Automobile Hacking

Research · September 2022

DOI: 10.13140/RG.2.2.27333.93925

1 author:

Shehan Franciscu
Sri Lanka Institute of Information Technology
7 PUBLICATIONS **0** CITATIONS

SEE PROFILE

Sri Lanka Institute of Information Technology

Automobile Hacking

Individual Assignment

IE2022 - Introduction to Cyber Security

Submitted by:

Student Registration Number	Student Name
IT20017910	Shehan Franciscu

28.05.2021

Date of submission

Table of Contents

1. **Abstract**
2. **Introduction**
3. **Evolution of Automobile Hacking**
    - **3.1.1. Major incidents**
    - **3.1.2. Most common attack vectors**
    - **3.1.3. What is the impact?**
4. **Future of the Automobile Hacking**
5. **Conclusion**
6. **References**

Abstract

‘**Automobile Hacking**’ is a rising threat in the cyber space and so on social. Modern vehicles have lot of computer-aided circuits/systems for manage the properties of vehicle. These are very important and sensitive parts of the modern automobiles. Because of that automobiles vulnerable to attack by third-party. In this report, I have described, what is automobile hacking?, that is why? , how can it be happen? , who are attacking?, rules and regulations, recent related incidents , existing countermeasures and safeguards for avoid those attacks, hypothetical future trends and finally I have suggested some ideas of my own to protect automobiles from attackers. I have studied and used prior reliable research papers and online sources to gather and align this information.

Introduction

Nowadays, modern vehicles contain lot of on-board circuits and computers. Those computer and circuit systems do very simple and complicated processes in a vehicle. Because of that they become the most valuable and well-developed parts in modern automobiles. Those computer aided systems, processing everything from engine controls to the sound and video entertainment systems. These computers, called Electronic control units (ECU), they paired with each other via multiple networks and communication protocols including the Controller Area Network (CAN). Controller area network is a component for build connections between engine and brake control. As like as there are lot of circuits in a modern vehicle. We called those vehicles as 'Connected auto-mobiles'. That complexity creates more advancements and as well as more malfunctions on vehicles. Those new connected vehicles may be an easy target of an attacker (Hacker). It can be happened via various mediums and methods.

Consumers are becoming more concerned about cyber-attack flaws in wired and self-driving automobiles. According to a new Munich study of nearly 1,500 United States adults, 37% are either somewhat or very serious about the cybersecurity and protection of cars with internet connectivity and automated vehicles. Similarly, 35% were concerned that an influenza, malware, or other silent cyber-attacks could harm or ruin a vehicle's records, equipment, or operating systems . [1].

UNECE WP.29 and ISO/SAE 21434 regulations are active for cyber threats on automobiles.

All above in-car computer systems are open to risky cyber-space. There are so many persons who are looking to get advantages from newest technologies. But it can be via good or bad way. If there are any vulnerability in that technology, it will be a victim of a hacker. Automobile field also a victim in the cyber world. It has been recorded lot of security breaches related to automobiles in past few years. Solutions were found for most of them. But still, cyber activists find more new vulnerabilities in newest vehicles at day by day. Let us see how all of these begun and what is the current position.

❖ Evolution of Automobile hacking

Automobile hacking has a significant history. It already has a 15-year history. Despite the fact that at least 36 million vehicles on the road today are now wired to the web, but auto manufacturers seem did not get that issues too seriously. When whole world focus on Artificial Intelligence(AI) and remotely accessible technologies, largest vehicle manufactures have included these types of technics into their modern vehicles. Such as GPS, ETC, Auto braking systems, more sensitive air bags etc.… Those computer-based systems were able to increase productivity and safety of vehicles. With the addition of those technologies, new path has open to the hackers for the commonweal, steal data or extort ransoms.

Hackers began to focus on engine management technics to control superchargers and fuel injectors around 2002. Tripinnate showed in 2005 that it intercepts or transmits suddenly in-car audio signals using Bluetooth. In 2007, England company Path of Reversal showed hackers how the integrity of in-coach navigation systems could be compromised by sending false road news via FM which would cause cars to re-rout**. [2]** When security researchers reported electronic vulnerability within the concept of the connection car in 2014, the potential for connected vehicles to be hacked became reality. The thinking leadership review 'Risk Perspectives for Connected Vehicles' published by the IET and Knowledge Transfer Network in early 2015 outlined many of the threat cars and their possible results for the primary time. It was partially based on inputs from 50 engineering and technical experts from a variety of fields. The report also examined motives which could lead cybercriminals to focus on the security vulnerabilities of a connected car as a survey of inherent technological vulnerabilities. They included vehicle robbery, data robbery, denial/extort, fraud and the reassignment of vehicle identifiers. In the review of the "Connected Vehicle Risk Perspectives," a number of main challenges are identified if the automotive industry is to produce products that are truly cyber-secure. **[3]**

IET.pdf

- **Major incidents : [4]**

2002 - VW, Audi, Porsche and Ford.

In 2002, a group of teenagers decided to hack their own vehicles. It is a system overwrite, not a hack.

2005 – Few auto brands

Because of a couple of whisperers of Automobiles, Bluetooth could have been hacked as time passed, allowing for the recording of conversations or the uploading of contact information.

2007 - All Brands

The reverse route has hacked a radio feed, and appears to be closing Europe's roads, diverting traffic away from a particular road.

2010 – Web Application has disabled vehicles

In 2010, the first widely publicized vehicle hacking occurred. The vehicles themselves were not hacked in this assault. Regardless, the intruder was prepared to physically disable the vehicles without known of the owners. An internal employee was developed a web application using customers' user credentials to access an internet program that enabled remote access to customer vehicle functions such as the engine immobilizer and thus the horn. The aim of this web application was to allow dealership staff to capture the cars of customers who did not make their loan payments on time. This is classified as unlicensed intrusion into web application. **[5]**

2010 - All Brands

Be grateful for white hat hackers because they do penetration tests for greater good. At this stage, researchers could, among other things, disable the brakes.

2010 & 2011 – CAESS Experimental Analysis

In 2011, the researchers set out to investigate the new vehicle's exterior attack surface and decide if an attack may be launched from a distance.. The infographic represents the various input/output channels on a modern car, each of which represents a possible point of entry for an intruder. As manufacturers continue to attach their cars, the attack surface grows larger. A would-be intruder would find the vehicle's cellular, Bluetooth, and Wi-Fi systems particularly appealing. **[5]**

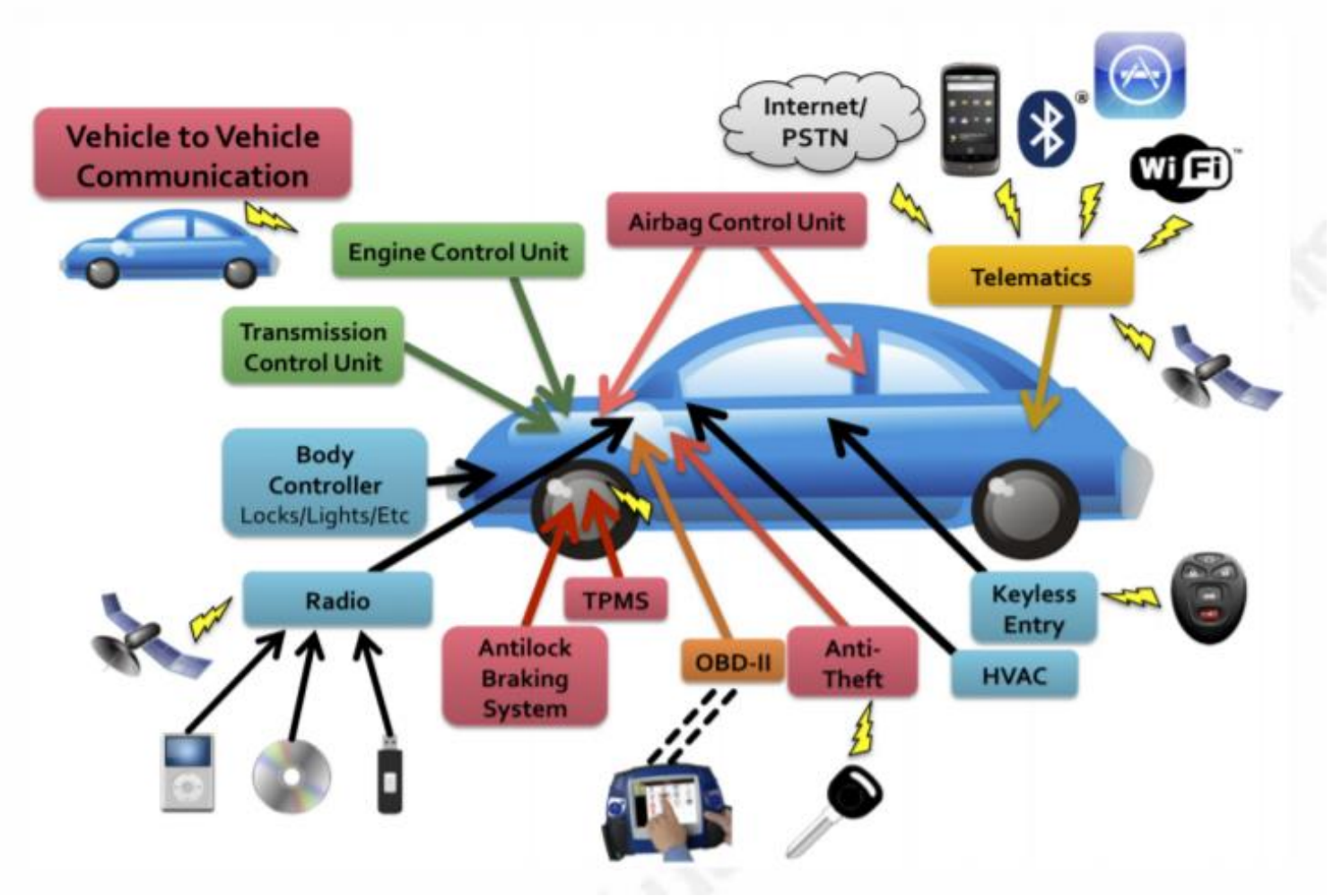


Figure 1 [5]

2013 – Miller and Valasek Physical Hack

Miller and Valasek are DARPA researchers. Their system included a laptop computer that runs Windows XP that was connected to the vehicle's OBD-II port through bunch of connecting wires. That's a proper way to get into a built car. They gained access to the CAN bus of a Toyota Prius by reverse engineering it. However, in the real world, it is not an anonymous attack. [5]

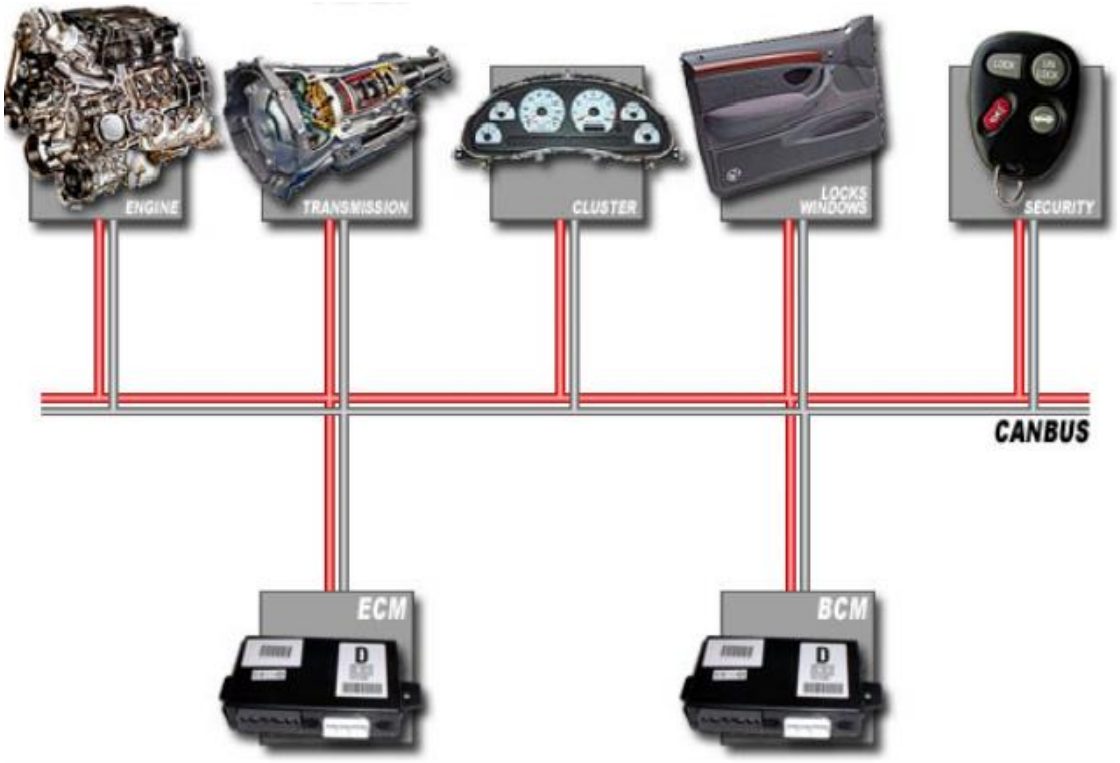


Figure 2 [5]

2014 – Vehicles with Push-Button Start

- This was a foreign, moving goal, similar to FCA. Nonetheless, no recall. “All of those parts are often purchased online for a low price.” The hackers gained full control of the vehicle.
- Kaspersky Labs performs a comprehensive vulnerability assessment of the BMW ownership experience (e.g., websites, apps) and discovers dangerous bugs , like open or start the vehicle.
- “Secure My Car” demonstrates, how breaking a window and plugging something into the service port assists a thief in disabling security and starting vehicles. [4]

2015 – Miller and Valasek Remote Hack

At this point, Miller and Valasek have a true thing. They were remotely attacked and gained access to a 2014 Jeep Cherokee. Moreover, unlike the 2013 attack, Because of the 2015 hack, Fiat Chrysler Automobiles (FCA) was forced to recall nearly 1.4 million cars for a critical security overhaul, and Sprint Corporation was forced to improve the security of its cellular carrier network. A “Kelley Blue Book survey of car buyers” conducted shortly after news of the Jeep Cherokee hack broke revealed that, 72 percent of drivers were " aware of the latest Jeep Cherokee hacking incident ". This is the first phase in automotive hacking that has had an impact on the car industry. [5]

2016 – Nissan, Mitsubishi, FCA

- An attacker took control of a Nissan Leaf in the north of England, including manipulating much of the control panel and extracting position history from the onboard computer.
- The Outlander's car alarm has a bizarre vulnerability: an intruder can disable the vehicle's protection by hacking the vehicle's Wi-Fi.
- Miller and Valasek pursue FCA again, but this time they demonstrate that they can accelerate and steer the vehicle. After, they ironically gain access of the vehicle’s cruise control. [4]

2018 - All Brands

Clamp published, “in 2018, an unsettled server providing open access quite 1.5 million Internet of Things provided by Viper Smart Start, enabling improper vehicle location, password resets, door unlocks, alarm disables, engine starts, and vehicle robberies, just as OEMs thought they had released a safe vehicle.”

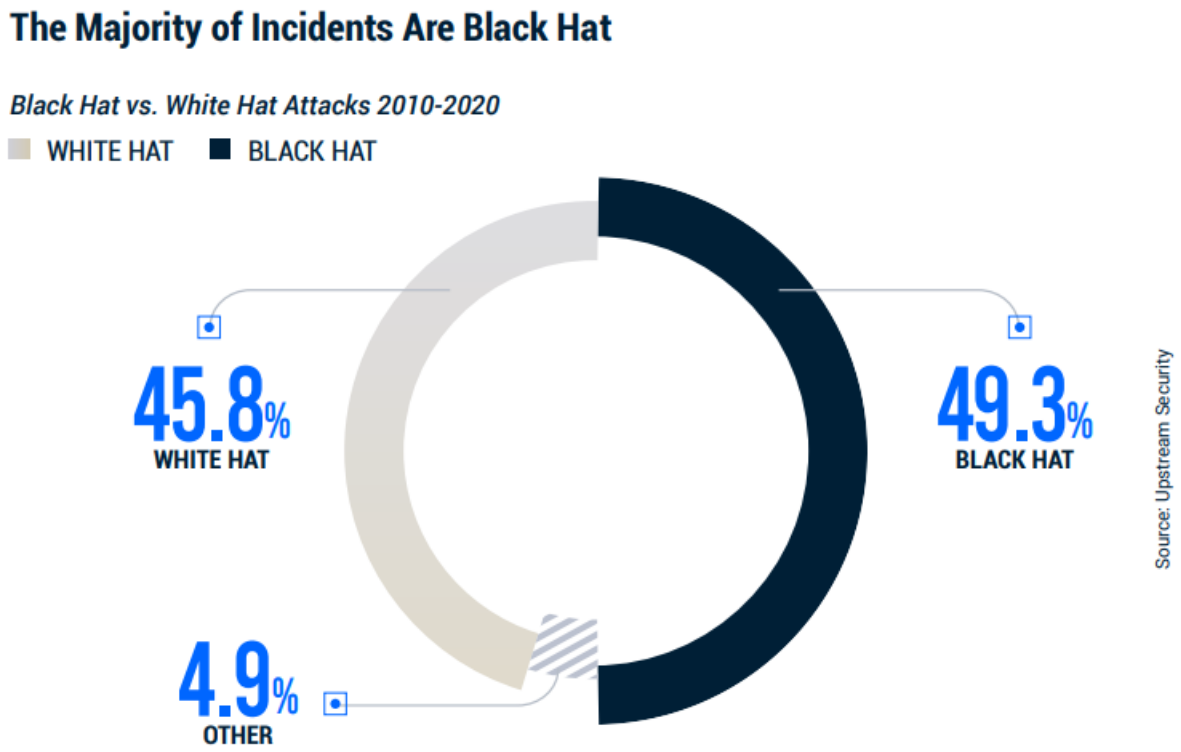
2021 – Honda Manufacturer

“Honda may confirm that a cyber-attack occurred on the Honda network,” a Honda executive officer stated in a press release. It went on to say that the problem was interfering with its computer servers access capability, send email, and use other computer infrastructures. “Efforts are being made to reduce the effect and restore full functionality of manufacturing, distribution, and growth activities.” The company, which manufactures motorcycles, cars, generators, and lawnmowers, among other things, stated that “ one of its internal servers was attacked from the outside”. It went on to say that “ the virus had spread across its network ” but gave no detailed information. [6]


TOP 2020 CYBER INCIDENTS
JANUARY
FEBRUARY
APRIL
MAY
JUNE
AUGUST
4,118 vehicles were stolen in India with cheap electronic devices that enabled the thieves to bypass the engine control module, unlock the vehicle, start the engine, and access the vehicles' computer[21].
A Mobileye 630 PRO and Tesla Model X hack fooled the ADAS and autopilot systems to trigger the brakes and steer into oncoming traffic[22].
19 vulnerabilities were found in a Mercedes-Benz E-Class car, allowing hackers to control the vehicle remotely, including opening its doors and starting the engine[23].
Hackers took full control of an OEM's corporate network by reverse-engineering a vehicle's TCU and using the telematics connection to infiltrate the network[24].
Hackers found passwords and API tokens for Daimler's internal systems after source code of a connected car component was made publicly available[25].
Hackers publicly offered to sell car rental information of 3.5 million Zoomcar users on the dark web[26].
Toll Group, an Australian transportation fleet, was hit with a ransomware attack for the second time in 2020, affecting 1,000 servers and 40,000 employees[27].
Honda stopped production in a number of its plants after its networks in Europe and Japan were attacked with the Snake ransomware[28].
More than 300 vulnerabilities were found in over 40 ECUs developed by 10 Tier-1 companies and OEMs[29].
A hacker was able to gain control over Tesla's entire connected vehicle fleet by exploiting a vulnerability in the OEM's server-side mechanism[30].

Figure 3 [7]

Who is attacking?



In order to identify and avoid attacks, organizations must first consider the people behind them. Hackers are commonly classified into two types: White Hat and **Black Hat**.

White Hat hackers, who are mostly do research, don't typically have malicious intent. According to Up stream's study, black hat hackers was responsible for 49.3 percent of public events from 2010 to 2020. The report also covers events that occurred as a consequence of business operations in which private information was inadvertently released or discovered by customers. Upstream performed the analysis.

The result is cyberattacking and black-hat attacks in the IT domain. In-depth associated with black hat attacks on vital OT infrastructure, such as hospitals, power plants, and government buildings. In September 2020, a patient died as a result of a cyber-attack on a German hospital. More than 1,500 software bugs have been identified to Uber's bug bounty program. In January 2020, Tesla offered 1 million US dollars and a Tesla as a bug bounty incentive, setting a new high in bug bounty programs [7].

In recent years, the number of companies running bug bounty programs has grown, including Tesla, GM, Ford, FCA, Daimler, and others. The number of car-sharing services, such as Uber, has also risen in recent years.

To gain access to utilities, hackers are searching for ways to circumvent protection measures. Although White-hat hackers may not be intending maliciously, they can reveal vulnerabilities. "Gray-hat" hackers who hack for personal gain rather than malicious gain can also be dangerous. “A hacker reverses engineered BMW's ConnectedDrive software in June 2020 to build an open-source app that retrieves real-time vehicle charging information. In December 2019, a gray-hat hacker used an Arduino computer to build an Android application that added features to multiple Mercedes vehicle models by injecting CAN messages” [4].
Users can use the app to monitor door locks and display custom text on the instrument cluster display.

Insurance

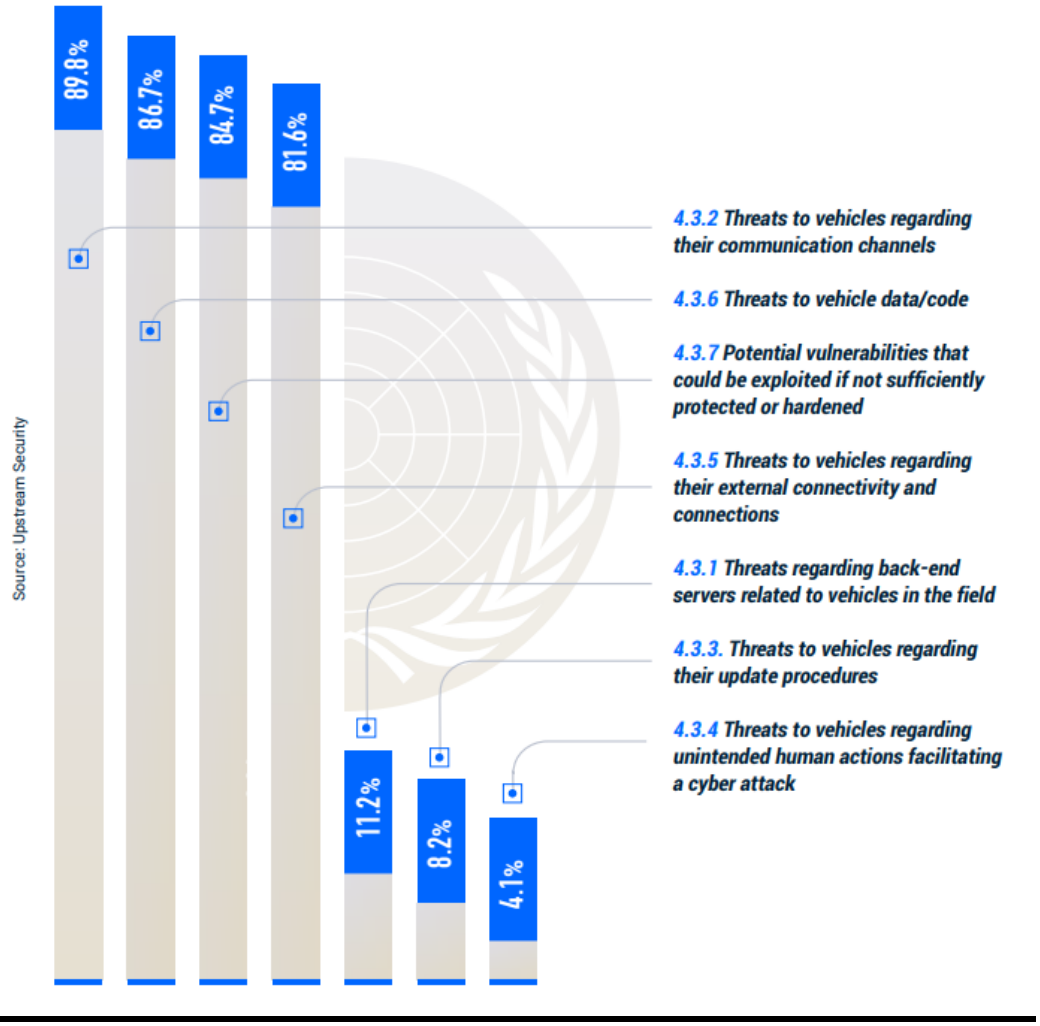
Auto insurance industry is worth 200 billion of US dollars. Insurance firms may identify locations, vehicle types, component susceptibility, and other factors are more vulnerable to cyber-attacks. Dash cam footage is sometimes used as evidence of insurance cases to prove fraud, vandalism, or injuries. Insurance firms also use odometer readings to calculate a driver's mileage and therefore the cost of insuring the car. “A hacker was able to edit the metadata associated with dash cam videos, including the logged data and location, and even replace the video itself, in July 2020” [7].

Rules and Regulations

Automotive cybersecurity is still a developing area. Traditional automotive safety and security legislation and guidelines did not adequately address cyber risks associated with modern-day connected vehicles. The number of cyber-related automotive vulnerabilities is predicted to increase when connected cars grow. To mitigate the anticipated increase in cyber-attacks on connected vehicles, governmental agencies and an effort has been made by independent standardization bodies to require increased entrenched cybersecurity measures from OEMs, component and software manufacturers, and mobility service providers [7].

WP.29

'The World Forum for Harmonization of Vehicle Regulations of the United Nations Economic Commission for Europe' requires that policies be applied across four distinct disciplines. Millions of vehicles worldwide are expected to be affected by the latest legislation. The regulations essentially make safety a mandatory component of future connected vehicles. The first UNecE WP29 is concerned with uniform provisions for the approval of vehicle software updates. The second governs vehicle software update and software update procedures (SUMS). The third section is concerned with cybersecurity and cybersecurity management systems (CSMS) The fourth focuses on the current passenger car demand in the ten largest WP29-regulated countries [7].

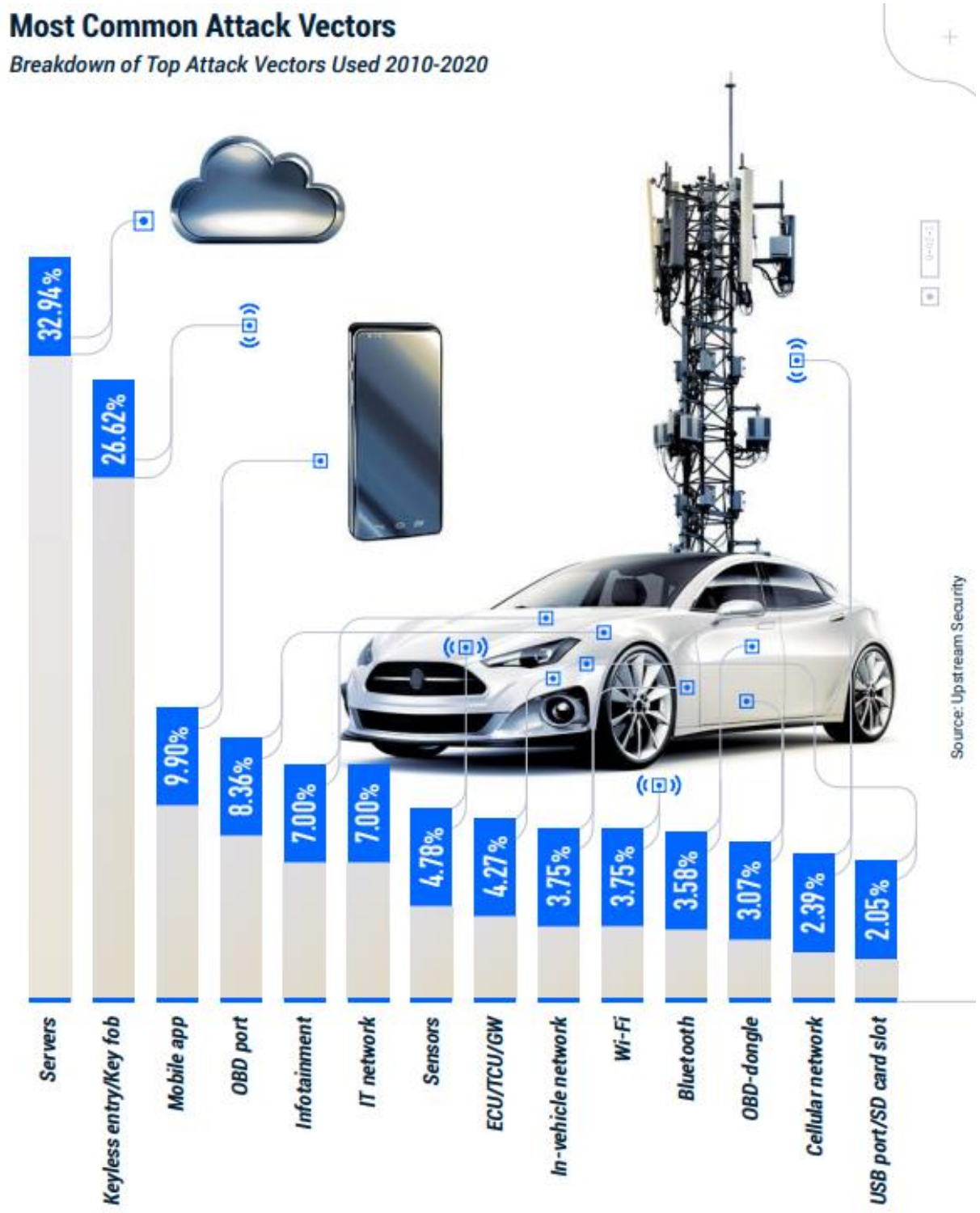


ISO/SAE 21434

SAE International and ISO set the industry standards related to automobile cyber security to address the issue. “The standard was specifically developed to ensure the safety and security of the ultimate road-user/driver. It establishes cybersecurity as an integral element of engineering throughout the lifecycle of a vehicle. It was created using four main working groups focusing on risk management, product development, production, operation, maintenance, maintenance and decommissioning, and a process overview. It calls for effective methods of lessons learned, training, and communication for automotive cybersecurity related to the standard” [7].

Most common attack vectors

Attack vectors are the methods used by attackers to get control of vehicles. One attack incident may contain several attack vectors. This is a graph from Upstream security 2021 report which display most popular attack vectors analyzing incidents since 2010.



• Server attacks

Server attacks can be directed at a variety of servers, including telematics command-and-control servers, database servers, web servers, and others. These attacks are remote and long-distance, meaning that hackers don’t need to physically connect with the vehicle .
Since the OBD port was introduced in the 1990s, vehicles have been vulnerable to cyber-attack since they gave access to management systems for the vehicles. However, it was hard to hack a vehicle at the time that involved costly technology, direct physical access and proprietary software [8].

In April 2020, ‘Pen Test Partners’ researchers warned of the dangers of a server attack until they were able to seize complete control of the company network from the TCU [9].
After messing with a vehicle's TCU, the researchers discovered that they could use the telematics link to hack the company network and gain complete control of the back-end servers using admin credentials. In their study, researchers could've used network rights to carry out lateral movement and observe thousands of automobiles by having access to the telematics server. The hacker gained access to Tesla's network by exploiting a flaw in To and discovered it to be a repository of server images. [10]

• Keyless entry

Most keyless entry vehicles also have keyless start technology, which allows you to start your car's engine and drive away wirelessly. ‘Thatcham research’ examined the safety features of 13 new cars in March 2020 and discovered that seven of them already had bugs in their entry scheme. Security holes or glitches in software may be exploited by hackers. 4 of the vehicles failed the ThatchAm relay theft tests. [11] “A cryptographic algorithm in key fobs employed by major OEMs in many cars, allowing hackers to clone the keys and steal the cars” [12].

Several flaws were discovered in 2020 with the keyless entry devices that allow hackers to open secured doors simply. In March 2020, researchers noticed that the HR-V 2017 remote keyless device delivers an equivalent RF signal for each door - open request. Open request. In July 2020, a researcher discovered a fault in the NFC Tesla Model 3 [7].

Researchers and white-hat hackers conduct keyless entry attacks. A Bulgarian technology firm marketed items matching old Nintendo Game Boys for £20,00043 in July 2020. The devices were marketed to car thieves as "advanced locksmith tools," and they were used to unlock car doors by catching wireless key signals and acting as a responder that the car recognized as a licensed remote.

• Mobile applications

In the automotive industry, smartphone devices are commonly used. In August 2020, Google announced that their service, Android Auto, would be available in more than 100 million cars "in the coming months." [13] Any vulnerabilities or bugs in the operation of a mobile app can lead to malicious manipulation and serious damage. Google and Apple, as well as other firms, are attempting to force their inventions through the door. [14]

“A car owner in China discovered a bug in Tesla's app in August 2020, which displayed five cars in Europe instead of his own vehicle. White-hat hackers discovered alarming vulnerabilities in mobile apps in 2020. Mobile apps were the third most widely used attack vector between 2010 and 2020. These bugs may be used to launch large attacks that jeopardize critical information and, as a result, the safety of all road users.” [7]

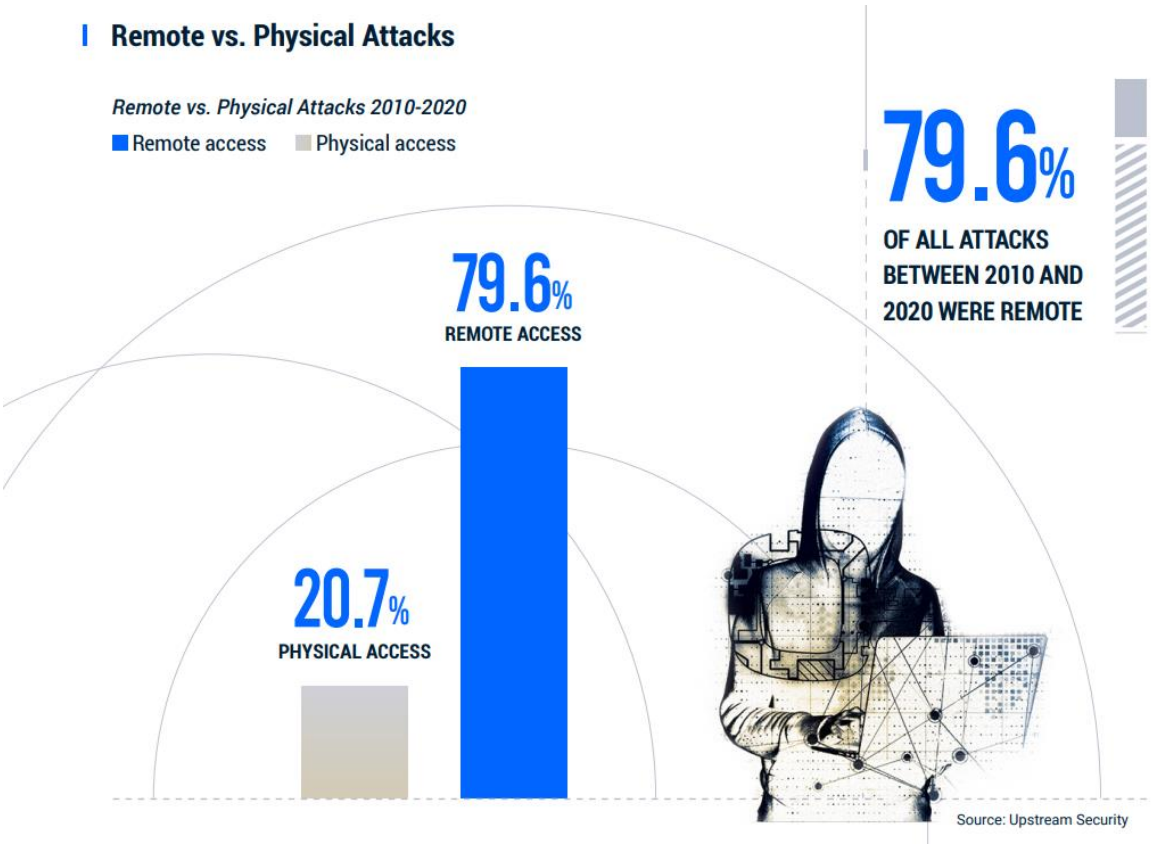


Figure 4 [7]

The vast majority of automotive cyber-attacks are categorized as either remote or physical. Physical attacks need an attacker to make physical contact with the vehicle in order to hack it. Remote attacks are often short-range and can be performed from a few steps away or from anywhere in the world. For example, in July 2020, Tesla's battery management system was retrofitted by a hacker and improved hardware, which might boost the capacity of the vehicle. In January 2020, hackers created a desktop adaption connected with the Tesla servers and carried out activities remotely using Tesla's Mobile API [7].

What is the impact?

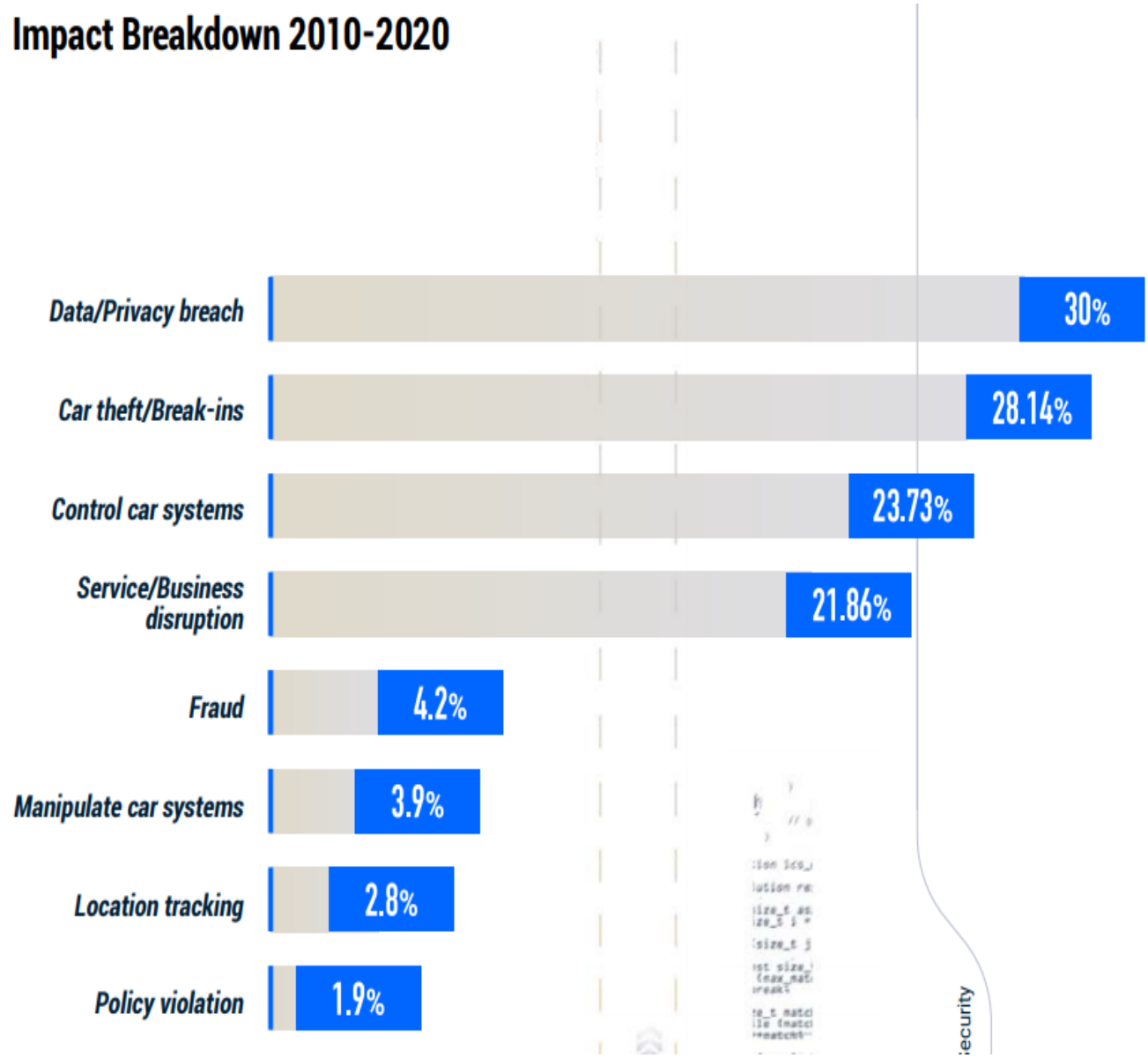


Figure 5 [7]

The effect of an attack refers to the outcome of the attack. Many cyber events can have a variety of effects on the target. The following map shows the impacts of automobile cyber attacks between 2010 and 2020 that 30 percent of occurrences have involved infringed data and privacy, while break-ins and theft of cars accounted for 28.14% [7].

• Data and Privacy breaches

“In 2020, the average cost of a data breach was USD 3.86 million”. [15] In this sector, the average time to detect and contain a violation was 9 months. Hackers usually exploit data in order to sell it for a profit. A shocking case was released in August 2020, in which Departments of Motor Vehicles across the United States sold drivers' personal details. According to reports, the California DMV alone made USD 50 million per year from the selling of this data. [7]

In August 2020, a marketplace inside dark web offered lots of personal data points belonging to French motorists for Euro 10 per identity. The personal details of 3.5 million Zoom car users have been made public.

• Car theft & Break-ins

Car robberies, which accounted for 28 percent of all accidents in 2020, were one of the most significant effects of cyber incidents over the last decade. Car theft is a thriving "market" for criminals, with increasing numbers registered globally. In 2020, car thefts in the United Kingdom increased by 60%. [16] A gang of robbers in India was apprehended in September 2020 for robbing over 100 vehicles using electronic devices. “Two Toyota Tacoma trucks and a Toyota 4Runner truck were stolen from Canadian driveways in January 2020 after hackers allegedly reprogrammed the vehicles' keyless push start ignition.” According to a February 2020 survey, car-sharing apps were also used to steal vehicles in 2020, with 75 of the 200 auto thefts reported to authorities in Washington, D.C. using the car-sharing app. Get out there and rent out their personal vehicles to augment their profits. [7] .

Figure 6 [7]

- **Control & Manipulate Car Functions**

Researchers discovered 19 security flaws in a Mercedes-Benz connected automobile in February 2020. They were able to obtain access to the car's back-end servers, allowing them to remotely track the vehicle. A hacker installed a video game on a Mercedes W203's infotainment device in October 2020 and programmed various controls inside the car to improve his gaming experience. According to experts, other attacks highlighted very severe threats that could have disastrous consequences. The findings were published in the journal Cybersecurity Week.

- **Financial Damage**

Automotive cyber-attacks can have both direct and indirect financial ramifications, many of which are severe. Direct expenses include recalls, manufacturing shutdowns, ransomware fees, and stolen automobiles or accounts. Due to a ransomware attack on its networks in Europe and Japan, Honda was forced to cease production at some of its operations in June 2020. A ransomware attack reached 1,000 servers of an Australian business in February 2020 [7].

The same company was hit with another ransomware attack in May 2020, prompting it to pack up a range of its IT systems. Hidden expenses include stolen trade secrets, reputation damage, and pirated vehicle updates and services. After copying 14,000 data, including product prototypes, to his own laptop, a former Google engineer who worked on the company's autonomous vehicle division pleaded guilty to stealing trade secrets in August 2020. He started his own firm, which was bought out by Uber, prompting Google to sue Uber in 2017 on the basis that Uber had acquired the prior engineer's company in order to retrieve the stolen materials. In July 2020, it was announced that Tesla has filed a lawsuit against EV company starter Rivian and four former workers for allegedly obtaining trade secrets via new personnel. Brand image damage has a direct influence on sales, albeit this is often difficult to quantify. According to a 2020 report, 84 percent Buyers would not order another car from a retailer if their records had been infected by a hack in the previous year [17] .

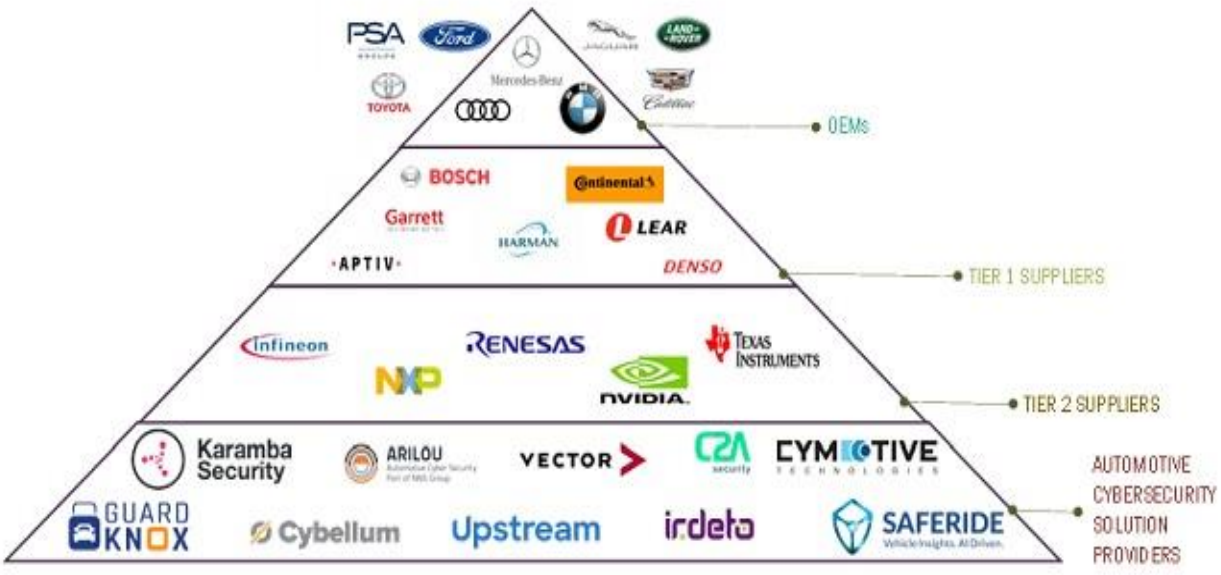


Figure 7 [18]

❖ Future of the Automobile Hacking

According to a new report by Uswitch, "cyber-attacks on connected cars have risen by 99 percent in 2019". The "online and telephone comparison and switching service" has established 4 major methods in which cars are often hacked, ranging from app flaws & data theft to keyless auto theft and even remote vehicle control [7].

Currently, approximately 67 percent of all new vehicles sold are linked in some way, but that figure is projected to increase to 100 percent by 2026, implying that vulnerabilities must be minimized. Automobile cybersecurity has been identified as vital by stakeholders in the automotive industry, including OEMs and external regulatory organizations. As a result, the automotive cybersecurity market is likely to increase significantly, with McKinsey estimating a leap from 4.9 billion USD in 2020 to 9.7 billion USD by 2030 [18].

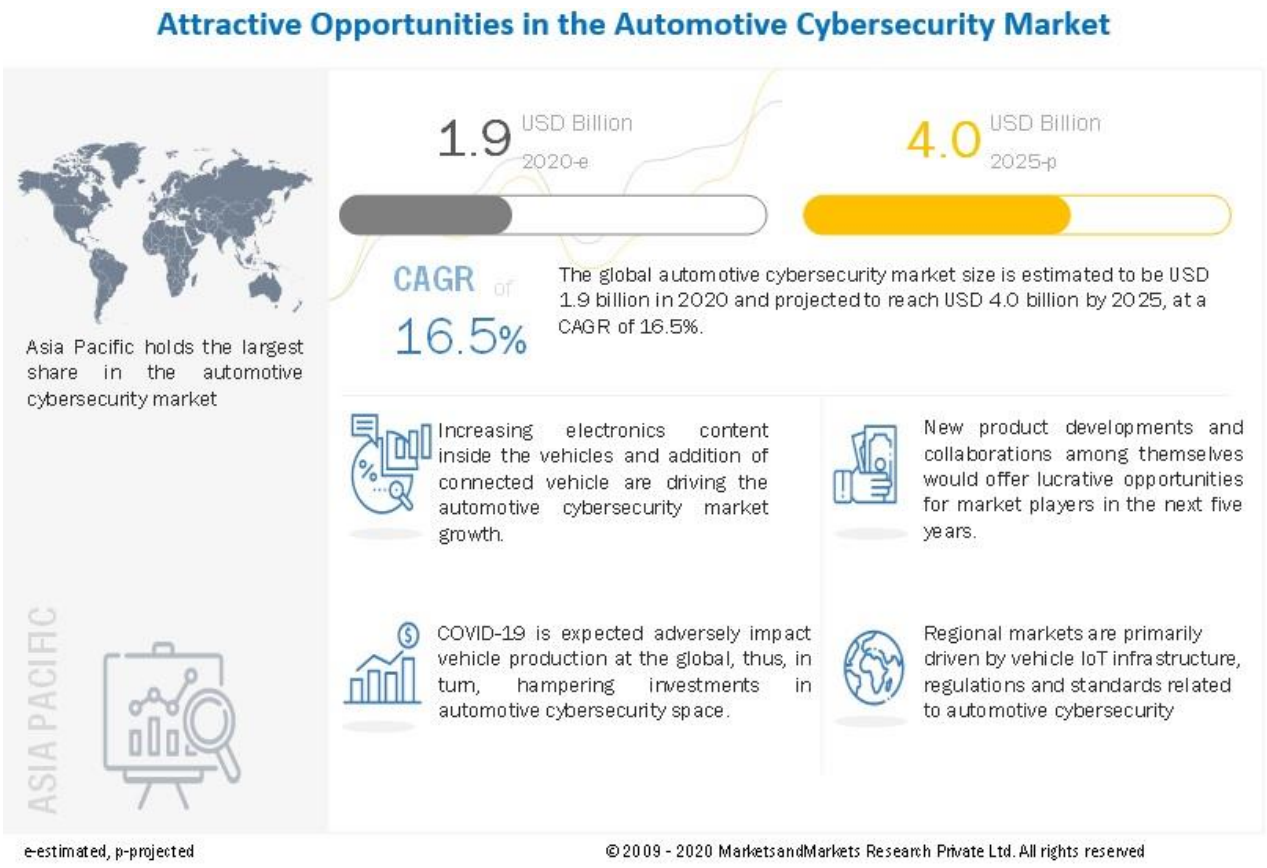
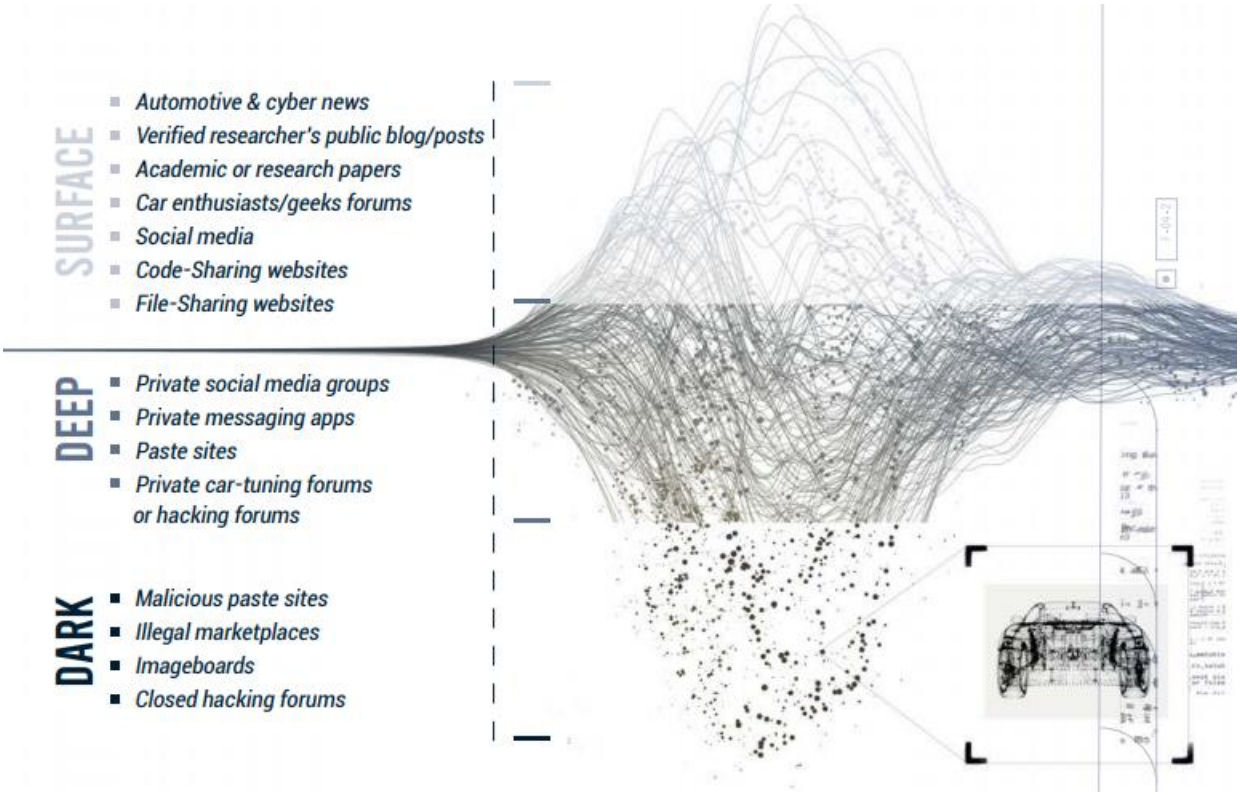


Figure 8 [19]

Deep web and dark web activities.

Deep web material is not publicly available via conventional browsers and search engine indexed. Links to the dark web involves anonymous forums that require registration (or even personal vouching). In May 2020, a hacker gained access to the entire contents of a GitLab server belonging to corporate email provider Daimler and shared it on various file-sharing sites. The story was first shared on the hacker Telegram channel, but it was widely publicized a day later on prominent tech sites such as ZDNet. The server housed 580 repositories for the component, which included photographs, code, comprehensive documentation, and development environments . [7]



Within the deep and dark web, there are various ways to interact with content and other users. Automotive-related material can be found in forums, marketplaces, chat apps, and paste pages on the deep and dark web.

Many vehicles related cyber threats have been discovered and addressed on the deep and dark web, and they may constitute a significant portion of potential cyber threats to the automobile industry. as well as:

•Infotainment hacking, CAN-bus reverse engineering, chip tuning, and program hacks or unauthorized upgrades

•The sale or release of OEM-related information and credentials obtained via data breaches.

•Discussions and sales of equipment for vehicle theft or alteration, such as key signal grabbers, key-fob programmers, GPS jammers, radar detectors, and other similar products.

•Hacking or theft involving car-sharing or ride-sharing accounts •Sale of bogus driver's licenses or auto insurance

Solutions:

• Security by design

Security by design involves thinking about a component's or software's security from the start. This is often accomplished by ensuring that all vehicle parts are designed, constructed, and tested for security flaws, and that any dangers detected are neutralized. While original equipment manufacturers (OEMs) are solely accountable for vehicle defense, all vendors in the supply chain must also follow security-by-design activities. According to the UNECE handout for the WP.29 regulation, cybersecurity measures must be implemented across 4 disciplines, with one specifically requiring " Securing vehicles by design to mitigate risks along the value chain. " [19]

• Implementing a Multi-Layered Cybersecurity Solution

In IT and enterprise security, the need for multi-layered security is well known. Companies should increase their investments in perimeter protection, end-point solutions, cloud security, internal segmentation technology, and other technologies since networks are subject to an expanding number of attack vectors.

- **Developing an efficient VSOC**

Many large organizations now use Security Operations Centers (SOCs) to manage Information Technology networks. As a result of the increased sophistication and sophistication of cyberattacks targeting to safeguard cars, facilities, fleets, and road users, OEMs must construct integrated vehicle SOCs (or VOCs) to track, identify, and respond to cyber occurrences. A VSOC, also known as a "car SOC," "mobility SOC," or "automotive SOC, allows cybersecurity for the post-production process and can play a significant part in assuring the safety of connected vehicles and the smart mobility ecosystem, allowing businesses to track their entire networks and vehicles in real-time **[7]**.

- **Tracking cyber threats through automotive-specific threat intelligence**

OEMs, Tier 1 and 2 vendors, and mobility service providers can track threat intelligence and supplement threat identification with data from external sources. An advanced threat feed that includes monitoring cyber incidents discovered on the surface web, deep web, and dark web will offer OEMs with a comprehensive picture of their cyber-related risks [7].

Conclusion

Automobiles have a significant impact on the lives of many people. Suppliers are now held accountable by the general public as a result of numerous important advancements in the field of vehicle device safety in recent years. People are becoming increasingly aware of the serious ramifications of car security weaknesses in the real world, which could be a catalyst for change. The problem is profound and complex, and the answer is neither simple nor inexpensive. The time has come, though, for manufacturers to stop patching security holes and begin creating secure systems from the ground up.

Here are some suggested solutions, countermeasures or mitigation methods for automotive related cyber - attacks.

- To deter auto thieves, use steering or wheel locks, as well as other physical deterrents. It is more valuable for avoid physical attacks.

- Maintain the software in your vehicle by downloading any security patches or new upgrades as soon as they are available. Think of software upgrades as a way to stay one step ahead of cybercriminals. Keep it in your best practices list.

- Only install mobile applications from the verified sources. They are more likely to be trustworthy since they have been evaluated to guarantee that they adhere to quality and data security standards.

- Be cautious about app permissions. A red flag is an app that requests access to data that is unrelated to its purpose.

- Remove all personal information from an automobile before selling it, to avoid passing personal information on to the future owner. If you missed this step, it is like, have been opened a door for attacker by your hands.

- After installing a mobile app, check the performance of your phone on a regular basis. Malicious applications appear to rapidly drain the battery since they operate in the background unnoticed. If left unchecked, this might become a major issue once hooked it to your vehicle.

Keep update with new technology and technical news can be a real help to avoid been attack by bad hacker. Any technology gives us to lots of benefits, but all of them embed with high - risky vulnerabilities which open gate to dangerous cyber – space. Always, Risk is yours !!!

- **References**

[1] "Munchire," [Online]. Available: https://www.munichre.com/hsb/en/press-and-publications/press-releases/2021/2021-04-06-cyber-car-tech-survey.html. [Accessed 2021].

[2] R. Ferguson, "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. [Accessed 2021].

[3] F. Persson, "Information security risk review and analysis," 2017.

[4] S. Tengler, "FORBES," 2020. [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=1c0e02c37f65. [Accessed 2021].

[5] R. Currie, "Developments in Car Hacking," SANS, 2015.

[6] J. Tidy, "BBC," 2021. [Online]. Available: https://www.bbc.com/news/technology-52982427. [Accessed 2021].

[7] U. SECURITY, "GLOBAL AUTOMOTIVE CYBERSECURITY REPORT 2021," UPSTREAM.AUTO.

[8] "upstream.auto," [Online]. Available: https://upstream.auto/research/automotive-cybersecurity/?id=4690. [Accessed 2021].

[9] "upstream.auto," [Online]. Available: https://www.upstream.auto/research/automotive-cybersecurity/?id=5520. [Accessed 2021].

[10] "upstream.auto," [Online]. Available: https://www.upstream.auto/research/automotive-cybersecurity/?id=7160. [Accessed 2021].

[11] "upstream.auto," [Online]. Available: https://www.upstream.auto/research/automotive-cybersecurity/?id=5180. [Accessed 2021].

[12] "upstream.auto," [Online]. Available: https://www.upstream.auto/research/automotive-cybersecurity/?id=5280. [Accessed 2021].

[13] "automotive-iq," [Online]. Available: https://www.automotive-iq.com/autonomous-drive/articles/how-apps-are-changing-the-driving-experience. [Accessed 2021].

[14] "buick," [Online]. Available: https://www.buick.com/discover/connectivity/alexa-built-in. [Accessed 2021].

[15] "IBM," [Online]. Available: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/. [Accessed 2021].

[16] "dailymail," [Online]. Available: https://www.dailymail.co.uk/news/article-8244625/Car-theft-rockets-60-cent-parts-UK-motorists-face-greater-risk-despite-lockdown.html. [Accessed 2021].

[17] "Autonews," [Online]. Available: https://www.autonews.com/article/20160620/OEM06/306209973/dealers-vulnerable-to-hackers-survey-warns. [Accessed 2021].

[18] "gsaglobal," [Online]. Available: https://www.gsaglobal.org/wp-content/uploads/2020/03/Cybersecurity-in-automotive-Mastering-the-challenge.pdf. [Accessed 2021].

[19] "unece," [Online]. Available: http://www.unece.org/info/media/presscurrent-press-h/transport/2020/un-regulations-on-cybersecurity-and-software-updates-to-pave-the-way-for-mass-roll-out-of-connected-vehicles/doc.html. [Accessed 2021].

[20] Petit, J. & Shladover, S. E., "Research Gate," 2015. [Online]. Available: https://www.researchgate.net/publication/266780575_Potential_Cyberattacks_on_Automated_Vehicles.

[21] "USA today," 2018. [Online]. Available: https://www.usatoday.com/story/money/cars/2018/01/30/car-renters-beware-bluetooth-use-can-reveal-your-private-data/1080225001/. [Accessed 2021].

[22] J. Hayes, 2020. [Online]. Available: https://eandt.theiet.org/content/articles/2020/03/hackers-under-the-hood/. [Accessed 2021].

[23] "autonews," [Online]. Available: https://www.autonews.com/article/20160620/OEM06/306209973/dealers-vulnerable-to-hackers-survey-warns. [Accessed 2021].

[24] "techcrunch," [Online]. Available: https://techcrunch.com/2020/08/11/android-auto-gets-google-calendar-integration. [Accessed 2021].

[25] "swindonadvertiser," [Online]. Available: https://www.swindonadvertiser.co.uk/news/18274808.police-issue-warning-thieves-steal-keyless-entry-cars/. [Accessed 2021].