## Foundations of security

## Assisted Driving and Multimedia system for cars

CAR GUARD

Car Guard

## Abstract

This report explores the implementation of a system that provides cars with two services, assisted driving and multimedia functions. Using DREAD and STRIDE, analyzing the risks of implementing the two services and solving it with secure designs. As well as exploring the vulnerabilities of having a backdoor installed to the services. The market is growing and the demand for assisted driving services is large, this report helps exploring the gain and risk of a system that is getting released into the market.

## Introduction

Cars that are being manufactured today come with all sorts of tools and services that try to make the driving experience better for the driver. With the advancement in technology, cars can think and calculate faster than the human mind ever could, and it's all connected to the internet. According to (McKinsey & Company, 2014) "Today's cars has the computing power of 20 personal computers, around 100 million lines of code and processes up to 25 gigabytes of data an hour.". Most of these changes are to protect the driver and passengers, and as many as 153.158 casualties of all severities in reported traffic incidents in 2019, statistics by (GOV.UK, 2020) According to (Sheehan, 2020) from 2018, the advancements done on cars regarding safety technology has reduced the traffic accident by 10% in just 5 years. As technology advances we are looking for new ways to better the safety of drivers and passengers, that's where assisted driving comes in. With assisted driving, it will help reduce the traffic accidents in the next upcoming years. As well as offering a full fletched multimedia service that can aide the driver in navigation, fuel usage and overall health check of the car.

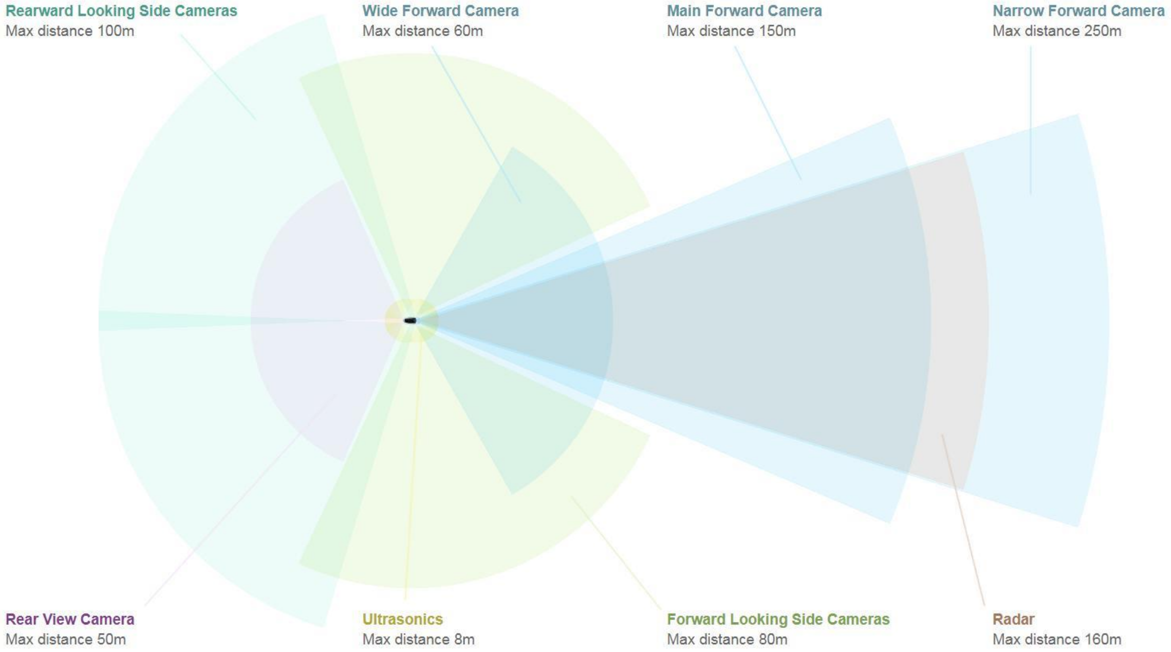
## Product description & background research

Car Guard is a system made for cars that offers 2 services for the driver that aims to help with driving, navigation and overall health of the car:

- The multimedia service assists the driver with a multimedia setup that displays GPS and mileage to the destination, suggesting when the car should go for a health checkup and which parts that should be checked, as well as calculating how much fuel it uses to reach the designated destination.
- The other service is assisted driving that calculates the distance between other cars in the vicinity, by using cameras and sensors, to keep the car at a safe speed and

distance from other cars. Connected to the internet it can analyze the traffic infrastructure and read the traffic light and traffic sign network.

Car Guard's assisted driving is a partial automation. The steering, acceleration and deceleration can be controlled by the car, but the driver always needs to keep an eye out and have their hands on the wheel. Famous automobile makers such as Tesla have an autopilot function like this (Tesla Motors Club, 2020), which is known as a level 2 automation. It helps the driver to slow down and avoid cars in traffic, as well as a handful of other functions such as self-parking and automatic lane changes. By using cameras and sensors as well as a forward-facing radar, Car Guard can achieve a partial automation function to its drivers which takes inspiration from Tesla's hardware. (Tesla, 2020)



*Tesla's cameras and sensors*

According to (Phelan, 2019) traffic crashes, vehicle damage and injuries are down thanks to assistance systems that are becoming more common in cars. Further in the article it mentions that a study done in 2018 by J.D. Power, include some results from drivers with assisted driving systems where drivers report that blind sport alert, back-up and parking cameras and forward collision alerts helped avoid a crash. From this research it is clear that assisted driving systems are a part of the future, and the market is growing quickly. And as mentioned in (Wagner, 2020) drivers in suburban and urban areas are willing to increase their car budget by 13 percent in order to buy a self-driving car. The market is growing quickly and there is demand for self-driving cars.

The multimedia service offers the driver a set of different functions to use, to make the driving experience as safe as possible. A screen to present the driver a GPS that displays fuel usage per mile, when to stop to refill the tank and since it's connected to the internet it can display the speed limits and road signs in the area. It also has a health check system, that tells the driver when to do a check-up on the car, displaying which part of the car that might need a checkup by using sensors that are installed.

With these features there are vulnerabilities. From (Greenberg, 2015) a Jeep got hacked remotely because of it being connected to the internet. The two hackers spent a year developing a program to exploit the Jeep's system. They were able to kill the engine, turn on the stereo and air-condition, as well as a few other things. A smart car can save lives but also ruin them if we don't think off all possible security measures, as it is vulnerable to attackers.

## Threat analysis

**0** to **5** is a low-risk rating

**6** to **10** is a high-risk rating

| Item | Software |
|---|---|
| Title | Wireless carjacker |
| Application | Operating system |
| Threat Target | System: Assisted driving |
| Threat Type | Spoofing identity |
| Risk | **Damage:** The attacker could gain access to the car system and at a low speed they can kill the engine, accelerate the car or give the wrong alerts to the driver. **10**<br>**Reproduce:** Can access the car system remotely as it is connected to the internet. **9**<br>**Exploit:** Attacker must have a lot of experience to be able to develop a software to carjack a car remotely. **5**<br>**Affected users:** Would be the driver, passengers, pedestrians on the sidewalk, other cars in the vicinity. **7**<br>**Discover:** It is getting well known that smart cars are vulnerable to attacks as they are connected to the internet, but as mentioned above it would require someone very experienced to be able to wirelessly sabotage the car. **3** |
| Risk Rating | 8 (Hard to exploit, if not it would be a 10) |
| Secure Design Recommendations | Regularly update and patch the system. Employ white hat hackers to test the systems security. |
| Backdoor | A backdoor shouldn't be necessary to implement. If there was a backdoor implementation regarding the operating system and its function to control the car it would cause serious security vulnerabilities. The risk rating would go from **8** to a **10** as it is quite complex to attack the system as of now. |

| Item | Hardware |
|---|---|
| Title | Hardware failure |
| Application | Operating system |
| Threat Target | Multimedia: Car health check |
| Threat Type | Tampering with data |
| Risk | **Damage:** The attacker can tamper with the car-health alerts that the driver can view. Telling the driver that a part needs to be changed or checked. **3**<br>**Reproduce:** Can reproduce it several times but overdoing it will make the driver suspicious. **2**<br>**Exploit:** Attacker must have some experience as he needs to attack remotely but tampering with data is fairly easy. **6**<br>**Affected users:** Would be the driver and passengers. Driver would either have the car checked up or try and fix it himself, or not care about it because it keeps displaying warnings and one time there's an actual warning, he ignores it. **5**<br>**Discover:** Smart cars are vulnerable to attacks as they are connected to the internet and this wouldn't require as much expertise to do. **6** |
| Risk Rating | 3 |
| Secure Design Recommendations | Implement a monthly or every 3rd month car health check-up in the system so if there is an attacker breaching through the layers of security he will struggle with bypassing the timed check-up (the systems timed health check is connected to a server so the attacker can't just modify the time and date) |
| Backdoor | A backdoor shouldn't be necessary to implement as it is a timed check-up of the hardware, having access to this feature shouldn't be a priority. Although giving a backdoor access could be exploited as the backdoor would give access to the server storing the date and time. |

| Item | Software |
|---|---|
| Title | Sensitive data |
| Application | Operating system |
| Threat Target | Multimedia: GPS |
| Threat Type | Repudiation |
| Risk | **Damage:** Could be severe depending on the hacker's intentions. The attacker could access personal information about the driver. Where he drives to and from every day, his home address and work address. **6**<br>**Reproduce:** Can reproduce it several times as it is connected to the internet but would need access to the server where it is being stored. **7**<br>**Exploit:** Attacker would have some knowledge on how to breach the systems GPS logs. **7**<br>**Affected users:** The driver's home address and work address are sensitive information and can be dangerous depending on the intentions. **6**<br>**Discover:** Would be easy to do if the hacker knows what he is doing or is determined to find out the driver's information. **8** |
| Risk Rating | 8 |
| Secure Design Recommendations | Having the GPS logs safely secured on a separate server with AES encryption. |
| Backdoor | Would make it even less secure, but as it is encrypted an attacker would struggle with gaining access to the information. |

| Item | Software |
|---|---|
| Title | Stealing all data |
| Application | Operating system |
| Threat Target | Entire multimedia service data |
| Threat Type | Information disclosure |
| Risk | **Damage:** Attacker could steal all the data of the driver. Saved GPS locations, Contact details, phone numbers and personal details of the driver.**8**<br>**Reproduce:** Attacker must access the server where the data is stored. **5**<br>**Exploit:** The attacker would have to have some knowledge on gaining access to servers and pull out data. **5**<br>**Affected users:** the driver/owner of the car. The owner's privacy would be at stake. **7**<br>**Discover:** Having the details stored on a server would be a bit difficult for the attacker to access, regarding login details. **4** |
| Risk Rating | 8 |
| Secure Design Recommendations | Use AES encryption on all data stored on the servers, use 3rd party authentication to access the information. |
| Backdoor | A backdoor would make it even more vulnerable as it would bypass encryptions. |

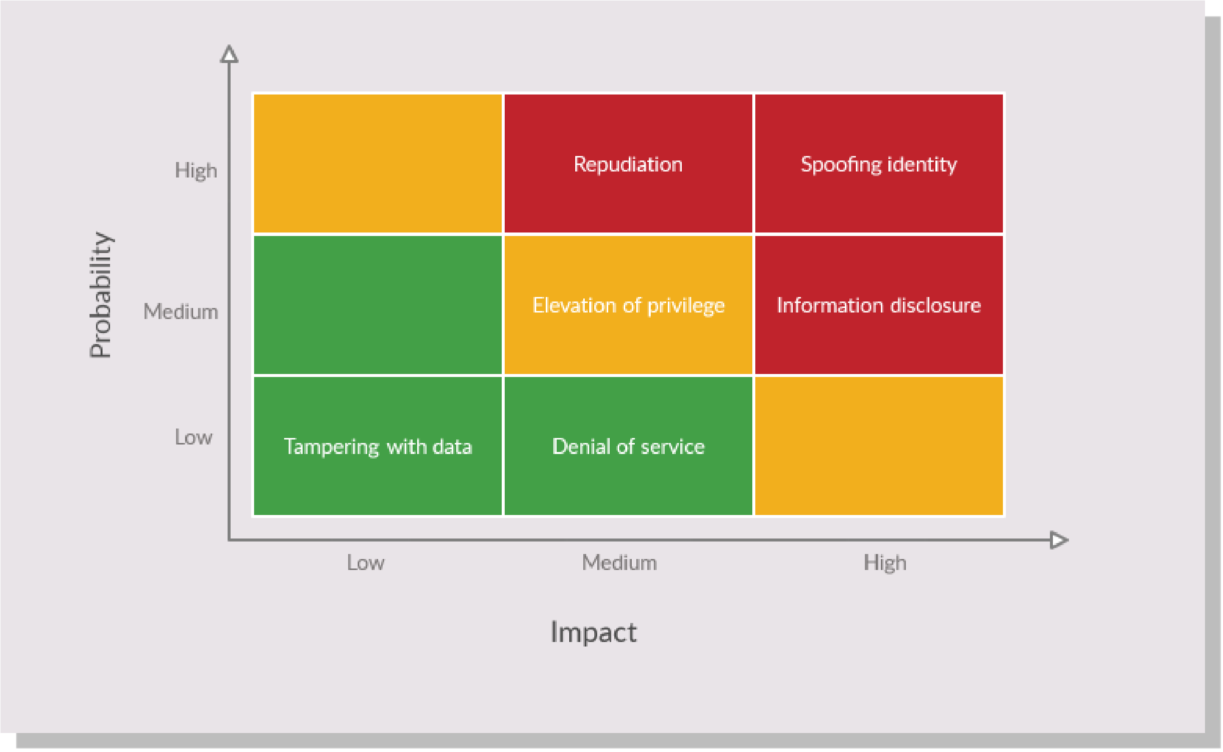
| Item | Network |
|---|---|
| Title | Network kill switch |
| Application | Internet |
| Threat Target | All multimedia functions |
| Threat Type | Denial of service |
| Risk | **Damage:** Attacker could kill the network connection by using a DDoS attack, which would kill all the functions that requires internet to work. **5**<br>**Reproduce:** A DDoS attack could be reproduced quite easily. **6**<br>**Exploit:** There are tools and programs made for DDoS which makes it easy to do, the attacker would only need the IP. **8**<br>**Affected users:** The driver. Network access would be lost and functions that require internet would not work. **5**<br>**Discover:** As mentioned, there are tools to perform DDoS attacks so the attacker would need to discover the IP. **6** |
| Risk Rating | 4 |
| Secure Design Recommendations | Installing a DDoS mitigator that diverts the traffic to centers that handle high traffic. |
| Backdoor | Having a backdoor to the multimedia system shouldn't be necessary as it would make the system more vulnerable, but it requires logins. |

| Item | Hardware |
|---|---|
| Title | Admin |
| Application | Operating system |
| Threat Target | Administrative functions |
| Threat Type | Elevation of privilege |

| | |
|---|---|
| Risk | **Damage:** An attacker could gain access to an admin connection and edit data and software. **9**<br>**Reproduce:** Hard to reproduce when the attacker needs to physically access the car. **6**<br>**Exploit:** As mentioned, the attacker would need to physically access the car alter it. **6**<br>**Affected users:** Depending on the attack, the driver and the passengers could be at risk if the attacker decides to alter data connected to the assisted driving function. **8**<br>**Discover:** The attacker would need a lot of knowledge and preparation to carry out a physical attack. **6** |
| Risk Rating | **7** (As it is a physical attack) |
| Secure Design Recommendations | Strong authenticator, making it hard to edit the data by storing logs of when and why the data was edited/updated. |
| Backdoor | A backdoor could put the system in a vulnerable position, as the attacker could view data, logs and updates to the system so he would “time” his attack with an update, leaving the change unnoticed. |

| **Threat** | **D** | **R** | **E** | **A** | **D** | **Rating** | **Risk** |
|---|---|---|---|---|---|---|---|
| **Spoofing Identity** | 10 | 9 | 5 | 7 | 3 | 8 | High |
| **Tampering with data** | 3 | 2 | 6 | 5 | 6 | 3 | Low |
| **Repudiation** | 6 | 7 | 7 | 6 | 8 | 8 | High |
| **Information disclosure** | 8 | 5 | 5 | 7 | 4 | 8 | High |
| **Denial of service** | 5 | 6 | 8 | 5 | 6 | 4 | low |
| **Elevation of privilege** | 9 | 6 | 6 | 8 | 6 | 7 | Medium |

## Risk Severity Matrix



| Probability \ Impact | Low | Medium | High |
|---|---|---|---|
| High | 🟧 | 🟥 Repudiation | 🟥 Spoofing identity |
| Medium | 🟩 | 🟧 Elevation of privilege | 🟥 Information disclosure |
| Low | 🟩 Tampering with data | 🟩 Denial of service | 🟧 |

## Secure design specification

When designing a service, an app or a project for users that especially requires internet, you need to be clear on one thing and that is that security planning should be done from day one. In all phases and layers of development security must be implemented. Testing and finding flaws/errors in code before releasing it to the public, as well as after releasing it to the public. Being one step ahead of attackers is a hard, time consuming task but with frequent patches to the system it makes the system less vulnerable and harder for attackers to "crack". Verify that all confidential data have effective access controls, identify how confidential data is treated and consider how implementing external components can change the way attackers can attack your system. Making the security familiar and friendly to the users is a requirement, it shouldn't affect users that comply with the rules.

## Conclusion

This report has analysed the threats that can occur when creating a service like Car Guard. Having taken examples of different attacks that can arise regarding the multimedia service and assisted driving service, from low risk to high risk, but also trying to solve this with secure designs. Taking into consideration the request of installing a backdoor to the service that the government can use has been proven to create a lot of vulnerable access points where it originally wouldn't.

As mentioned earlier in the report, there is a growing market for self-driving cars and vehicles that offer some form of assisted driving. People want to feel safe behind the wheel, and pedestrians and other drivers will also feel safe. There is always room for improvements and when we get advancements in the autonomous vehicle industry it will likely be a majority of the population owning self-driving cars than not.

## References:

Greenberg, A. (2015) *Hackers Remotely Kill A Jeep On The Highway—With Me In it.* Available at: https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/ (Accessed 23 November 2020)

GOV.UK. (2020) *Reported Road Casualties Great Britain, Annual Report: 2019*. Available at: https://www.gov.uk/government/statistics/reported-road-casualties-great-britain-annual-report-2019 (Accessed 23 November 2020)

McKinsey & Company (2014) *What's driving the connected car.* Available at: https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/whats-driving-the-connected-car (Accessed: 23 November 2020)

Phelan, M.(2019) *These Car Features Could Prevent Your Next Crash*. Available at: https://eu.usatoday.com/story/money/cars/2019/06/10/traffic-accidents-decline-because-of-car-features/1407386001/ (Accessed 25 November 2020)

Sheehan, S.(2020) *UK Road Accidents Down 10% In Past Five Years Thanks To New Safety Tech.* Available at: https://www.autocar.co.uk/car-news/industry/uk-road-accidents-down-10-past-five-years-thanks-new-safety-tech (Accessed 23 November 2020)

Tesla Motors Club (2020) *Explaining The Six Levels Of Vehicle Automation.* Available at: https://teslamotorsclub.com/blog/2018/07/02/explaining-the-six-levels-of-vehicle-automation/ (Accessed 24 November 2020)

Tesla (2020) *Future of Driving.* Available at: https://www.tesla.com/en_GB/autopilot?redirect=no

(Accessed 25 November 20202)

Wagner, I. (2020) *Consumers Worldwide Willing To Pay AV Premium By Metro Status 2019*. Available at: https://www.statista.com/statistics/1068659/self-driving-cars-consumers-willing-to-pay-premium-metro-status/ (Accessed 26 November 2020)