Sri Lanka Institute of Information Technology

Introduction to Cyber Security – IE2022

Assignment – 2023 June

Automotive Hacking

IT22151056

De Silva K.R.K.D

WD.CS.01.02

Abstract

Today’s automobiles can be regarded as interconnected technologies. With the increasing interconnection, control, and dependence on current technology, they are vulnerable to a variety of cyber risks including the hacking of sensitive data and automated takes of important networks. The issue of automotive hacking has become a significant concern in recent years. This report delves into the evolution, vulnerabilities present in modern vehicles, various types of automotive hacking, ethical and legal considerations, financial implications, standards, and requirements, as well as potential advancements in this field. The summary of this report includes my personal insights and conclusions.

Table of Contents

ABSTRACT……………………………………………………………………2

INTRODUCTION TO THE TOPIC…………………………………………5

EVOLUTION OF THE TOPIC………………………………………………7

Historical Overview……………………………..……………………7

Types of Automotive Hacking Attacks………………………………12

Hacking a car by physical access……………………………………12
Keyless Entry………………………………………………………...14
Telematics…………………………………………………………....15
Smartphone Access………………………………………...……...15

Vulnerabilities in Today's Automobiles……………………..……..16

Door Locks……………………………………………………………17
In-vehicle infotainment systems………………………………………17
Systems for-on board diagnostics……………………………………..18
Telematics systems…………………………….…………………...18
Gatekeeper and Protocol Vulnerability………………………………..18

Financial Impact of Automotive Hacking……………………………..19

Risks and Consequences………………………………………………20

Remote Control Takeover……………………………………………..21

Data Theft……………………………………………………………..21

Innovative Approaches to Industry Challenges………………………..21

Segmentation and Isolation……………………………………………22

Hardware Security Modules (HSMs) …………………………………22

Secure Boot……………………………………………………………22

Penetration Testing…………………………………………………….22

Secure Software Updates……………………………………………...23

Encryption……………………………………………………………..23

Intrusion Detection System (IDS) ……………………………………23

Industry Collaboration and Standards of Automotive Hacking……….24

UNECE R 155 ….…………………………………………………….25

ISO/SAE 21434……………………………………………………….25

UNECE WP.29 -26……………………………………………………27

FUTURE DEVELOPMENT IN AUTOMOTIVE HACKING……………..24

The Security of Autonomous Vehicles………………………………..28

Supply chain security…………………………………………………29

Data Privacy and Regulations………………………………………...29

Integration with Smart Infrastructure…………………………………30

CONCLUSION…………………………………………………………..31

REFERENCES…………………………………………………………..31

INTRODUCTION TO THE TOPIC

There are various threats to cybersecurity that happen in the modern world because most of the things that are available now are made by circuits. And because many things in the market lack the necessary security, hacking happens a lot. Automotive hacking is a common sight in the modern world as vehicles are one of the most sold items in the market. Today's vehicles come loaded with computerized technology which allows easy connectivity for drivers in areas like airbags, speed control, door locks, and various driver support systems. They interact with Wi-Fi as well as Bluetooth, which attracts several vulnerabilities and security risks.

There are many ways that automotive hacking is possible, and each one has a different set of dangers. Hackers can access a vehicle's system remotely, usually using internet connections, by taking advantage of software or firmware weaknesses. The capacity to modify inside parts like USB ports is made possible by physical attacks, which demand simple entry to the vehicle. Automobiles are vulnerable to attack because of many software and communication systems. Modern vehicles provide lots of possible attack paths, that security professionals have started to highlight. Some real-world exploits have moved manufacturers to remove automobiles and update the software on mobile applications. [1]

According to the information from the OICA website, the world has recently produced more than 85,000,000 vehicles in 2022, and the amount is rising continually. This represents a 6% increase from 2021. [2]According to the above information, it appears that if there is a small fault in the vehicles, it affects a large number of people. Therefore, vehicles must have a powerful security system. By doing so, you can get benefits like preventing loss of money, vehicle safety, and reducing loss of life.

Car hacking didn’t happen before the advent of the automobile. However after the engine control unit was discovered, the car started being hacked. But the real turning point is the increasing connectivity of vehicles to external networks such as the Internet. If a device is connected to the Internet, there is always a possibility of it getting malware. Many attacks were made. Since then Tesla Model S, Toyota server breach, Nissan car hack, and Honda car hack have happened.

This report looks into automobile hacking in the digital world, covering how attackers attack, which systems are vulnerable, actual incidents, and how we can secure vehicles in the modern day.

EVOLUTION OF THE TOPIC

Historical Overview

Automotive hacking has a 20-year history. It started in 2002. In this first attack, hackers targeted engine management technologies that control performance superchargers and fuel injectors. Then, in 2005, Trifinite demonstrated how to secretly capture or transmit in-car audio transmissions using Bluetooth. By transmitting false traffic updates over FM, which forced cars to reroute, the UK company's inverted path showed in 2007 how hackers can damage the security of in-car navigation systems. [3]

When security researchers showed they could control the ECU of cars in 2010, it represented a major turning point in automotive hacking. Once they gained access, the researchers practically had the ability to override or interfere with almost every system in the car. This included the capacity to switch off the engine, disable the brakes, and affect other safety features. [4] Furthermore, in a marvelous situation, over 100 drivers in Austin, Texas faced an unsetting scenario when their vehicles were remotely disabled or when their horns began to sound out of control. This strange and unexpected situation occurred as a result of an intrusion using a web-based automobile immobilization technology. [5]

Researchers proved that physical access is not required in a follow-up study that was published in 2011. They demonstrated how an automobile’s electronic systems could be remotely affected, controlling various operations such as steering, braking, and acceleration, showing that mechanical tools, CD players, Bluetooth, cellular radios, and wireless communication channels may all be utilized for remote exploitation. [4]

In 2013, An academic article demonstrating how to hack several different brands was published by a group of Dutch and British scientists. The High Court of Britain quickly issued an injunction to prevent further publication of the material due to the ease with which wireless unlocking automobiles may accomplished. [6]

A number of incidents related to automotive hacking occurred in 2014, In this YouTube video, car security researchers uncovered vulnerabilities in car technology, urging manufacturers to address flaws. Mathew Solnik demonstrates wireless control of a car, emphasizing automotive cybersecurity. [7] This video explains that in a worrying presentation by “Secure My Car” vulnerabilities in Ford and BMW vehicles with push-button start systems were made public. The need for improved automotive security is highlighted by the possibility that attackers could enter through a damaged window and connect to the service port, essentially deactivating the security features and starting the car. [8] In a thorough threat assessment of the BMW ownership experience, Kaspersky Labs found important vulnerabilities in websites and mobile apps. These problems extended to the car’s ability to be remotely unlocked and stated, highlighting the need for stronger security protocols. [9]

In 2015, in this segment that aired on “60 Minutes,” Leslie Stahl and DARPA showcased a vehicle’s capabilities while purposefully keeping the manufacturer and model a secret. Instead of sharing the car’s specific characteristics, the emphasis was on highlighting its alarming implications. Viewers were taken in by the vehicle’s mystery and its shown skills, which caused requests for more information and clarity. [10] In another incident in 2015, Miller and Valasek’s infamous attack led to the fastest recall in NHTSA history. Their ability to remotely disable a car’s throttle attracted a lot of attention and established their place as legends in the automotive hacking world. [11] According to the

NETWORKWORLD website, Tencent demonstrated its successful hack of Tesla automobiles at the DEFCON conference, but limited media attention was given to it. Tesla's quick action in detecting and fixing the vulnerability in their automobiles was the cause of this mild reaction. By being proactive, Tesla was able to avoid significant security concerns and in-depth media coverage of the issue. [12]

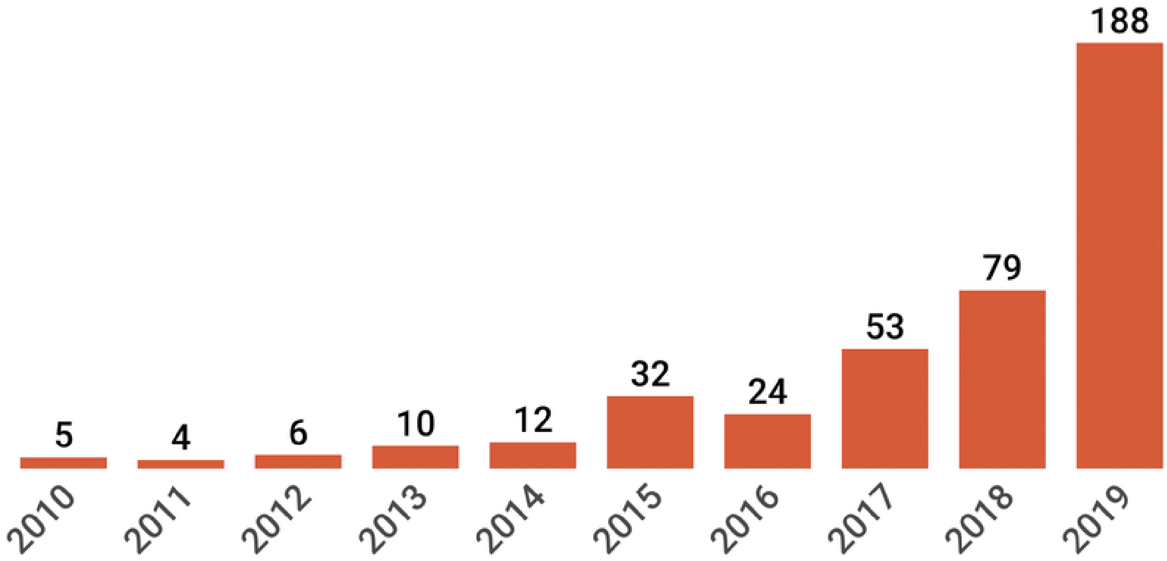

Figure 1: Growth & distribution of cyber attacks on connected vehicles between 2010 and 2019

In 2015, According to an incident in Car Driver, cyber security expert Samy Kamkar found a vulnerability in a number of connected car systems that left them open to hacking. He showed how he might use this exploit to remotely control features in OnStar-equipped automobiles, underlining the dangers that could come with connected automotive technology. [13] Again in the same year, A server security weakness that exposed millions of automobiles to theft was discovered in 2013. The keyfob's communication could be recorded and used by thieves to gain unauthorized access to automobiles. Nevertheless, this security threat was first kept a secret for two years, in part because legal actions in British courts prevented the public from learning about it. [14]

A number of incidents related to automotive hacking also occurred in 2016. A recent “Hack Yourself First” workshop for software developers in a training session for ProgramUtvikling in Norway addressed 16 essential security modules. The variety of topics covered highlighted how crucial it is for modern developers to be aware of online dangers, from SQL injection to API request control. [15] In this same year, A concerning weakness was discovered in the vehicle alarm of the Mitsubishi Outlander. A hacker might destroy the car’s security system and make it vulnerable to theft or attack by accessing the car’s Wi-Fi. [16]

Again in 2016, A hacker easily grained electrical access to a jeep, started it, and drove away, thereby stealing the car, in a real-world incident that was seen on a security camera. [17] In the same year, Once more focusing on FCA, Miller and Valasek showed off their remote acceleration and steering skills. Even the cruise control system was taken over by them. [18]

In 2016 and 2017, Chinese security researchers identified vulnerabilities in Tesla automobiles over the past two years. Tesla, however, swiftly responded to and fixed these problems, displaying a high level of reactivity in managing security worries. [19] In 2017 again, A vulnerability in the Blue Link smartphone app let hackers take advantage of unreliable Wi-Fi connections. They exposed a serious security vulnerability by being able to access sensitive user information and even remotely start cars. [20]

Over 1.5 million IoT devices, including Viper Smartstart, were exposed to a serious vulnerability in 2018 due to a misconfigured server by Calamp. Unauthorized entry, position tracking, password resets, door unlocking, engine starts, and car thefts were all made possible by this issue. [21]

ADAC research from January 2019 found that 237 automobile models with keyless entry systems were 99% hacker-prone. Control of automotive systems is a serious concern (27.22% of attacks), giving hackers the ability to alter vehicle operations. About 12.72% of automotive cyber incidents are caused by vulnerabilities in mobile apps. [22]

In 2020, According to Edinburgh News, Claims were flaws in the Ford Focus and Volkswagen Polo models that use “connected” technologies, such as internet-linked media systems. [23] For the advantage of security researchers, the “Car Hacking: Attack and Defense Challenge” data was provided in 2020. It was developed by a number of organizations, including Culture Makers and the Korea Internet and Security Agency. [24]

A North American EV company encountered a cyberattack in April 2021 where thieves breached the door of the vehicles using a drone equipped with a Wi-Fi dongle. In London in September 2021, thieves took 25 high-end European-made vehicles using advanced hacking tools. The biggest automotive dealer in Europe, Emil Frey, experienced a ransomware attack in January 2022 that had an impact on their systems and client data, but the particulars of the breach were kept a secret. [25]

Types of Automotive Hacking Attacks

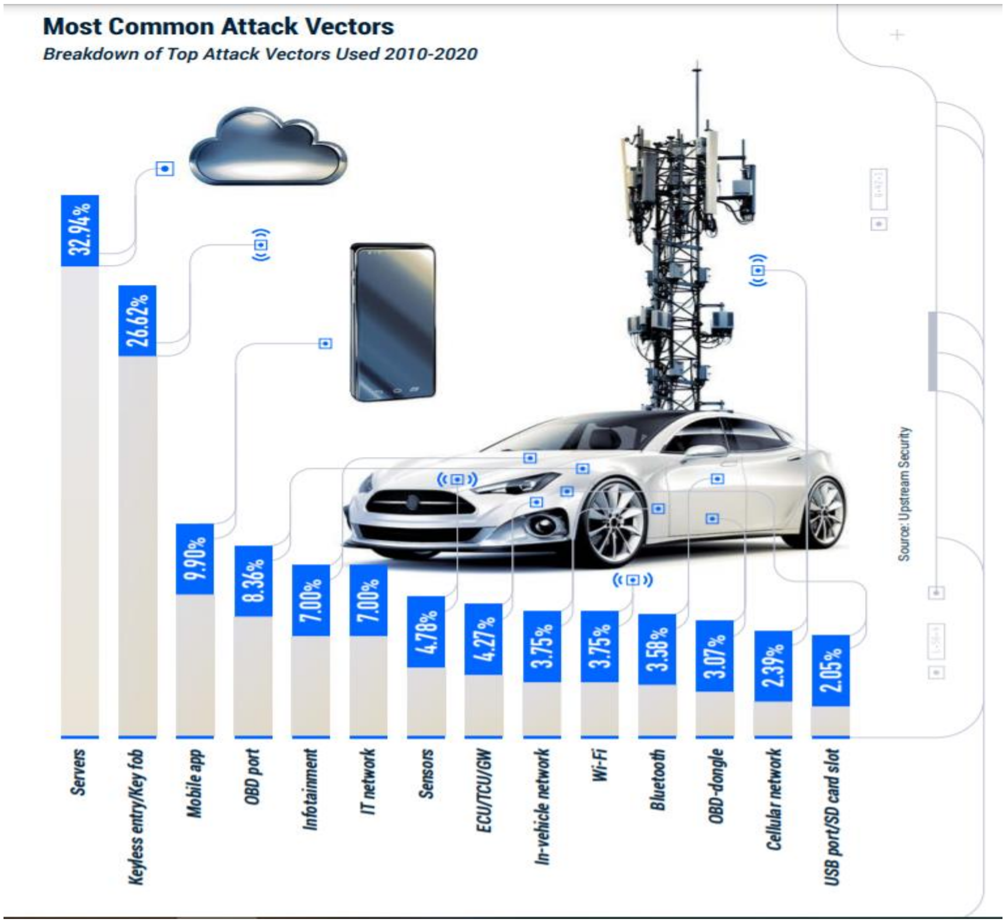

Figure 2: Most Common attack vectors

Attacks on automotive electronics aim to compromise the security and privacy of the people who are riding in the vehicles by taking advantage of vulnerabilities to take over essential functions. Understanding the different kinds of automotive hacking attacks is essential for both consumers and the automotive sector because it emphasizes the necessity for strong security measures to fend off cyber threats in the constantly changing automotive environment. This introduction serves as a jumping off point to examine several types of automotive hacking attacks, such as physical attacks, remote attacks, ransomware attacks, CAN bus attacks, ECU hacking, telematics and relay assaults, and keyless entry vulnerabilities. To mitigate and avoid cyber threats in the automobile industry, proactive measures are needed because each form of attack poses different risks and problems.

Hacking a Vehicle by Physical Entry

In a history of automotive hacking, several times the vehicle has been physically hacked. Since 1996, On-board Diagnostics 11 (OBD 11) has been a requirement for all automobiles, providing a standard connector for accessing in-vehicle data. The second generation OBD interface, known as OBD11, makes it easier for a car’s Electronic Control Unit(ECU) to communicate with different sensors, engines, and exhaust controls. Diagnostic Trouble Codes(DTCs) are used to record information that the ECU finds in sensor data that is outside of normal ranges. An OBD scanner is used to connect with the vehicle’s ECU through the OBD system, generally via a 16-pin Diagnostic Link Connector(DLC), which is advantageously placed next to the driver’s seat, frequently under the dashboard, and is easily accessible without the use of tools. To avoid illegal connections, authentication during the OBD scanner pairing process is essential. However, remote attacks are problematic because exploitation requires that attackers be nearby the scanner physically. [26]

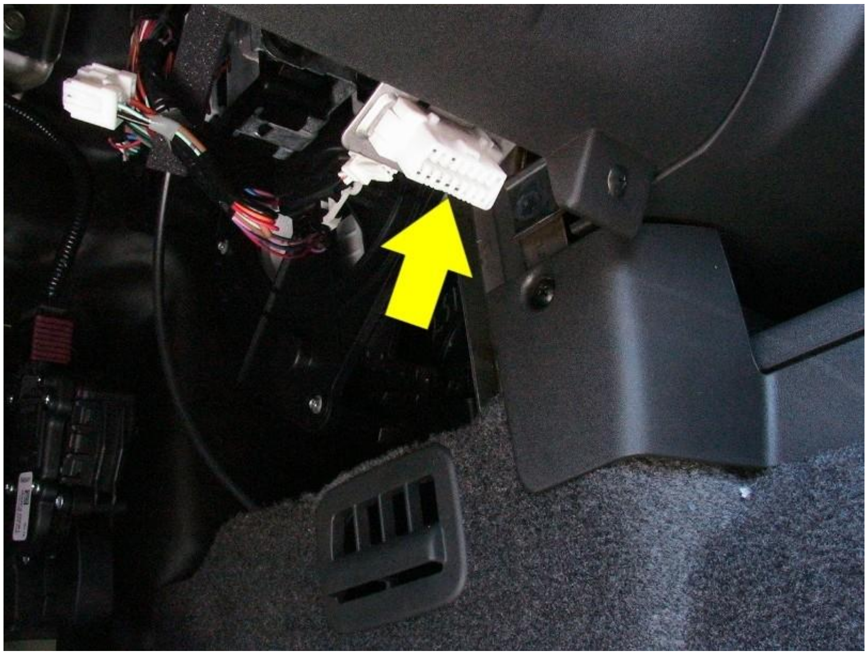

Figure 3: OBD port [27]

In this article, it said that some equipment is needed to cleanly hack a vehicle. The OBD11 port would be the entry point for communication on the CAN system. ICSim, Socketcand, and Kayak tools want to install on Kali Linux for hack a car using OBD port and Kali Linux. [28] To attack the vehicle someone used to USB. They used several types of USB attacks to hack those vehicles. It has the ability to launch attacks, steal important data, and deliver malware. [29]

Keyless Entry

The most vulnerable vehicles to this kind of attack are those with keyless entry systems. “This is because radio transmitters are being sold online that give criminals the ability to spoof keyless systems to gain entry to cars and start them up, “says Walsh. At least 110 vehicles from 27 different manufacturers are currently known to be vulnerable to this form of hacking. In addition, a thief could quickly drive off in your automobile if they were able to hack your keyless entry system. [30] Within a five to twenty meter range, the key fob may communicate with the vehicle. Using Dos attacks and Software Defined Radio, hacker can break into a vehicle by taking advantage of the keyless entry device. [31]

Telematics

According to this website [32], A Telematics Control Unit (TCU), which functions as a bridge in a computer network, is an essential part of linked cars. It connects to numerous systems and allows for internal and external communication utilizing Bluetooth, WiFi, and GSM. Telematics systems collect information from the computer systems of the car, including GPS coordinates, and send it to the manufacturer's computers for analysis. The TCU's GSM interface is frequently targeted during penetration testing of connected automobiles since compromising it can allow access to the vehicle's CAN bus. Understanding how the TCU, Head Unit (HU), and Infotainment System interact is crucial for wireless communication.

Smartphone Access

Hackers may able to access the gadgets you have associated with your connected automobile by hacking into the car itself. Passwords, driving habits, financial information, and credit card numbers are just a few of the details that could be at risk if your system is breached. In order to obtain the owner of an automobile’s personal information, hackers can also use connected car apps. Several instances have occurred when rental car films had unrestricted access to personally identifiable information of its clients. This kind of leak might pose a serious security concern. [31]

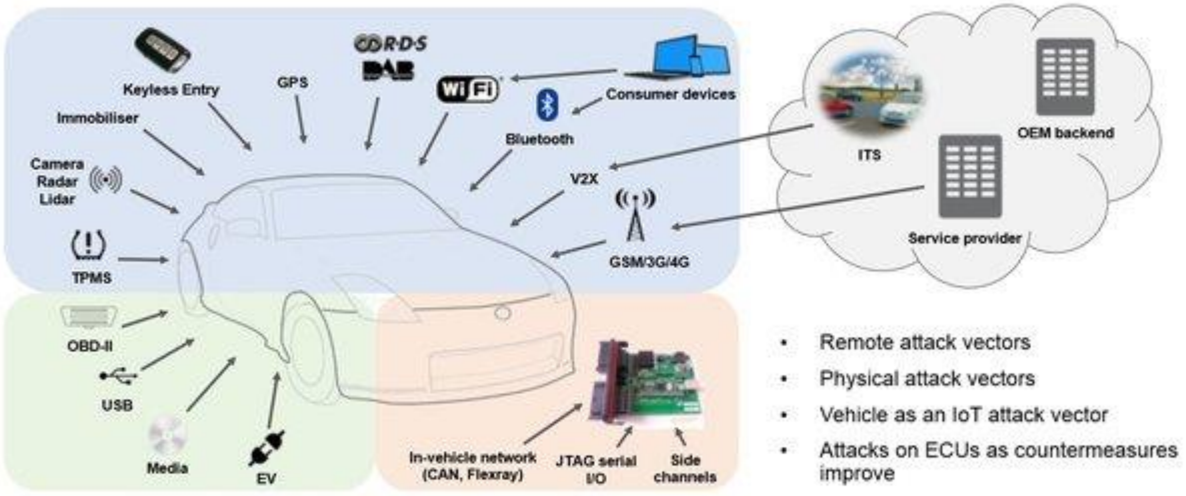

Figure 4: Can a car be hacked [33]

Vulnerabilities in Today’s Automobiles

In our increasingly connected world, vulnerabilities in today’s car have grown to be a serious problem. The potential attack surface for cyber threats has greatly increased as cars have become into advanced computing devices on wheels. The modern automobile has a number of security issues that could endanger drivers, passengers, and data, from software vulnerabilities to insecure communication channels. In order to protect the transportation industry’s future, this introduction looks at the many weaknesses present in modern cars. Vehicles are vulnerable to GPS spoofing and other threats because the automotive industry faces cybersecurity difficulties like software security, weak authentication, and supply chain threats. [34] There are some vulnerabilities have in automobiles.

Door Locks

By the use of a remote control key fob, users of modern cars can easily unlock their vehicles thanks to radio frequency remote keyless systems. The convenience of this innovation, however, comes with security risks because it is vulnerable to signal spoofing, which is the emission of false signals to look like genuine key fob. Notably, documented real-world incidents of signal spoofing-based car hacking exist. Keyless entry security measures may now be quickly bypassed thanks to a method developed by security researcher Silvio Cesare, highlighting how open these systems are to abuse. [35]

In-vehicle infotainment systems

The majority of in-car entertainment systems let users download smartphone apps made by outside developers. The in-car infotainment system may be impact if a mobile app has malware. In this context, it's important to note that the Android market alone offered over a million harmful apps for download in 2013. The most widely used malware applications were FAKEINST and OPFAKE. Without the user's consent, FAKEINST sends SMS messages while disguising itself as a legitimate program. OPFAKE likewise poses as a trustworthy program, but instead of delivering text messages, it opens websites that are infected with malware. [35]

Systems for-on board diagnostics

On-board diagnostics systems provide information about the components of the car and are accessed through the port on the car. However, thieves can also take advantage of this convenience. At the Center for Automotive Embedded Systems Security(CAESS), researchers showed how malware could be installed through the OBD-11 connector to take control of things like wipers and brakes. Tool that may reprogram keys also present concerns because key information can be intercepted by thieves. Professor David Stupples brought up how simple it is for criminals to acquire the information needed for key decoding. [35]

Telematics systems

Vehicle telematics systems perform a variety of tasks, including anti-theft protection and crash alerts. These systems are vulnerable to manipulation by hackers. Attacks can take one of two forms, hackers breaking intro related wireless networks or mechanics injecting malware into the telematics system. The latter situation poses a real threat to vehicle security, according to a research article written by computer experts from the University of Washington and the University of California. [35]

Gatekeeper and Protocol Vulnerability

The lack of an unified "gatekeeper" in today's world of vehicle technology presents a serious challenge. Modern cars' combination of various technologies not only lacks a central authority, but frequently places communication over security.

This leads to protocols that, while enabling smooth device-to-device communication, might not have strong security safeguards. [36]

Additionally, the flaws discovered in autos are similar to those discovered in cell phones and computers, especially focusing on protocol flaws. The risks are greater because bad actors may be able to hack ECU, which govern critical functions like braking and navigation. Such access compromises the security of personal data, including home addresses and phone Ips, as well as car functions. [36]

Financial Impact of Automotive Hacking

Automotive hacking can have a huge financial on automakers and other stakeholders. According to a report by Upstream Auto, an Israeli cybersecurity solutions provider, the automobile sector could lose up to $24 billion over the course of the next five years as a result of cybersecurity on connected cars. The analysis of over 170 occurrences in the " Smart Mobility" space between 2010 to 2018 led to the creation of the research, which reveals that hackers targeted smart mobility vehicles using both direct physical attacks and long-range wireless attacks. These instances revealed flaws in the industry, showing that each new service or connected organization introduces a new attack vector, possibly putting drivers and passengers in danger. Addressing these cybersecurity issues within the automobile industry is necessary due to the swift integration of connected car and the growing complexity of smart mobility services. [37]

Risks and Consequences

Significant privacy and safety issues are posed by automotive hacking, especially as vehicles become increasingly linked. Hackers have access to data, can change controls, steal data, and maybe extort producers. This underlines the urgent need for improved automotive cybersecurity. Vulnerabilities in a vehicle’s software can be exploited to disable safety measures, manipulate acceleration and braking, and even cause accidents. Because a cyberattack might have disastrous results, including loss of vehicle control and risks to passengers and other road users, the security of autonomous vehicles is of the utmost significance. The public’s trust and a safe and widespread deployment of autonomous vehicles depend on ensuring their security. [38]

A data breach at Toyota in February resulted in the exposure of 3.1 million consumers’ personal data. Such occurrences decrease consumer confidence, which lowers sales and marker share. The financial strain on victims can be made worse by hackers who use stolen data for phishing, financial fraud, or ransom. To protect cars, data, and customers from new cyber dangers, manufacturers must invest in strong cybersecurity safeguards. This entails doing vulnerability analyses, executing multi-factor authentication, and encrypting data for secure connections, among other things. Addressing automotive hacking concern is essential for safety, privacy, and consumer trust in the business as automotive technology develops and vehicles become more connected and autonomous. [38] There are some illicit activities are here,

Remote Control Takeover

This worrying position allows hackers to remotely take full control of essential vehicle systems like steering, acceleration, and breaks. This puts other nearby roads users in danger in addition to the occupants within the car. [39]

Data Theft

The vast amounts of personal data that are stored in connected vehicles make them gold mines. This includes vital details like past locations, driving tendencies, and even physiologies data. These sensitive data may be stolen in the event of a successful cyberattack, which would result in serious privacy violations and identity theft. [39]

Innovative Approaches to Industry Challenges

Vehicles are becoming connected and autonomous, placing the automobile industry at the forefront of technological advancement. But these developments also carry with them new difficulties, particularly in the area of cybersecurity. The risk of vehicle hacking increases as cars rely more on data and software. Innovative methods are now being developed in response to this to protect automobiles, safeguard private data, and guarantee the safety of passengers and other road users. The following measures are among those being implemented.

Segmentation and Isolation

To guard against unauthorized access to crucial systems, automakers are building segmented and separated networks inside of cars. As a result, the entire vehicle is protected from compromise in the event of an assault on one subsystems. [40]

Hardware Security Modules (HSMs)

HSMs are included into vehicles to offer authentication, safe key storage, and cryptographic services. They aid in protecting the confidentiality and integrity of data shared between internal and external systems of the vehicle. [40]

Secure Boot

During the startup phase of the car, a function known as Secure Boot checks the legitimacy and integrity of the software and firmware. By doing this, harmful software cannot be installed on vehicle's systems. [40]

Penetration Testing

In-vehicle system vulnerabilities can be found and fixed with regular penetration testing. This proactive strategy assist in identifying security flaws before hackers may take advantage of them. [40]

Ethical hacking and bug bounty programs play a crucial part in today's digitally connected automotive ecosystem. The proactive detection and correction of vulnerabilities in automobile systems is greatly aided by ethical hackers, sometimes known as "white hat" hackers. Through bug bounty programs, these professionals work with automakers and suppliers to find security problems that could otherwise go undetected. [40]

Secure Software Updates

The use of over-the-air(OTA) software update system by automakers enables remote installation of security fixes and feature upgrades for vehicles. This lessens the requirement for in-person dealership visits and guarantees that the autos have the most recent security measures installed. [40]

Encryption

Data transmission between automobiles servers, and external devices must be protected by encryption. By encrypting data, automakers can stop encryption. By encrypting data, automakers can stop listening and illegal access to confidential information. [40]

Intrusion Detection System (IDS)

IDS are used in cars to track network activity and find malicious or suspicious activities. IDS can warn drivers or the vehicle’s systems about potential cyberattacks and start protective steps. [40]

Industry Collaboration and Standards of Automotive Hacking

The coordinated approach and the creation of thorough industry standards are crucial in combating the ongoing danger posed by automotive hacking in the quickly changing field of automotive technology. With modern vehicles becoming more connected and complicated, it is crucial for manufacturers, cybersecurity experts, and regulatory bodies to band together in order to create and implement effective safety measures. UNECE R 155, ISO/SAE 21434 and UNECE WP.29 are some industry collaboration and standards related automotive hacking.

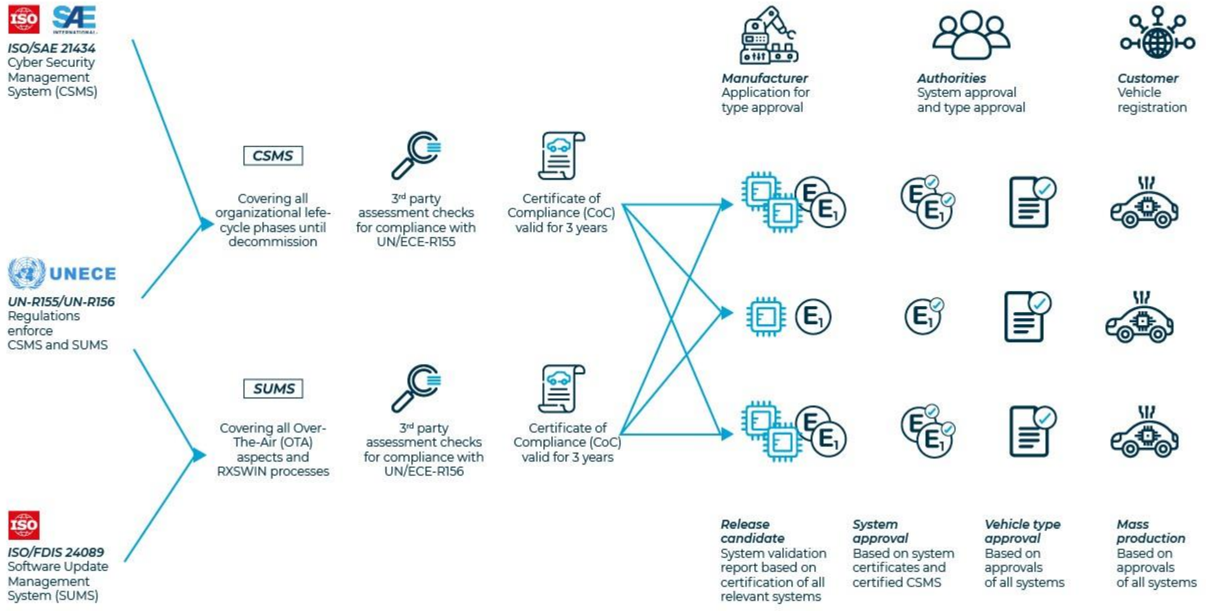
ISO
SAE INTERNATIONAL
ISO/SAE 21434
Cyber Security Management System (CSMS)
UNECE
UN-R155/UN-R156
Regulations enforce CSMS and SUMS
ISO
ISO/FDIS 24089
Software Update Management System (SUMS)
CSMS
Covering all organizational lefe-cycle phases until decommission
3rd party assessment checks for compliance with UN/ECE-R155
Certificate of Compliance (CoC) valid for 3 years
SUMS
Covering all Over-The-Air (OTA) aspects and RXSWIN processes
3rd party assessment checks for compliance with UN/ECE-R156
Certificate of Compliance (CoC) valid for 3 years
Manufacturer
Application for type approval
Authorities
System approval and type approval
Customer
Vehicle registration
E
E1
Release candidate
System validation report based on certification of all relevant systems
System approval
Based on system certificates and certified CSMS
Vehicle type approval
Based on approvals of all systems
Mass production
Based on approvals of all systems

Figure 5: Understanding UN/ECE Regulations NO155. And No.156 [41]

UNECE R 155

UNECE R 155 mandates the adoption of a Cyber Security Management System(CSMS) by all automobile manufacturers to maintain a high standard of safety throughout the whole lifecycle oof a vehicle, including any necessary improvements. It promotes continuing safety system evaluations by acknowledging the dynamic nature of software development and assurance. Additionally, the CSMS makes sure that safety standards are followed throughout the entire supply chain, which is a difficult effort given that vendors presently contribute more than 70% of the software volume. [42]

For complete security to be maintained throughout a vehicle's lifecycle, a Cyber Security Management System is necessary. IT includes monitoring for new vulnerabilities and well-known attacks, risk management to identify and reduce cyber threats, and independent evaluations by recognized testing organizations. Information security becomes a mandated, risk-focused practice when a CSMS is implemented. In order to guarantee long-term security, UNECE R156 requires vehicles to have a Software Management System(SUMS). It creates a legal foundation for "Over-the-Air"(OTA) updates enabling quick, mobile vehicle updates. [42]

ISO/SAE 21434

The new ISO standard has become effective following an extended worldwide conformity process. The engineering specifications for cybersecurity risk management during the idea, development, and post-development phases are governed by ISO/SAE 21434, "Road vehicles-Cybersecurity engineering." [43]

Similar to typical management systems like ISO 27001, the methodology of ISO 21434 asks for the execution of processes and procedures when taking identified risks into account. The standard’s stated goal is to guarantee the safety of all electrical and, especially, data-processing electronic devices for the entirety of a vehicle’s product life cycle, up until its disposal. By doing this, it hopes to establish itself as a reliable, legally enforceable norm for cybersecurity in the automotive industry. [42]

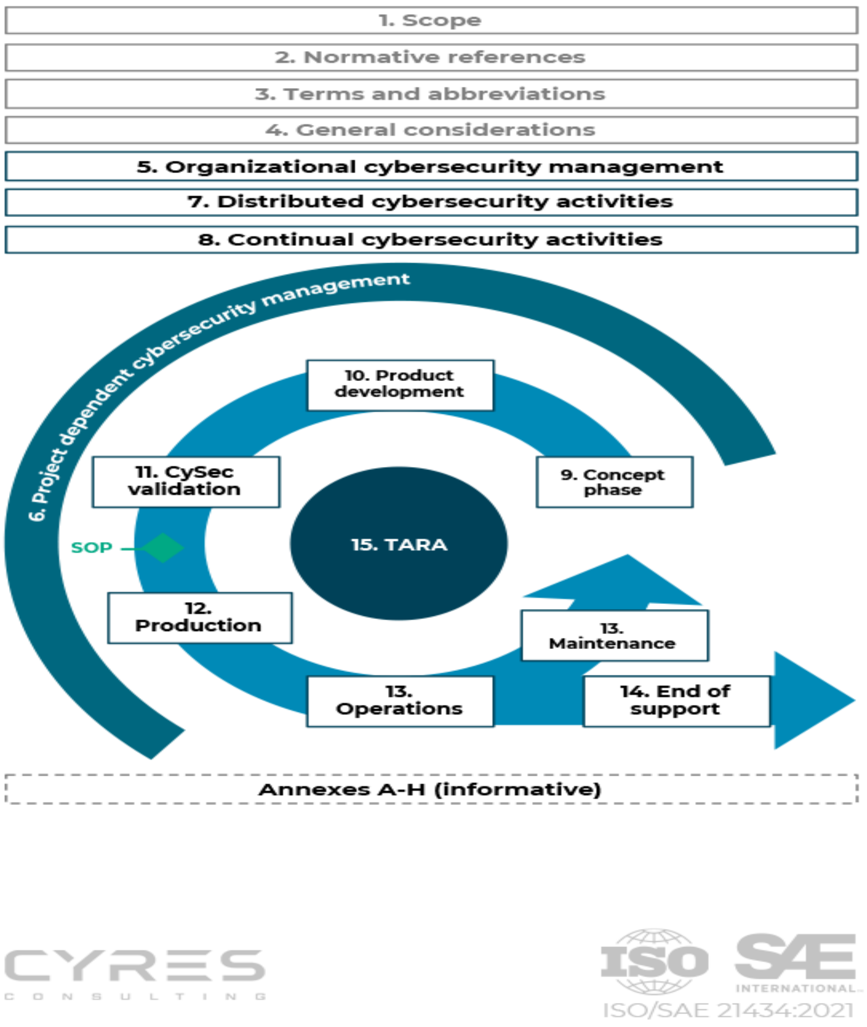
1. Scope
2. Normative references
3. Terms and abbreviations
4. General considerations
5. Organizational cybersecurity management
7. Distributed cybersecurity activities
8. Continual cybersecurity activities
6. Project dependent cybersecurity management
10. Product development
9. Concept phase
11. CySec validation
15. TARA
SOP
12. Production
13. Maintenance
13. Operations
14. End of support
Annexes A-H (informative)
CYRES
CONSULTING
ISO
SAE
INTERNATIONAL
ISO/SAE 21434:2021

Figure 6: ISO/SAE 21434

UNECE WP.29

A global cybersecurity rule to improve connected vehicle security was introduced in July 2020 by WP.29, a unit of the UNECE's Sustainable Transport Division. For new passenger vehicles in the EU and other countries, this rule enforces cybersecurity and Software update standards. To promote safer and more environmentally friendly automobiles, WP.29 attempts to integrate technology. [44]

In order to comply with WP.29's cybersecurity and software update standards, automakers must address vehicle cybersecurity risks, implement security measures throughout the supply chain, and monitor and respond to security incidents. Secure software updates are security incidents. Secure software updates are also required. From January 2021. This legislation will cover the development, production, and post-production phase for passenger car, vans, lorries, busses and light vehicles. [44]

FUTURE DEVELOPMENT IN AUTOMOTIVE HACKING

Cybersecurity is a major be concerned as the automotive sector develops further. The industry provides a fertile environment for innovation as well as new cybersecurity concerns due to the rise of connected automobile, autonomous driving, and interconnected systems. This investigation probes the realm of car hacking, evaluating the dangers and changing security measures in a sector that is constantly being altered by the Internet of Things(IoT), artificial intelligence, and sophisticated telematics.

To solve flaws in its software and supply chain security, the automotive sector is continually developing and adopting new technology. A expanded strategy can also assist in real-time detection and prevention of potential cybersecurity threats. Additionally, it can increase the efficiency of currently in place security measures and lower the likelihood of cybersecurity issues. The adoption of suck a strategy is essential for shielding cars and passengers from the mortal risks posed by hackers. This is crucial now more than ever as the automobile sector develops and adjusts to ne cyber risks. [45] Here are some of the most pressing issues and potential solutions.

The Security of Autonomous Vehicles

Autonomous vehicles must balance cutting-edge technology and traffic safety, therefore their security is of utmost importance. Threats to cybersecurity present particular difficulties that must be overcome if autonomous driving is to be trusted and widely used. Real-time data and advanced algorithms are used to control fully autonomous car. To avoid potential malicious interference and maintain the safety and reliability of autonomous driving systems. It is crucial to ensure the security of sensor data, communication routes, and decision-making. [40]

Supply chain security

In the automobile industry, supply chain security is a major concern. To avoid cyber threats and vulnerabilities, the integrity and safety of parts, software, and communication routes across the supply chain are essential. Strong security measures are required due to the automotive supply chain's complexity and interconnectivity. It is crucial to ensure the dependability of third-party components and to enforce strict security guidelines for all vendors, Proactive security procedures are necessary to protect automobiles from cyber attacks and vulnerabilities given the number of participants. [40]

Data Privacy and Regulations

The automobile sector places a high priority on data privacy and regulation. Consumer confidence and industry integrity both depend n the safeguarding of sensitive data and compliance to changing regulations as vehicles become more linked. Vehicle-generated data analysis and collecting pose significant privacy and ownership issues. It can be difficult to strike a balance between the need for data-driven innovation and the protection of consumer privacy and obedience to data protection laws. [40]

Integration with Smart Infrastructure

A significant advancement in automotive technology is the integration of connected automobiles with smart infrastructure. It improves efficiency, traffic management, and safety. But it also brings up serious issues with data security, system resilience, and cybersecurity, necessitating creative solutions to protect this interconnected environment. It will be difficult to secure the larger ecosystem when automobiles are more closely incorporated into intelligent transportation infrastructure. Securing vehicle-to-infrastructure (V21) communication and guaranteeing the durability of transportation networks are two examples of how to do this. [40]

CONCLUSION

In conclusion, from the early days of physical automobile access to advanced keyless entry and telematics attack, the evolution of automotive hacking has seen considerable advancements. Due to issues with on-board diagnostics and telematics systems, weaknesses in in-car infotainment system, and door lock vulnerabilities, modern vehicles are becoming more and more prone to attack. Significant financial effects are seen by both manufacturers and customers. To combat these dangers, new strategies, industry cooperation, and standards have arisen, placing a focus on cybersecurity and safety. Looking ahead, the future of automotive hacking necessitates constant adaptation and development in security measures as technology progresses, necessitating strong safeguards for the longevity of the sector.

References

[1] "Automotive hacking (Wikipedia)," [Online]. Available: https://en.wikipedia.org/wiki/Automotive_hacking.

[2] "OICA(International Organization of Motor Vehicle Manufacturers)," [Online]. Available: https://www.oica.net/wp-content/uploads/By-country-region-2022.pdf.

[3] "Medium," [Online]. Available: https://medium.com/s/new-world-crime/a-brief-history-of-hacking-internet-connected-cars-and-where-we-go-from-here-5c00f3c8825a.

[4] "Wikipedia," [Online]. Available: https://en.wikipedia.org/wiki/Automotive_hacking#cite_note-4.

[5] "wired," [Online]. Available: https://www.wired.com/2010/03/hacker-bricks-cars/.

[6] S. Tengler, " Forbes (Top 25 Auto Cybersecurity Hacks: Too Many Glass Houses To Be Throwing

Stones)," [Online]. Available: https://www.forbes.com/sites/stevetengler/2020/06/30/top-25-auto-cybersecurity-hacks-too-many-glass-houses-to-be-throwing-stones/?sh=6d93adcd7f65.

[7] "How to hack a car: Phreaked Out (Episode 2)," 29 May 2014. [Online]. Available: https://www.youtube.com/watch?v=3jstaBeXgAs.

[8] "How car are stolen through OBD port theft and key cloning," 11 August 2014. [Online]. Available: https://www.youtube.com/watch?v=dvmSOEKfkug.

[9] "kaspersky (Connected car are noe reality, but are they secure?)," [Online]. Available: https://www.kaspersky.com/about/press-releases/2014_connected-cars-are-now-a-reality-but-are-they-secure.

[10 0] "CBC news(Car hacked on 60 minutes)," 6 February 2015. [Online]. Available: https://www.cbsnews.com/news/car-hacked-on-60-minutes/.

[11] "WIRED (Hackers remotely kill a jeep on the highway- with me in it)," 21 July 2015. [Online]. Available: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[12] A. Shahani, "npr (Tesla Model S Can Be Hacked, And Fixed)," 6 August 2015. [Online]. Available: https://www.npr.org/sections/alltechconsidered/2015/08/06/429907506/tesla-model-s-can-be-hacked-and-fixed-which-is-the-real-news.

[13] "CARANDDRIVER (Researcher: BMW, Mercedes Vulnerable to Remote Unlocking Hack)," 13 August 2015. [Online]. Available: https://www.caranddriver.com/news/a15353272/researcher-bmw-mercedes-vulnerable-to-remote-unlocking-hack/.

[14] J. Pagliery, "CNN BUSINESS (Volswagen hid a car hacking flaw fow years)," 14 August 2015. [Online]. Available: https://money.cnn.com/2015/08/14/technology/volkswagen-car-hacking/.

[15] "Troy Hunt (Controlling vehicle features of Nissan LEAF's across the global via vulnerable APIs)," [Online]. Available: https://www.youtube.com/watch?v=Nt33m7G_42Q.

[16] "BBC NEWS (Mitsubishi Outlander hybrid car alarm 'hacked')," 6 June 2016. [Online]. Available: https://www.bbc.com/news/technology-36444586.

[17] "ADAC," 17 March 2016. [Online]. Available: https://www.youtube.com/watch?v=xHCUpLBGIKQ#action=share.

[18] K. Lin, "MOTORTREND (Hackers That Exposed Jeep Cherokee Security Flaws Wreak More Havoc)," 4 August 2016. [Online]. Available: https://www.motortrend.com/news/hackers-that-exposed-jeep-cherokee-security-flaws-wreak-more-havoc/.

[19] E. Weise, "USA TODAY (Chinese group hacks a Tesla for the second year in a row)," 28 July 2017. [Online]. Available: https://www.usatoday.com/story/tech/2017/07/28/chinese-group-hacks-tesla-second-year-row/518430001/.

[20] L. Armasu, "tom'sHardware (Hyundai 'Blue Link' Vulnerability Allows Thieves To Start Cars Remotely)," 27 April 2017. [Online]. Available: https://www.tomshardware.com/news/hyundai-blue-link-vulnerability-thieves,34248.html.

[21] V. Stykas, "SECLISTS.ORG (Calamp.com Incorrect privilege assignment could lead to full user and vehicle compromise)," 14 May 2018. [Online]. Available: https://seclists.org/fulldisclosure/2018/May/37.

[22] E. G, "atlasVPN (Automotive cyber incidents double in 2019, reaching 188 vulnerabilities)," 6 July 2020. [Online]. Available: https://atlasvpn.com/blog/automotive-cyber-incidents-doubled-in-2019-reaching-188-vulnerabilities.

[23] M. Allan, "Edinburgh News," 13 April 2020. [Online]. Available: https://www.edinburghnews.scotsman.com/lifestyle/cars/serious-security-flaws-expose-popular-ford-and-vw-cars-to-hackers-2537259.

[24] "HCRL (Car Hacking: Attack & Defense Challenge 2020)," [Online]. Available: https://ocslab.hksecurity.net/Datasets/carchallenge2020.

[25] "AIEDGE LABS (Top Automotive Cyberattacks in 2021 & 2022)," [Online]. Available: https://edgelabs.ai/blog/edge-computing-top-cyber-attacks-in-2021-2022-for-the-automotive-industry/.

[26] C. Nguyen, "HCLTech (OBD11 - Security Attention for Automobile)," 16 January 2023. [Online]. Available: https://www.hcltech.com/blogs/obdii-security-attention-automotive.

[27] "OBD port," [Online]. Available: https://www.google.com/url?sa=i&url=http%3A%2F%2Fwww.totalcardiagnostics.com%2Fsupport%2FKnowledgebase%2FArticle%2FView%2F4%2F6%2Fwhere-is-my-cars-obd-port-located-obd2-locator&psig=AOvVaw0dv9eMQYuhO0j34yZsd4gn&ust=1697998480642000&source=images&cd=vfe&op.

[28] Anthony, "Introduction to Car Hacking: The VAN bus," 01 August 2022. [Online]. Available: https://www.offsec.com/offsec/introduction-to-car-hacking-the-can-bus/.

[29] E. Hayden, "TechTarget (USB attacks)," 2019. [Online]. Available: https://www.techtarget.com/searchsecurity/feature/USB-attacks-Big-threats-to-ICS-from-small-devices.

[30] L. Campbell, "Reader's DIggest (5ways hackers can take control of your car)," [Online]. Available: https://www.rd.com/list/ways-hackers-can-take-control-of-your-car/.

[31] F. Ali, "MAKEUSEOF (4 ways your car can be hacked and hot to prevent it)," 19 April 2021. [Online]. Available: https://www.makeuseof.com/ways-your-car-can-be-hacked-prevent-it/.

[32 "The Hitchhiker's Guide to Hacking Connected Cars: ECUs Demystified(Linkdin)," 15 June 2018. [Online]. Available: https://www.linkedin.com/pulse/hitchhikers-guide-hacking-connected-cars-ecus-

] alissa-valentina-knight/.

[33] "Quora," [Online]. Available: https://www.quora.com/Can-a-car-be-hacked.

[34] H. Agarwal, "appknox (Hackers vs. The automotive Industry: Vulnerabilities Identified in Hyundai)," August7 2023. [Online]. Available: https://www.appknox.com/blog/hackers-vs.-the-automotive-industry-vulnerabilities-identified-in-hyundai.

[35] D. Dimow, "INFOSEC (Information Security vulnerabilities of Automobile)," 13 January 2015. [Online]. Available: https://resources.infosecinstitute.com/topics/vulnerabilities/information-security-vulnerabilities-automobiles/.

[36] H. Labus, "HELP NET SECURITY (Modern cars: A growing bundle of security vulnerabilities)," December 14 2021. [Online]. Available: https://www.helpnetsecurity.com/2021/12/14/modern-car-vulnerabilities/.

[37] N. Goud, "Cybersecurity INSIDERS (Auto Industry could loss $24 billion to cyber attacks)," [Online]. Available: https://www.cybersecurity-insiders.com/auto-industry-could-lose-24-billion-to-cyber-attacks/.

[38] S. E, "The Driz Group (Cybersecurity Blog) [Driving on the Edge: The Alarming Rise of Automotive Hacking and the Race to Secure Our Vehicles]," 04 10 2023. [Online]. Available: https://www.drizgroup.com/driz_group_blog/driving-on-the-edge-the-alarming-rise-of-automotive-hacking-and-the-race-to-secure-our-vehicles.

[39] T. Dhiman, "the payments association (Navigating the cyber highway: The growing threat of automotive hacking)," 11 September 2023. [Online]. Available: https://thepaymentsassociation.org/article/navigating-the-cyber-highway-the-growing-threat-of-automotive-hacking/.

[40] "Linkdin (The emergence of automotive hacking: Tips for securing your vehicle)," 11 September 2023. [Online]. Available: https://www.linkedin.com/pulse/emergence-automotive-hacking-tips-securing-your-vehicle/.

[41] "UNderstanding UN/ECE REgulations No.155 and No.156," 11 April 2023. [Online]. Available: https://www.linkedin.com/pulse/understanding-unece-regulations-155-156-pem-motion/.

[42] H. Schmeken, "dqs (Automotive Cyber Security: New mandatory regulations)," 06 December 2022. [Online]. Available: https://www.dqsglobal.com/intl/learn/blog/automotive-cyber-security-new-mandatory-regulations#automotive-cyber-security-neue-verbindliche-vorschriften-chapter05.

[43] "KUGLER MAAG CIE (The ISO/SAE 21434 standard on automotive cyberseurity in effect)," [Online]. Available: https://www.kuglermaag.com/automotive-cybersecurity/welcome-iso-sae-21434/?utm_term=&utm_campaign=GA-PMax-Alle+L%C3%A4nder_EN-Cybersecurity_Training&utm_source=adwords&utm_medium=ppc&hsa_acc=4401108778&hsa_cam

=19826312621&hsa_grp=&hsa_ad=&hsa_src=x&hsa_tg.

[44] "BlackBerry (WP.29 cybersecurity vehicle regulation Compliance)," [Online]. Available: https://blackberry.qnx.com/en/ultimate-guides/wp-29-vehicle-cybersecurity.

[45] J. Hurtado, "PRESCOUTER (Securing the road ahead: The Auto industry's response to car hacking)," May 2023. [Online]. Available: https://www.prescouter.com/2023/05/securing-the-road-ahead-the-auto-industrys-response-to-car-hacking/.

[46] "www.oica.net," [Online]. Available: https://www.oica.net/wp-content/uploads/By-country-region-2022.pdf.