EasyChair Preprint

№ 9530

# Security Threats and Risks in Automotive

João Fernandes



January 3, 2023

# Security Threats and Risks in Automotive

João Fernandes

Lusófona University
jpfernandes1602@gmail.com

**Abstract.** Safety and security are both qualities that concern the overall system. In this study, I have tried to understand the consequences of one or more security breaches in the automotive sector and the impact, origins, and solutions. The focus of this research was documentary analysis, seeking to understand a case study where the ADAS system does its job and the main consequences of an invasion of Crackers to the security system. In the next phase, using interviews to study a car brand, understanding in a more intimate way the failures, how they can occur, and how they are solved. Through the survey, it will be possible to focus on the statistical data of this problem, offering a relationship between the security of the car and its drive and studying the vulnerability to the invasions of Crackers**.**

**Keywords:** Safety, Security, Impact, ADAS system, Solutions, Crackers, Vulnerability

## 1 Introduction

Automotive innovations have transformed the industry as we know it where wheels and an engine once powered cars, and now they are a kind of data network on wheels. However, with new technological advances come new vulnerabilities and network risks. Driving habits are often unseen data, only becoming available to fleet managers when accidents occur. Brands are increasingly concerned with security, so this paper will address two topics: one ADAS system, how it makes driving safer, and the impact of " Crackers " invasions in cars' security systems. The main objectives in focusing on these two topics are to try to understand the importance of both, how they evolved until today, based on news and articles, and to try to understand that both have a huge impact on safety in the automotive sector.

To counteract traffic accidents, we could change human behavior and adopt vehicle-related and physical road infrastructure-related measures. Another approach is transitioning from passive safety measures to active try measures. Passive safety measures include airbags, car body structures, seatbelts, and head restraints. Active safety measures include electronic stability control (ESC), and anti-lock braking systems (ABS). [Damian Grzechca, 2019][3]

Technological Advances have made significant contributions to vehicle safety, value, and functionality from stability control to electronic fuel injection, navigation, and theft prevention. They have also increased connectivity, adding many functions common to smartphones, such as cellular data and voice functionality, web browsers, online games, and entertainment.

For this project, I interviewed a former BMW engineer to try to understand how a company deals with an attack of Crackers, in this case, we will talk a little about an attack on the application, which controls everything in the car, opening doors, starting, and stopping the engine…

Finally, a questionnaire study to determine whether people are very or somewhat vulnerable to attacks by "Crackers".

## 2 Innovation in next-generation cars

By advancing network connectivity in cars, the industry has enabled innovative functions, some of which are already available. These new functions are often referred to as “cyber-physical” features, since they require collecting data from the physical environment and cybersystems, making automotive operation decisions, and executing such decisions with physical consequences. Some of these innovations include [2]

- Advanced driver assistance systems (ADAS): Smart lighting control, adaptive cruise control, collision avoidance, driver fatigue detection, lane departure warning, and parking assist.
- Advanced fleet management: Usage and behavior monitoring, warranty restrictions by zone, real-time telematics, and package tracking.
- Smart transportation: Traffic congestion, vehicle sharing, and fuel efficiency are influencing existing operating modes and creating new ones. Vehicle-to-infrastructure and vehicle-to-vehicle communications, such as smart intersections, traffic light control, road trains, and traffic management, are key contributors to smart city operations.

The goal of the next generation of vehicles is for driverless vehicles to become a reality to achieve zero fatalities and/or crashes, improved traffic flow, and other benefits, with early examples already visible from Daimler, Ford, Google, Tesla, and others. Automotive innovation drives the need for embedded security solutions and architectural design to mitigate emerging threats. There are already prototypes of future innovations to ensure security,

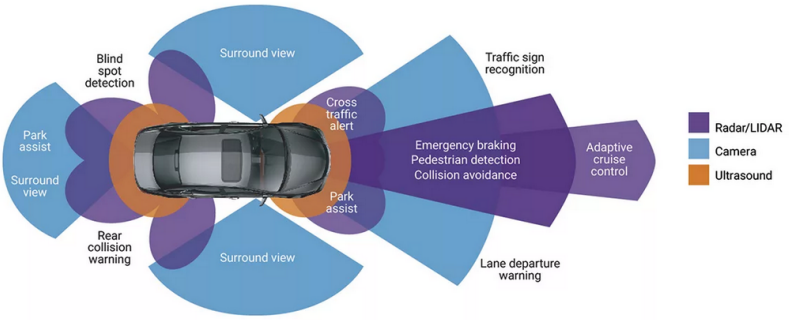
for example, Jaguar Land Rover shows that the car of the future will be able to learn from the driver's routine, it will be able to know which radio station the passengers usually listen to on their way to work and Lamborghini's Urus can change shape depending on the moment, they will be able to adapt to the environment in which they ride. [V. Caputo, 2016][4]

## 1. System ADAS

The ADAS system was developed to provide a safe and effective driving experience, trying to reduce and/or avoid the risk of collision. This ends up being a system that benefits the driver of the car with the ADAS system and other drivers on the road.

Advanced Drive Assistance Systems (ADAS) cannot completely prevent accidents, but they could better protect us from some of the human factors and human error is the cause of most traffic accidents. [Adam Ziębiński, 2019][3]

Self-driving cars use a variety of these applications and technologies to gain 360-degree vision, both near (in the vehicle's immediate vicinity) and far. That means hardware designs are using more advanced process nodes to meet ever-higher performance targets while simultaneously reducing demands on power and footprint.




In this paper, the ADAS system discussed will be Mobileye, a collision avoidance, and alert system. Equipped with strategically placed intelligent multisession sensors, Mobileye systems act as an extra angle of vision for the driver, constantly monitoring the dynamic driving environment and providing drivers with real-time visual, audible, and vibration alerts.

How it makes our driving safer, with pedestrian and cyclist imminent collision alerts within the front and side danger zones of the vehicle; imminent collision alerts with vehicles traveling in front of any speed giving the driver time to react and take corrective action; speed limit recognition alerts to warn

the driver if the vehicle is exceeding the permitted speed limit and help the driver to maintain a continuous safe driving distance and provide visual and audible warnings if the distance becomes dangerous.

**Case Study (Yoshida Taxi - ADAS system implementation)**

The case study I will present is about a taxi company in Japan, where the average age of the employees is between 60–65 years old. Due to the average age of the employees and lack of demand for jobs in this field, the taxi company came up with a solution to decrease the number of collision cases, because as you can imagine, it must have been high due to the age of the employees.

The solution was to install the ADAS system, more specifically Mobileye's. The combination of Mobileye alerts and the telematics system allowed Yoshida to analyze each driver's habits.

According to Yoshida, the results were remarkable, collisions fell by eighty-five percent.

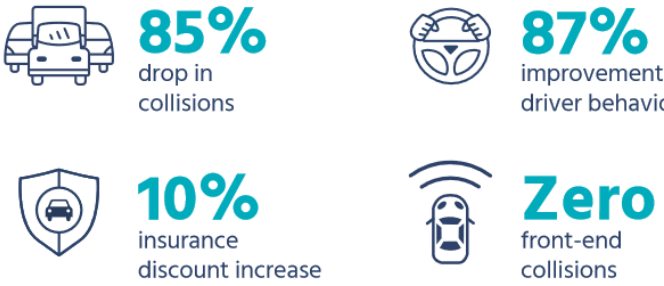



*Figure 1 - Statistical data of the case study~*

Installation of the ADAS system is a major advantage for both safety and comfort.

## 3 Crackers and Security System Invasion

The more connected we are, at home, on our mobile phone, or in our car, the more exposed we are to attacks by crackers, who break into vehicle security systems. The technological advances around car safety are unquestionable, but digitalization and connectivity have opened doors to new forms of criminality. By using techniques in vehicles that can be hacked, technology makes it possible to hack into your car parked outside your home, for example.

What is the difference between a Hacker and a Cracker? The Cracker's objective is to damage systems and have access to all their data, through the

Internet connection, he can find out the vehicle owner's telephone number, name, electronic address, and address, follow all his itinerary and usual trips, control several functions of the car, from the air conditioning to the electronics of the braking system, open and close doors and even start and stop the engine and the Hacker's objective is to elaborate and modify computer software and hardware, either developing different functionalities or adapting old

It is important to be aware that no modern car is inviolable. Depending on the level of digitization, the model you drive every day will be vulnerable. The only way to reduce the risk of being taken by surprise during a cyber-attack is to stay informed and alert. There are, however, some recommendations from manufacturers:

- **Up-to-date software:** Most of the time, updates are created to cover cybersecurity gaps. Keep your car's software up to date with the versions provided by the manufacturer.

- **Check before connecting:** USB devices can be the most common "Trojan horse" when installing malicious software.

- **Be careful with downloads:** The smartphone is taking on more and more functions. Be more attentive to all the programs and applications you download.

**Case Study (My BMW App – Identify Theft)**

Identify theft is the crime of obtaining another person's personal information to use their identity to commit fraud.

When I interviewed the engineer, I asked him what the most common identity theft is, and he replied that it is from the application that can control, for example, opening the car and starting or stopping the engine. Then he explained one of the ways to identify the theft, to access the personal account in the application you need the mobile phone number, so they were able to find out the phone number of a customer, they went to a "Vodafone" shop, for example, and with knowledge inside Vodafone, they were able to create a SIM card with that phone number, thus being able to enter the customer's account with the phone number, controlling all the features that the application allows.

One solution I propose is to reinforce the authentication on new devices, with a strong two-way authentication, one with the phone number and the

other with a code from a card given when buying the vehicle. I think that this way security is ensured because this card is unique.

## 4 Study of people's security vulnerability

The questionnaire seeks to understand whether people are very or somewhat vulnerable to cyber-attacks on their car's security system. Two different graphs will appear for the same question, as I divided the questionnaire between those who drive and those who do not have a driving license. There were ninety participants, sixty-five drivers, and twenty-five non-drivers.

By analyzing the answers, I can conclude that:


*Figure 2 – Question 1: "Do you know what a hacker is?"*


*Figure 3 – Question 2: "Do you know what a cracker is?"*

With the results of questions 1 and 2, I can conclude that most people know what a hacker is, but also a large part does not know what a cracker is, although they are very similar, both have different dangers that can be crucial to our security system. I also asked people who knew what a Cracker was if they knew the difference between a cracker and a hacker; the answers were positive.


*Figure 4 – Question 3: "Do you usually connect your smartphone to your vehicle?*

We can see that most people are exposed to phishing, which is not good. A method that can change this percentage is, for example, using CDs to play music and stopping the car to answer calls, so we avoid connecting the smartphone to the vehicle and are less vulnerable.


*Figure 5 – Question 4: "Does your vehicle have Wi-Fi access?"*


*Figure 6 – Question 5: "Is the car paired with a smartphone app?"*


*Figure 7 - Question 6: "Does the car have assisted driving?"*

With the results of questions 4,5 and 6, I can conclude that most people still do not have access to advances in technology, for example, having an app from scratch connected to their car, as in "My BMW App". On the one hand, it is good because they are less vulnerable to Cracker attacks through these technological advances, but on the other hand, they are less safe in everyday life, because the technological advances, such as the ADAS system, bring more safety for both the driver and other people on the road.


*Figure 8- Question 7: "Do you have any idea of the danger of an invasion of your security system by Crackers?"*


*Figure 9 - Question 8: "Do you agree with the advances in technology in the automotive sector?"*

With the results of questions 7 and 8, we can see that most people are not aware of the "danger" of hacking into the car's security system, and yet they agree with the technological advances and are putting their lives even more at risk.

## 4 Conclusion

In short, the use of new technologies such as the ADAS system is important to ensure comfort and especially safety for both the driver and all those around him and protect us from pirate attacks that can cause many problems and endanger the driver.

However, the use of new technologies can also be dangerous, because the brands, as we have seen in the case of BMW, do not care so much about digital security as about the physical security of the driver, which is good for Crackers, who have more facility to break into a system.

So, the conclusion I reach is, the evolution of new technologies in the automotive sector is something recent, it still needs to be thought about because they do not give so much importance to digital security, and the target audience, drivers, or future drivers is still not aware of the computer dangers.

I want to thank the BMW engineer for his participation and my safety and audit professor, Hugo Barbosa, for the opportunity to choose this topic for the paper, it helped me to understand a little more about digital security in the automobile sector and the risks that we are willing and that we have no notion of.

## References

2. D. Clare, S. Fry, H. Handschuch, H. Patil, C. Poulin, Dr. Wasicek and R. Wood (2016) 'Automotive Security Best Practices". McAfee. https://www.mcafee.com/enterprise/en-us/assets/white-papers/wp-automotive-security.pdf

3. Zielinski, R. Cupek, D. Grzechca, and L. Chruszczyk, (2019, November) 'Review of advanced driver assistance systems (ADAS)", Conference Paper in APC Conference Proceedings. pp. 1 to 6. https://www.researchgate.net/publication/321364551_Review_of_advanced_driver_assistance_systems_ADAS/link/5cb42b544585156cd7992ddd/download

4. Caputo.V (2016), "10 inovações tecnológicas que os carros terão no futuro". Exame.55anos. Consulted to December 18, 2022. https://exame.com/tecnologia/10-coisas-que-os-carros-terao-no-futuro/

5. Hotta. K (2016). Yoshida Taxi Collision Rates by 85%. MOBILEYS An Intel Company. https://adas.pt/wp-content/uploads/2022/05/Caso-Estudo-Mobileye-1.pdf

6. "Crackers": os piratas informáticos que lhe entram no carro. MOTOR24. Consult to December 26, 2022. https://www.motor24.pt/noticias/crackers-os-piratas-informaticos-que-lhe-entram-no-carro/1562583/, last access 28/11/2022

7. Hussain. A. (2022). What Is Identity Theft? Definition, Types, and Examples. Investopedia. Consulted to December 22, 2022.

https://www.investopedia.com/terms/i/identitytheft.asp, last access 09/12/2022

8. What is ADAS? Synopsis. Consulted to December 26, 2022. https://www.synopsys.com/automotive/what-is-adas.html