Cybersecurity Risks on Automotive Industry

Bruno Rodrigues

Lúsofona University of Porto, Portugal
bfrodrigues15@gmail.com

Abstract. In plain twenty-first century, technology has exploded and exponentially grows everyday bringing innovation and commodity to the human being. One aspect where technology was revolutionary was in the automotive industry. Themes like artificial intelligence supercharged cars with the capabilities that we know today. With innovation comes an increase in complexity and thus increases the concerns related with cybersecurity.
In this paper we will talk about the vulnerabilities and the effects that those have to the end consumer, also we will discuss some mitigation techniques that can be implemented both at manufacturing and software development level.
We will start by introducing the actual picture of the automotive industry and what advancements have been made till now. Here it will be discussed not only the actual techniques used and their vulnerabilities but also the reason behind such security threats in a world where we have achieved some high security standards.
Then will breakdown vulnerabilities in means of access (physical and remote). It will be described and explained the methodology applied to the different parts of an autonomous vehicle as well as some techniques and technologies that can help mitigate these vulnerabilities and contribute to a better and safer automotive future.
In the end will be presented a cyberattack example to round up the concepts discussed along the paper.

Keywords: Cybersecurity, Autonomous driving, Vehicles, Data Security, Communication

1 Introduction

Automotive industry has been revolutionizing herself lately. With the increasing advancements in technology, automotive brands started to adopt the benefits and the commodity that comes with terms like artificial intelligence consequence of the exponential growth when it comes to technological developments.

According to [1] "autonomous driving, connected cars, electric vehicles, and shared mobility have dominated the agenda of automotive industry leaders in recent years.

10.11228/dpsc.03.01.006

These innovations, built on the digitization of in-car systems, the extension of car IT systems into the back end, and the propagation of software, turn modern cars into information clearinghouses."

The main problem related with the increasing automation and "intelligence" of this type of vehicles is that to achieve this type level of complexity there is a growing need in adding lines of code. Every year cars get more complex and thus their ECU´s (Engine Control Unit) get a bigger number of lines of code. Has we know, every time we add code, we are increasing debug time and clearing room for possible vulnerabilities. Has stated by [2], "the average modern high-end car software is 100 million lines of code, to be compared with Windows 7 (39.5 million in 2009) or a Boeing 787 (13.8 million)."

This statement shows the complexity and the humongous amount of terrain to be covered by manufacturers and their counterparts.

This paper will focus on the "who" and "how" of those vulnerabilities and what improvements can we implement at the different manufacturing levels to achieve safer vehicles in the future.

On section 2 we will start by describing and contextualize the current picture in automotive industry.

On section 3 will be discussed sources of vulnerabilities and exploits on modern vehicles and some techniques to mitigate those vulnerabilities.

Then on section 4 we will see the importance of human behavior in cyberattacks success together with some examples that illustrate those same behaviors.

Finally, it will be presented an example of a real cyberattack to understand some of the concepts talked about along the paper as well as some recommendations regarding those vulnerabilities and exploits.

2 Current Picture in Automotive Industry

Today when we are looking for our next car, we look for some key aspects: fuel consumption, comfort, performance, and pleasure to drive.

These aspects are overrated by car manufacturers because these are the ones that sell their product. This is not a concern when it comes to the traditional vehicles but when we talk about cars with ever growing complexity when it comes to technology and automation, this can be considered a security threat. "This measure of quality is underpinned by regulatory activities that impose minimum standards for managing cybersecurity risks and require OEMs" (Original Equipment Manufacturer) "to have the ability to fix security issues via software updates." [1]

Nowadays the most used methodologies in automotive security practices are security management, penetration testing and dynamic security testing (DAST)[3].

According to a study made by [3], from all the participants that answered the study only (61 percent) apply security patch management and (56 percent) made penetration testing to ensure vehicle security. Figure 1 below exposes adoption rates for the various security practices used nowadays.

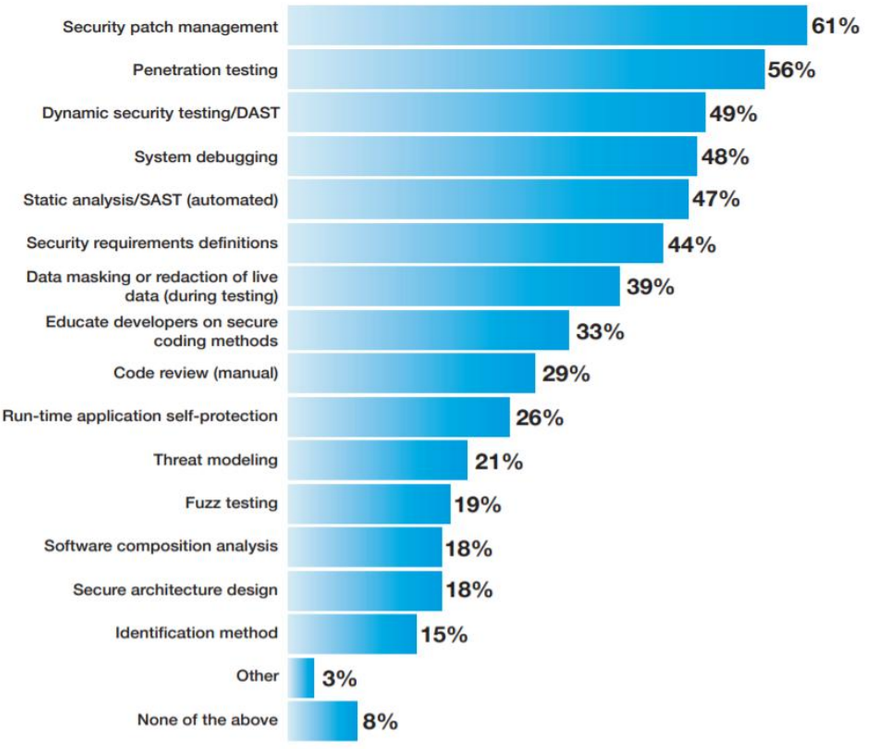

Fig. 1. - Adoption Rate of Cyber Security Practices in the Car Industry [3]

Secure architecture design stays at (15 percent) and code review (29 percent), two major steps to ensure a safe and less prone to breaches software. In contrast system debugging is quite high when compared with the previous two, sitting at (48 percent). This proves that the focus is on making it just work and ready from a consumer perspective, not making it work the right way by checking all the outcomes and variable in place.

This allows us to conclude the veracity of the statement made on the second paragraph on this section. Although there is plenty of countermeasures and practices that can reduce the risk of these vulnerabilities seems that manufacturers lack the ability to understand the need of investing in security.

3 Vulnerability Sources and Exploits

In this section we will breakdown vulnerabilities in current automated vehicles, but first let´s look at some factors that can increase the probability of these vulnerabilities being exploited:

- Implementation of software and hardware including apps, services and every form of communication offered by the vehicle
- Backend data and infrastructure which provide OEM firmware and OTA (Over-the-air) software updates
- Third party parts manufacturing and designing
- Driver behavior and knowledge

These factors will be described and broke down according to means of access in the next subsection:

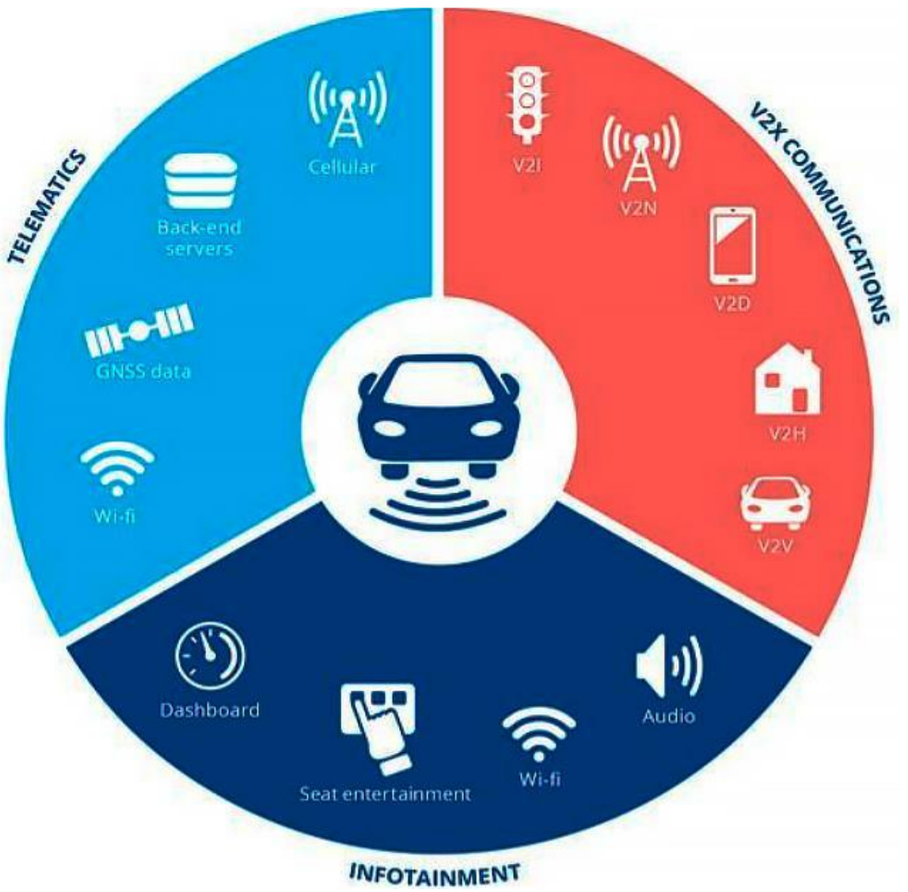

Fig. 2.- Smart Vehicles Ecosystem [4]

3.1 Physical Access Exploits

Physical access exploits have been one of the key aspects when it comes to whatever type of crime associated with vehicles. Along the years we have seen themes like theft and parts manipulation based on vehicle access and with the introduction of autonomous vehicles that vulnerability persists.

3.1.1 CAN (Controller Area Network) bus and ECU´s

Autonomous vehicles rely on CAN bus to control very important functions such as steering, acceleration and braking. This is considered the highest feasibility vulnerability at a physical access level since it controls the core aspects of a car.

A possible methodology of attack would be directly accessing the cables of the buses and manipulate them [5]. The risk underlying here sets on the nature of the ECU's and some of their purposes. One of the functionalities of this part is the capability of allowing service centers and authorized personnel to access the vehicle for diagnosis or modifications. Having direct access to the ECU's would allow hackers to have the same capabilities but with other intentions allowing for control over key functions of the vehicle.

Some examples of types of attacks achievable by targeting this unit:

CAN fuzzing attack-This attack bases itself in sending random data to CAN bus in [6]. The methodology sets behind listening and sniffing CAN messages over time.

CAN bus frame falsifying attack-This attack inserts incorrect data in CAN messages payload in order to falsify information [6].

CAN bus injection attack- Injecting data into a CAN bus can be used to send messages at an abnormal rate. "The purpose of this attack is to change frequency and amount of CAN frames."[6] This attack is achieved by manipulating vehicle´s decisions by overflowing the CAN bus with information.

3.1.2 Onboard Diagnostic ports

OBD or (Onboard Diagnostic) ports share a similarity with the methodology of attack described above. Here instead of physically manipulate the ECU and his counterparts the attacker takes advantage of the access to the service ports. By using these ports assigned to diagnose the vehicle during service, attackers can "eavesdrop on messages over these networks, send malicious messages, communicate with ECUs, and update ECU firmware using standard and low-cost off-the-shelf data logging and programming equipment."[7]

Such thing can be achieved by using the vehicles diagnostic port, if the target bus has pins that allow access to them, access can be achieved by swapping wires between the standard pins and target bus pins [8].

10.11228/dpsc.03.01.006

Methodologies to mitigate this type of attacks can be as follow:

- Parking vehicles in safe places and allow access only to authorized and trustworthy personnel [5]
- Implement software that monitors CAN inbound messages content and rate to detect abnormal behavior and control which messages are safe or not [5]
- "Implementing firewalls, whitelisting, and blacklisting of ECU messages to prevent unsafe commands" [5]

3.2 Remote Access Exploits

Most conventional cars nowadays have infotainment systems which allow to connect multiple devices to your car. Autonomous driving and connected vehicles are no different , in fact they are even more advanced in that matter. Unlike most of conventional vehicles, autonomous ones start to have OEM channels where telematic information and OTA software updates are available through those channels. All this connectivity allowance opens space for vulnerabilities at a remote level.

Now we will break down some common scenarios that explore vulnerabilities:

3.2.1 GPS and Cameras

This is considered a severe vulnerability when compromised since they are responsible for guiding the car. GPS tracks where the car is located at geographic level and camera reads the surroundings.

The most common exploitation on the GPS side is jamming. Here the attacker tries to falsify the location of the vehicle and provide wrong information to the driver. This type of attack is particularly difficult to detect due to environmental constraints.

When it comes to cameras, the methodology of the attack consists in blinding their vision. This can be made using high brightness IR LEDS or IR lasers [9].

This type of attack is on everyone´s reach since it uses components easily found online at a low price.

3.2.2 Onboard Sensors and devices

Onboard sensors can be incapacitated by an EMP (Electromagnetic Pulse) discharge. This type of attack generates an electromagnetic field to damage in-vehicle devices. Although this can be dangerous for the driver, not enough power can be generated to incapacitate a full vehicle [9].

Another type of attack is creating a ghost vehicle by using a digital radio frequency repeater, here the signal is replicated and retransmitted. Since this copy is very convincing the radar will interpretate it as an obstacle [9].

10.11228/dpsc.03.01.006

3.2.3 OTA Updates

Over-the-air updates are another source of vulnerabilities when it comes to remote access exploits. "remote OTA ECU firmware updates become increasingly important and expected, which increase the chances for malware to infect vehicles from remote sites."[7] The attacker just needs access to the back-end server and from there it requests execution of an OTA firmware update for a fleet of vehicles [4].

After that the process is just like a normal firmware update where the user accepts it and then the hacker uploads the modified firmware update which contains a backdoor and from that point on he has now access to the vehicles that installed that modified firmware [4].

3.2.4 Vehicle Infotainment

In-vehicle infotainment systems present multiple connection resources like Bluetooth, Wi-Fi, Zigbee or universal serial bus [9].

Most of these systems are based on well-known distributions that we use on our computers. This familiarity with operating systems like Linux, Green Hills, Windows CE, and QNX, allowing hackers to implement and reuse the knowledge that they already have from computers [5].

Other key aspect is reutilization. Manufacturers want to use software in as much vehicles as they can so that is easier to maintain and reduce costs on development which takes the same vulnerabilities to a wider range of vehicles.

Methodologies to mitigate this type of attacks can be as follow:

- Require authentication for both the user, OTA updates and services that directly influence important parts of the vehicle so integrity and availability can be maintained on core services and functionalities of the vehicle [5].
- Run infotainment communications on a different channel from the one that handles all the data related with operations and safety management [5].
- Encrypt OTA updates and allow to reverse them in case of a severe security breach [5].

4 Human Behavior and Vehicle Cyberattacks

Despite all the vulnerabilities and methodologies described in this paper, there is one more key intervenient when it comes to cyberattacks in vehicles and their success.

Drivers are one the most vulnerable parts on a vehicle cyberattack simply because is very easy for hackers to get access to the car by luring the driver into doing some type of action that triggers malware or other type of malicious implementation.

This is one of many examples of an ever-growing source of cyberattacks, social engineering. Simple events that at first site seem unharmful like opening a link sent through an email or message or opening a suspicious website can lead to malware injection in the same way it happens in our laptops, phones, and such. After all current autonomous vehicles are real computers where you can do everything that you would normally do on a laptop.

All the scenarios talked above are possible because of human behavior and lack of cybersecurity awareness.

Risky cybersecurity behavior is connected to the over-trust of automated technologies. "When the driver trusts their car too much, it is more prone to attack."[10][11] This happens because people misunderstand or are not well informed about the limitations of an autonomous driving vehicle or simply because they use technology on a daily basis and think they know all about it.

4.1 How Behavior Patterns and Skills Affect Vehicle Cyberattacks Sucess

Numerous studies have been made related with the relationship between human behavior and vehicle cyberattacks. According to those studies "people are prone to behaving in a more risky fashion towards cybersecurity if they are more extraverted, addicted to the internet, impulsive, and less conscientious." [10][12]

This fact allies to other human behavior variables such as the capability of assess a problem, reacting under pressure and multitasking. The capacity of problem assessment varies from people to people, "23% of people correctly handle less than half of cybersecurity scenarios; only 4% can handle more than 90% of scenarios." [10][13]

Other aspect is distraction. This one is common to automotive industry in general, nevertheless distraction plays a major role when it comes to abnormal behavior detection. Paying attention to other events or multitasking can prevent, for example, the driver from reacting to an unexpected turn caused by a remote attack.

Distraction can be paired with capability of reacting under stressing circumstances. An unexpected switch in a car behavior can make the driver stress and thus affect his decision capability leading to disaster. An attack success rate increases when the driver realizes he is not in control anymore, here the driver starts behaving irrationally and making untaught judgements opening space for unwanted events [10][14].

What was described in this subsection represents another source of cybersecurity vulnerability, one that is more abstract since it depends on the human mind. Nevertheless, manufacturers should invest in awareness as a way to mitigate cyberattacks since the driver plays such an important role in preventing them as we saw.

5 Jeep Cherokee Hack - A cyberattack Example

Now we are going to discuss an experiment presented in [15]. The objective with this discussion is to understand how the vulnerabilities and exploits talked above are explored in a real situation with a vehicle. Although the vehicles targeted in this study are not autonomous, the principle behind it remains the same.

We will start by describing which parts of the vehicle were explored to conduct the different types of attack achieved in the experiment.

- Explore infotainment system WIFI connection
- Exploring the link between CAN bus and a V850 Controller (cellular network)

The first type of attack consists of exploring the hotspot WIFI feature present in the infotainment system. The problem with this approach for who wanted to hack the vehicle were two factors.

First hotspot Wi-Fi is a paid service which on a long run would be costly for most people so it wouldn´t target a big audience, second you would still need to figure out the WPA2 password to connect to Wi-Fi which will be discussed next.

Now let´s take a look at the way WPA2 passwords are generated.

The system presents in the vehicles used in this study calculated the password by using the time/date which normally is acquired through the v850 controller by cellular network, so it is similar to the way our phones acquire the same time and date. The problem is that at boot time the system does not know time/date yet, so it uses a default time plus the time Wi-Fi service takes to boot. The combination of these two variables give us the password of the device, then you just need to convert it to UNIX epoch time, and you have the WPA2 password.

Obviously, the way passwords are generated makes it easy to guess since it results on a relatively small number of combinations if we would use a brute force attack. Experts estimate that it could take as low as one hour to discover the password through a brute force attack.

The focus of the attack relies on a specific TCP (Transmission Control Protocol) active port, the one used by D-bus. D-bus is an inter process communication mechanism that handles the data share between processes.

This mechanism allows to have access to the services and methods used to control several aspects of the infotainment and other features like ac and radio. Normally this D-bus has authentication implemented so that only authorized credentials can have access to those services. Nevertheless, Jeep didn´t have any authentication constraints so you could just declare yourself as Anonymous and have access to everything inside it. This

added to the fact that D-bus ran as root would allow to execute any commands with administrator privileges if a shell could be used.

5.1 D-bus Command Line Injection

Now that they granted access to all services, they had access to all services, during their research they found one service in particular that had a vulnerability, this vulnerability allowed the execution of any line of code or instruction that we wanted including changing volume or ac temperature. From this point on , they had access to the vehicle head unit where they could control every aspect except car essentials such has braking and steering.

5.2 Connection to CAN bus: The Challenge

So, until now, access to infotainment system has been totally granted, but the way it was designed prevents the infotainment system from connecting directly with the CAN bus so that the infotainment system cannot control physical parts of our vehicles such has steering.

Nevertheless, experts found that another unit, the v850 controller actually connects directly with the CAN bus. Although originally this was designed not to allow execution of code, just listen to CAN bus. This limitation was overridden has we are going to see later on.

Now that they knew the relationship between the v850 module and the CAN bus it was time to access this unit trough cellular network because not everybody would pay for hotspot WIFI connection, so that methodology was only useful to a minority of cases.

In order to do that experts bought femtocells which they used to connect a phone with cellular data from local carrier to the car. This allowed them to list IP addresses on the network and also find, not only the local IP address of the car they had, but multiple cars connected to the same carrier.

5.3 V850 Firmware Flashing

So up until moment experts were not still capable to connect to the CAN bus and actually affect the physical parts of the vehicle. So, the solution was to turn the attention to the v850 chip. The v850 chip was the only component accessible externally that had contact with the CAN bus.

In order to get over this limitation experts wrote their own version of the v850 controller firmware and flashed it.

Since once again firmware packages are not signed and flashing them did not require a signature either all they had to do was reflash the v850 controller with their firmware.

By flashing modified firmware to the v850 chip they overcame the initial challenge of sending messages to the CAN bus.

Now all that was left was to send shell commands to control key functions of the car such as steering, proximity sensors and such.

5.4 What can we take from this cyberattack?

This cyberattack is an example of the lack of investment in security by car manufacturers.

There were some barriers and security concerned design in some aspects till some extent. Nevertheless, a lot of vulnerabilities were found, and shortcuts were taken.

Some ways of improvement would be increasing the complexity of Wi-Fi WPA2 passwords generating algorithm, using a hash function to generate a unique signature to validate firmware updates and fix memory corruptions. These are some of the improvements that could be implement in first place.

Is also important to have in mind that to execute this attack physical access and time were needed. Firmware flashing involves a USB stick and direct interaction with the vehicle infotainment making this attack more difficult. Still, this vulnerability was present in approximately 1.4 million vehicles.

This proves the importance of manufacturers investing in safer methodologies and implementations as cars automation and complexity grows. The cult of a laid-back approach from manufacturer side resulted in many other studies and cyberattacks that happened exactly by the same reasons.

Luckily, most of this cyberattacks are not harm targeted and so we can learn more about how they happen and how to mitigate them.

6 Conclusion

Along this paper we presented numerous vulnerability and exploitation sources. These vulnerabilities and exploitations are the result of administrative decisions, priority hierarchy, software development lifecycle nature and security awareness between car manufacturers and their counterparts.

Nowadays security has evolved, and some manufacturers already see it has a threat and a feature worth investing. Nevertheless, there is still plenty to do, mainly when it comes to awareness and build the importance of security in people´s mind. Only that way we will end with laid back approaches both at manufacturing level and software development wise allowing vehicle industry and technology to grow together.

With the increase of customer awareness, new methodologies of mitigation and studies are in the works, futureproofing the viability of the ever-growing technology influence in vehicles.

This is a great opportunity to revisit and forward develop this subject evaluating which new threats evolved and how those are being threated, compare it with the current situation and even develop a case study based on those aspects.

7 References

1. Mckinsey and Company, "Cybersecurity in automotive-Mastering the Challenge", (2020)
2. Altran, "Cybersecurity in Automotive-How to Stay Ahead of Cyber Threats", (2018)
3. Ponemon Institute, SAE International, Synopsys , "Securing the Modern Vehicle Practices: A Study of Automotive Industry Cybersecurity Practices", (2018)
4. ENISA,"Enisa Good Practices for Security of Smart Cars", (2019)
5. Hodge, Cabell, Konrad Hauck, Shivam Gupta, and Jesse Bennett. "Vehicle Cybersecurity Threats and Mitigation Approaches." Golden, CO: National Renewable Energy Laboratory. NREL/TP-5400-74247, (2019)
6. Emad Aliwa, Omer Rana, Charith Perera, Peter Burnap, "Cyberattacks and Countermeasures for In-Vehicle Networks", (2020)
7. Zhang T., Antunes H., Aggarwal S., Defending Connected Vehicles Against Malware: Challenges and a Solution Framework. IEEE Internet of Things Journal. 1, (2014)
8. Aastha Yadav , Gaurav Bose , Radhika Bhange , Karan Kapoor , N.Ch.S.N Iyengar , Ronnie D. Caytiles," Security, Vulnerability and Protection of Vehicular On-board Diagnostics", *International Journal of Security and Its Applications Vol. 10, No. 4*, (2016)
9. Jonathan Petit, Steven E. Shladover, "Potential Cyberattacks on Automated Vehicles", (2014)
10. Václav Linkov, Petr Zámečník, Darina Havlíčková, Chih-Wei Pai, "Human Factors in the Cybersecurity of Autonomous Vehicles: Trends in Current Research", (2019)
11. Parkinson S., Ward P., Wilson K., Miller J.,"Cyber threats facing autonomous and connected vehicles: future challenges", *IEEE Trans. Intel. Transport. Syst.* 18, (2017).
12. *Hadlington L Heliyon,"* Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours", (2017)
13. Yan Z., Robertson T., Yan R., Park S. Y., Bordoff S., Chen Q, "Finding the weakes links in the weakest link: how well do undergraduate students make cybersecurity judgment? *Comput. Hum. Behav.* 84", (2018)
14. Moisan, F. and Gonzalez, C ,"Security under uncertainty: Adaptive attackers are more challenging to human defenders than random attackers", Frontiers in Psychology, 8:982, (2017)
15. Charlie Miller,Peter Valasek, "Remote Exploitation of an Unaltered Passenger Vehicle", (2015)