the various solutions to cybersecurity threats in depth such as authentication and encryption, malware detection, software analysis, VPNs (Virtual Private Network), and cryptography. This paper also provides information about some of the new regulations and standards that are currently adopted in the automotive industry. With the rapid change in automotive technology, it is important to be aware that cars can have up to 150 ECUs (Electronic Control Unit) and about 300 million lines of code in near future which could expose more vulnerabilities. (2020, McKinsey & Company). To meet the challenge of these automotive cyber security threats, it is important that awareness should be created among the product engineers and researchers working on future automobiles. This paper attempts at exploring the challenges with automotive cyber security and creating this awareness.

Introduction

Modern-day automobiles have a lot of software features to enable connectivity, electrification, and autonomous driving. This could lead to cyber-attacks/threats potentially putting people's lives at risk. There are multiple components of a vehicle that are connected to the network systems which allows hackers to use multiple techniques to hijack a vehicle's network system and send cyber-attacks which can potentially damage the vehicle and put it under their control. Over the last several years, modern cars have become data centers on wheels. Comparing the lines of code in modern connected cars with aircraft and PCs provides a glimpse into the challenges of securing these vehicles. Today's cars have up to 150 ECUs (Electronic Control Unit) and about 100 million lines of code; by 2030, many observers expect them to have roughly 300 million lines of software code (2020, McKinsey & Company). Modern cars, which always rely on some type of software, are easily made a target for cyber-attacks. The exploiting of the vulnerabilities within those systems can allow unauthorized access to the car by any individual or group, easily compromising the vehicle and having it under their full control. Hence, we need to focus on automotive cybersecurity, and the possible solutions to prevent attacks on connected vehicles.

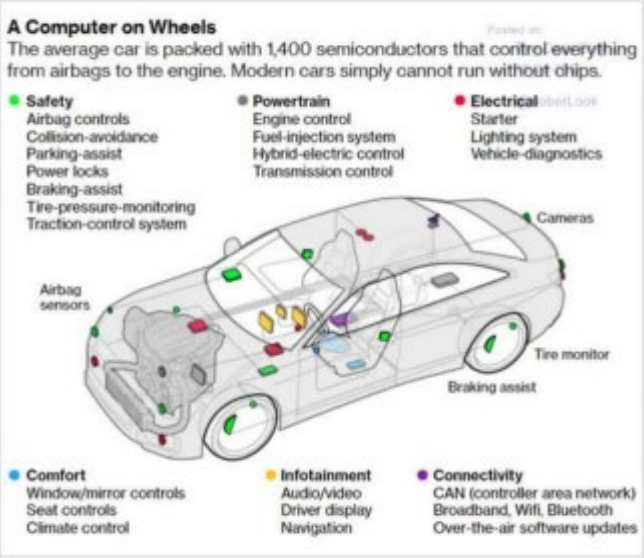

Figure 1. Car system breakdown, and the purposes of the parts. (2022, Scott Buchanan).

Related Studies

Cybersecurity attacks and threats are a major problem worldwide. According to the article by Tripwire (2022), the necessity for cyber security in the automotive industry was first introduced in the year of 2015, when 1.4 million connected vehicles were heavily impacted by a cyber-attack. This was proven through a demonstration conducted by researchers on how an attacker can control a connected vehicle. Ever since this has not only affected the automotive industry but also made it a target for many attackers to compromise a connected vehicle. As the automotive industry becomes more connected and digitized — and automotive companies open new revenue streams as a result — the attack vectors are evolving beyond traditional stakeholders. According to the article, the top cyberattacks vectors in 2022 were telematics and application servers (35%), remote keyless entry systems (18%), electronic control units (14%), automotive and smart mobility APIs (12%), infotainment systems (8%), mobile applications (6%), and EV charging infrastructure (4%). During the year 2023, there were around 295 major automotive and smart mobility related cybersecurity incidents reported from across the world.

According to an article by Typerwall (2023), in June 2020, automotive giant Honda was hit by a ransomware attack that halted operations at several assembly plants across the world. The attack was known as the "Snake" ransomware, a type of attack in which hackers encrypt sensitive files and decrypt the files in exchange for money from their victim. Many of these attacks continue to rapidly increase globally, and further security measures are implemented every day to keep the manufacturers safe.

Further real examples include, "Amid Russia's invasion of Ukraine, hackers disabled electric vehicle charging stations along Russia's M11 motorway and programmed them to display pro-Ukrainian messages" (*Team Nuspire, 2022).*

According to Global Automotive Cybersecurity Report (2023), "in April 2022, a German-based vehicle rental, car sharing, and ride-hailing service provider, was hit by a cyber-attack that forced it to restrict access to all IT systems, causing widespread disruption to its global operations.11 The company reacted quickly and effectively, restricting impact to short-term disruption in customer services and specific branches." Cyberattacks are increasing every year, becoming stronger and more accessible into the wrong hands who mainly target

the car manufacturing industries. Various attacks are also costing automakers more than $1 billion in losses, which is extremely bad.

According to Global Automotive Cybersecurity Report (2023), in June 2023 a South Korean OEM's infotainment unit was hacked despite multiple security fixes.

On Monday, November 13, Yanfeng's website stopped working, resulting in many US-based automakers reporting disruptions in their production. The US automakers affected by the cyberattack on Yanfeng include Stellantis, which encompasses the Chrysler, Dodge, Jeep, and Ram brands. (Maria Merano, 2023)

In December 2021, an automotive supplier was breached by ransomware gangs three times in the space of two weeks. (Team Nuspire, 2022).

Types of Cyberattacks On Connected-Vehicles

There are numerous types of cyber-attacks on connected vehicles, some of which include: Physical Attacks, Sensor Attacks, Software Attacks, and Network Attacks.

Physical Attacks

Hardware Modification: This type of attack occurs when the computer's physical component is damaged. Hardware hacking may also be the result of replacing, removing, or replicating components of hardware systems within a car. (Toni Jardini, 2021)

Node Replication: This is where physical hardware is duplicated by the attacker when they damage the network device by injecting some type of clone of the hardware itself into the environment (Toni Jardini, 2020).

Physical Damage: Any physical damage to a connected vehicle can potentially destroy its components like locks and headlights. Even worse, glass windows, brakes, windshields, and much more. Attacks can occur through multiple ways such as those (Toni Jardini, 2020).

Side Channels: Side channels are based on information gained from the implementation of a computer system to directly access the vehicle in service. A vehicle may be sold to a third party (such as a registered dealer), so data may be wiped or left on components of the car, which could serve as potential information disclosure vulnerabilities, privacy, and sensitive user data (Toni Jardini, 2021).

Sensor Attacks

(Controller Area Network) CAN Bus: This is a network communication component that allows communication between two different automobiles, or devices. Attacks on these devices may include signal injection, physical disruption to the device, spoofing, etc (Toni Jardini, 2021). These control areas can be specified as the car's 'nervous system' hence the reason why attacks on them can lead to life-threatening situations.

LIDAR (Light Detection and Ranging): LIDAR, also known as light detection and ranging, is a remote sensing method that helps a car sense and understand its surroundings. Typical uses for LiDAR in a vehicle include collision avoidance, adaptive cruise control, and object recognition (Toni Jardini, 2021). An attack on the car's sensors includes DoS attacks, spoofing, and object misinformation and recognition.

RADAR (Radio Detection and Ranging): Some of the ways a radar attack occurs on a vehicle include DoS, spoofing, and jamming. Spoofing attacks can manipulate the car's radar sensors which can mislead the radar with false information and direct the car to risk of collision incidents (Toni Jardini, 2020).

USB (Universal Serial Bus): Attackers can easily manipulate a vehicle's systems by injecting malware through a USB, which can potentially damage all the systems of a vehicle. Essentially, with a removable media

attack or USB drop attack, the attacker can program the device to perform any actions that they would be able to perform, just as if they were sitting at your computer. You can protect yourself from this kind of attack by never plugging an unknown removable media device into your computer or mobile device (2023, David Dungan). Many of these common attacks can occur anywhere including, hotels, airports, workplaces, etc.

CD (Compact Disc): Although CDs are usually used in cars to play music, there are possibilities for hackers to inject malicious codes into the music files when it's playing which can be corrupted and transmitted to the CAN bus allowing the attacker to access vehicle controls and commands/ECU.

Software Attacks

Infotainment Systems: Infotainments typically run operating systems such as those seen with Android, Integrity real-time operating system (RTOS), Linux, QNX, and Windows Embedded Automotive. Potential areas of attack are ransomware, crypto mining, keylogging, rootkits, etc (Toni Jardini, 2020).

Firmware: The computer software that provides a low-level control for a device's hardware. Hackers can inject malicious codes or information into the software which can alter the firmware's settings or cause update errors with the injected malware in the system (Toni Jardini, 2020).

Integrated & Third-Party Applications: Many common attacks happen through malicious and compromised third-party applications, which are used to trick the network system of the car resulting in false information to car sensors and radars. They often require access to a vehicle's command and control systems which can pose significant threats to the vehicle. As an example, in early 2022, a German cybersecurity researcher exploited a vulnerability in a popular third-party companion application,7 that gave him access to all the functions of the OEM's native application and allowed him to remotely control 25 EVs around the world. (Upstream, 2023).

Network Attacks

Controller Area Network (CAN): The controller area or the CAN, is the component of a vehicle that allows the microcontrollers and devices to communicate with each other. It is a common target for attackers, as they can inject malicious information and gain access to the network. They can also send direct or indirect access points to send messages through the CAN bus which can be tricked to unlock the vehicle and its control and sensor systems (Toni Jardini, 2020).

Local Interconnect Network (LIN): LIN is used to facilitate the intercommunication of the ECU, used to control lights, engines, air conditioning, steering wheels, seats, and doors. After CAN, LIN is the network most subject to exploitation by malicious agents. Among the threats to LIN, the most frequent and common are Message Spoofing (criminals send messages with inaccurate information so that vehicle communications are stopped), Response Collision (take advantage of the error-handling mechanism of the LIN), and Header Collision attacks (an attacker sends a fake header to collide with a legitimate header) (Toni Jardini, 2020).

FlexRay: A component that allows automotive communication protocol, is also exposed to various cyber-attacks that can affect the car, such as spoofing and DoS attacks (Toni Jardini, 2020).

Ethernet: Many of the attacks on the ethernet include man-in-the-middle attacks, MAC spoofing, malware, phishing, and various other cyber-attacks. Attackers can collect private data/information and steal sensitive information from individuals through malware injections (Toni Jardini, 2020).

Bluetooth: Bluetooth networks provide a capability for cyber attackers to intercept data and images passed between both cars and mobile phones. Bluetooth network attack examples include BlueBorne and Carwhisperer. BlueBorne is an attack vector by which hackers can leverage Bluetooth connections to penetrate and

take complete control over targeted devices. Carwhisperer is a hacking technique that can be used by attackers to hack a hands-free Bluetooth in-car system and connect it to a Linux system. (Toni Jardini, 2020)

Wi-Fi: Connected cars are attacked in various ways through its WiFi. For example, such attacks include "Man-in-the-middle attack" (or Attack hijack) and "Wi-F is spoofing". In the Man-in-the-middle attack, the attacker intercepts communications between two parties. WiFi spoofing is deployed via an open network or public free Wi-Fi network where the user who joined the Wi-Fi network will be asked to log in to a spoofed page. (Toni Jardini, 2020)

Remote Keyless Entry: This is a system that allows a person to unlock and start their car without using a key physically. It is another common target for many attackers who attempt to try to steal vehicles.

2010-2022 Impact Breakdown, Based on 1100+ Automotive-Related Cyber Incidents

Data/Privacy Breach	31%
Service/Business Disruption	23%
Vehicle theft and break-ins	22%
Control Vehicle Systems	13%
Fraud	3%
Manipulate Car Systems	3%
Location Tracking	3%
Policy Violation	1%
Other	1%

Figure 2. Impact breakdown of automotive-related incidents, in specific categories like fraud, privacy breach, vehicle theft, etc. Global Automotive Cybersecurity Report (Upstream Security Ltd, 2023).

Solution to Cyber-Attacks

An attack on a connected vehicle can vary through multiple techniques. Security gaps within data handling can allow malicious attacks to exploit the vehicle's vulnerabilities, resulting in compromising data privacy and security. For example, data manipulation: access to data can enable attackers to create fake alerts in a vehicle or alter performance data, paving the way for false diagnostics or potentially dangerous driving settings. (Numaan Huq, Phillipe Lin, et al., 2023).

Due to the risks of such attacks and to put an end to it, the automotive industry proceeds to take action on the issue. Connected vehicles are equipped with a variety of sensors and communication systems that allow them to interact with other vehicles, infrastructure, and the environment around them. This connectivity brings with it several benefits, such as improved safety, convenience, and efficiency; but it also provides new opportunities for malicious actors. (Cryptomatic, 2023).

Authentication and Encryption

Authentication is one of the most critical components in any device when it comes to keeping data safe and ensuring its privacy by giving access to appropriate people. As modern cars can track our information and data and keep it safe, it is important to install some kind of verification to access such materials, so that attackers have fewer chances of accessing them. Strong authentication mechanisms prevent unauthorized access to vehicle systems, such as biometric identification and multi-factor authentication, along with other advanced encryption techniques that protect sensitive data from cyber threats. Additionally, releasing software updates ensures that potential weaknesses are patched promptly, minimizes the risk of exploitation by cybercriminals, and boosts the system's overall security. (2023, SRM Tech)

Malware and Intrusion Detection

Intrusion detection systems are widely used to monitor suspicious activities in the network. In general, Intrusion Detection Systems (IDS) are employed when network security requires more sophisticated analysis. (Khan, Y. I. 2020). Detection systems or sensors that give the driver and passengers onboard awareness of any potential threat that is on the way and are the most critical layer of defense in a car. (Toni Jardini, 2020) Detection of attacks can be categorized into two categories; intrusion detection, which focuses on the network aspect, and malware detection, which is associated with executable code and file systems.

Software Vulnerabilities Analysis

Software vulnerability analysis is a technique that attempts to identify vulnerabilities in the code before its use. It is usually divided into three groups: static, dynamic, and combination analysis. Software Vulnerability Analysis In static analysis, the code does not need to be executed to perform verification checks. It can leverage various techniques to detect vulnerabilities, including lexical and data flow analysis. Whereas in dynamic analysis, the code is required to be executed to determine errors. Fuzzing (fuzz testing) is a common technique used for dynamic analysis where invalid, unexpected, or random data are used as inputs to a computer program. Combination analysis involves both static and dynamic analysis (Toni Jardini, 2020).

Quantum Cryptography

Quantum Cryptography (also known as quantum encryption) is the basic principle of quantum mechanics that allows secure communication between channels. The advantages include detection of eavesdropping and ensuring confidentiality and authenticity of transmitted data. Quantum technology enhanced security provides differentiated products with the highest level of trust, while assuring future-proof protection that will resist future technological advancements. It can be embedded reliably in the security system of any connected car to ensure trusted and secured in-vehicle and V2X communications. (2024, ID Quantique). Quantum cryptography

provides a form of defense against hackers who may try to intercept communication between connected vehicles and their systems. Quantum cryptography guarantees the integrity of data transmitted between vehicles and infrastructure, making it impossible for any malicious actor to tamper with the information. This ensures that the vehicles receive accurate, unaltered data for decision-making processes, leading to enhanced safety on the roads. (Oct 2023, Utilities One). As quantum computers become more powerful, the traditional cryptographic systems used by self-driving cars may become vulnerable. Quantum cryptography provides a future-proof solution, safeguarding against the potential threats posed by quantum computers. (2023, Utilities One). According to Rina Richell, an SEO Analytics Manager at the United States Cybersecurity Magazine, "There are good reviews of different VPNs that prove how effective a VPN can be in keeping automotive operators safe. VPNs can safeguard a car's engine control and electronics systems. On top of protecting connected cars from external attacks, a strong VPN will also allow car users to access the internet securely via the vehicle."

When a vehicle is sending or receiving data, there can be multiple risks of attacks in between the system, however, VPNs encrypt your data while the message is either sent or received and ensure security and protection against hackers. The different types of Quantum Cryptography include:

Quantum Key Distribution (QKD): QKD is one of the most prominent applications of quantum cryptography in securing communication for self-driving cars. It allows for the distribution of encryption keys over long distances, ensuring the confidentiality of data transmitted between vehicles, infrastructure, and even remote servers (2024, Utilities One). QKD provides information-theoretic security, meaning the secrecy of the key can be proven mathematically.: QKD ensures that the communication key used for encrypting and decrypting data remains secure and free from eavesdropping attempts.

Quantum Random Number Generators (QRNG): Random numbers play a crucial role in cryptographic protocols. Quantum random number generators exploit the inherent randomness of quantum phenomena, providing a source of unpredictable and truly random numbers. (Oct 2023, Utilities One). QRNGs generate numbers that are indeterministic and not influenced by external factors, ensuring stronger encryption. (Oct 2023, Utilities One).

Quantum-resistant Cryptography: While quantum cryptography offers a secure solution against quantum adversaries, it is still in its early stages of adoption. In the meantime, researchers are working on developing quantum-resistant cryptographic algorithms that can withstand attacks from both classical and quantum computers. Quantum-resistant cryptography future-proofs the security of autonomous vehicles against potential quantum threats. Implementing quantum-resistant algorithms alongside quantum cryptography ensures long-term security (Oct 2023, Utilities One).

Efforts Towards Standardization

Many of today's automotive manufacturers have started implementing safety regulations for their cars to prevent cyber-attacks; specifically: WP.29 R155 and the ISO/SAE 21434. According to the 2023 Global Automotive Cybersecurity Report, "the guidelines outline the process and specify risk analysis and response targets, emphasizing the need to consider life-long cybersecurity threats and vulnerabilities during development, production, and post-production phases." (2023 Upstream Security Ltd.)

With the help of R155, automakers can identify and respond efficiently to security risks, mobility services, and the vehicle's control systems, while the ISO/SAE, standard provides a structured cybersecurity framework, establishing cybersecurity as an integral element of engineering throughout the lifecycle of a vehicle, from the conceptual phase until decommissioning. (2023 Upstream Security Ltd.) It improves the safety of the vehicles and increases consumer confidence.

2022 Cyber Incidents Categorized by R155 Threats & Vulnerabilities

Vulnerabilities that could be exploited if not protected	42%
Threats in back-end servers related to vehicles in the field	31%
Threats to vehicles regarding communication	14%
Threats to vehicles regarding external connectivity and connections	6%
Threats to vehicle data/code	3%
Threats to vehicles regarding update procedures	2%
Threats to vehicles regarding unintended human actions facilitating the attack	2%

Figure 3. Threats and vulnerability incidents are categorized in the R155, and how much they were impacted. Global Automotive Cybersecurity Report (Upstream Security Ltd, 2023).

According to the United States Department of Transportation, the NHTSA (National Highway Traffic Safety Administration) "promotes a multi-layered approach to cybersecurity by focusing on a vehicle's entry points, both wireless and wired, which could be potentially vulnerable to a cyberattack." Their main goal is to collaborate with the automotive industries to address cybersecurity challenges and risks in a vehicle and seek solutions or methods to improve security. This article supports the main idea regarding the need for cybersecurity in connected vehicles, and also recommends a layered approach according to the National Institute of Standards and Technology (NIST) Cybersecurity Framework's five main functions:

Identify: The first function of the framework, NIST defines the Identify function as calling on the need to "develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities." The focus is on the business and how it relates to cybersecurity risk, especially considering the resources at hand. The outcome Categories associated with this function, for example, are Asset Management, Business Environment, Governance, Risk Assessment, and Risk Management Strategy. B, Ethan 2024).

Protect: The Protect function of the Framework Core is essential because its purpose is to develop and implement appropriate safeguards to ensure critical infrastructure services delivery. The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event. According to NIST, examples of outcome Categories within this Function include Identity Management and Access Control, Awareness and Training, Data Security, Information Security Protection Processes and Procedures, Maintenance, and Protective Technology (B, Ethan 2024).

Detect: The detect function makes it easier to recognize the occurrence of an event and is the most critical step in cybersecurity. Examples of outcome Categories within this Function include Anomalies and Events; Security Continuous Monitoring; and Detection Processes." (B, Ethan 2024).

Respond: Timely detection and rapid response to potential threats and incidents. The NIST defined the response function as "develop and implement appropriate activities to take action regarding a detected cybersecurity incident". Examples of responding outcomes are response planning, communication, analysis, mitigation, and improvements.

Recover: According to the NIST framework, “Recover is defined as the need to "develop and implement the appropriate activities to maintain plans for resilience and restore any impaired capabilities or services due to a cybersecurity event” (B, Ethan. 2024). The recovery process is a procedure that is performed to maintain and ensure rapid recovery of the systems or objects affected by cyber-attacks.

Results & Discussions

Cyber Security plays a crucial role within the automotive industry, helping with the prevention of network attacks on a vehicle. With all the types of attacks on a connected vehicle, it is important to be aware of the potential harm that can occur and the ways to prevent such attacks from happening in the future. As technology rises, cyber-attacks are becoming more common and stronger to defend from, but so is the prevention of the attacks as newer technology has helped improve the security within not just automobiles but everywhere in the world. Because most of the modern cars in today’s world are almost fully connected to the network in some way or form, it is important to understand and get an idea of the types of attacks that can occur within a vehicle.

Moreover, this paper stresses enough regarding the dangers of cyber threats and attacks on connected vehicles. As the automotive industry is one of the major targets for hackers to attack, it is important to spread information worldwide and make sure automakers know the eligible safety measurements that are necessary to add to connected vehicles so that they are not easily vulnerable to various attacks when encountered.

Conclusion and Recommendation

In conclusion, modern cars today have complex interconnected network systems inside them which puts them under target for cyber-attacks. The sole purpose of this research is to provide information on the mechanisms within a connected vehicle and the types of systems that are impacted through cyber-attacks and spread awareness of all the types of attacks and their severity on connected vehicles. Additionally, the paper discusses all the vulnerabilities of a automobile, clearly identifies the solutions, and provides factual data. Automotive security has become a very active research field, and vehicle manufacturers and suppliers have started focusing on this area.

Acknowledgment

I would like to thank my family, friends, Dr. Virgel, Dr. Sarada Prasad, and Coach Jo for helping and supporting me in writing this research paper on automotive cybersecurity, and for the resources they provided to me that allowed for the completion of this paper. I would also like to thank the Gifted Gabber team for helping me learn more about the basics of cybersecurity and the fundamental concepts.

References

Bresnahan, E. (n.d.). *NIST Cybersecurity Framework Core explained*. https://www.cybersaint.io/blog/nist-cybersecurity-framework-core-explained

Buchanan, S. (2022, January 4). *How Many Semiconductor Chips Are There in a Car?*. Economist Writing Every Day. https://economistwritingeveryday.com/2022/01/04/how-many-semiconductor-chips-are-there-in-a-car/

Connected car security: Connected and secure. Thales Group. (2023, March). https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/inspired/connected-cars/staying-secure

U.S. Department of Transportation. (n.d.). *Vehicle cybersecurity*. NHTSA. https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity

Dungan, D. (2023, August 18). *Dangers of USB attacks: How you can protect your cyber self*. Cyber Blog. https://www.in.gov/cybersecurity/blog/posts/dangers-of-usb-attacks-how-you-can-protect-your-cyber-self/

2022 Global Platform. (n.d.). *Globalplatform Homepage - GlobalPlatform*. Cybersecurity in Automotive. https://globalplatform.org/wp-content/uploads/2022/11/GP_-Cybersecurity_In_Automotive-_WP_v1-2022-11-29_PublicRls_SIGNED.pdf

Huq, N., Lin, P., Kropotov, V., & Vosseler, R. (2023, November 15). *Preempting threats to connected cars: The importance of cybersecurity in a data-driven automotive ecosystem*. Security News. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/preempting-threats-to-connected-cars-the-importance-of-cybersecurity-in-a-data-driven-automotive-ecosystem

Hansen, S. (2023, January 31). *Cybersecurity for Connected Vehicles*. Secure Cryptographic Solutions. https://www.cryptomathic.com/news-events/blog/cybersecurity-for-connected-vehicles

ID Quantique, Automotive Security. (2022, December 16). https://www.idquantique.com/random-number-generation/applications/automotive-security/

Merano, M. (2023, November 14). *Stellantis production affected by cyberattack on Chinese supplier*. TESLARATI. https://www.teslarati.com/stellantis-production-yanfeng-cyberattack/

Nuspire, T. (2022, November 15). *Examining the top 5 automotive cybersecurity threats*. Security Boulevard. https://securityboulevard.com/2022/11/examining-the-top-5-automotive-cybersecurity-threats/ (2023)

QA Consultants - Software Testing & Quality Engineering. Automotive Cybersecurity. (2023). https://qaconsultants.com/wp-content/uploads/2021/01/Cybersecurity-for-Connected-Autonomous-Vehicles-Summary.pdf (2023).

2023 SRM Technologies Private Ltd. (2023, November 14). *Automotive Cyber Security Threats and protective measures: Srmtech*. SRM Technologies - Global Partner for Digital, Embedded, and Product Engineering Services. https://www.srmtech.com/knowledge-base/blogs/automotive-cyber-security/

Stern, R. (2022, September 14). *Infographic: Top Real-World Threats Facing Connected Cars and Fleets*. Upstream Security. https://upstream.auto/blog/infographic-top-real-world-threats-facing-connected-cars-fleets/ (2023).

Security in Automotive Radar and Vehicular Networks. (n.d.). https://www.caee.utexas.edu/prof/bhat/ABSTRACTS/SecurityOverview_mmWave_V2X.pdf (2023).

2024 UTILITIES ONE. (2023, October 25). *Exploring the Potential of Quantum Cryptography in Secure Communication for Autonomous Vehicles*. Utilities One. https://utilitiesone.com/exploring-the-potential-of-quantum-cryptography-in-secure-communication-for-autonomous-vehicles

YEGDate, H. (2023, November 13). *Staying Secure on the Road: How a VPN can Protect Your Cars Connectivity*. Edmonton. family. https://www.cybersaint.io/blog/nist-cybersecurity-framework-core-explained (2024)