EP2790 Security Analysis of Large-Scale Computer Systems
Autonomous Car Manufacturer

Kalogiannis Konstantinos

January 9, 2020

1 Introduction

This report will concentrate its focus on describing our autonomous car functionality by connecting all the relevant sub-systems together and providing a thorough risk assessment. Our company is responsible for developing and releasing cars that can function in a highly autonomous fashion making use not only of Adaptive cruise control(ACC) but also Cooperative Adaptive Cruise Control(CACC)[18] in order to promote less fuel consumption, less accidents and better working conditions for the vehicle operator[5]. To that end, our vehicles need to behave, under any circumstance, according to the specifications provided to the customer and simultaneously fulfil the ambitions of the investors. To achieve both of those critical requirements all the modules need to be protected against adversaries that may wish to harm or subvert certain functionalities for their own gain. We will focus only on the security risks of our infrastructure leaving aside risks that may arise from society itself or faults that manifest in an non malicious way. Furthermore, distribution of the cars to the various dealerships and registration of those car to our back-end infrastructure are not examined in this report.

Considering that vehicles with autonomous functionality is an emerging market[8] with more and more companies entering the fray, it is of paramount importance that our systems are thoroughly tested before being released thus providing a safe base in which the company can thrive. This may seem easy, but it will be proven through this report that identifying threats for all our components is not a trivial task and although an exhaustive research will be conducted, there are empirical evidence, in the form of zero-day attacks, to show that previously unknown weaknesses can always be found and exploited. Our aim is to categorize all those threats and create an easy to digest report for the purpose of achieving better resource allocation when tackling them.

Before delving into the business goals and how those interact with our system we should first identify in an abstract fashion all our technical components. There are three different categories we can refer here[20] beginning with the

ECU	Description	Assets
Coordinator	The primary goal is to facilitate communication between the various ECUs	Coordinator ECU
Tyre Unit	The main functionality of this ECU is to monitor the tires and log usefull information	Tyre pressure/traction sensors
Steering System	Responsible for all functions pertaining to guidance of the vehicle and safety countermeasures	Steering Wheel sensor Steering Wheel vibrator
Telematics Control Unit	In charge of connecting the vehicle with the cloud	3g/4g antenna
Instrument cluster	Provides the visual feedback to the driver for speed, oil, lights etc.	Instrument panel
Vision Control Unit	Handles the localization of the vehicle along with mapping the environment	LIDAR/Cameras Parking Camera GPS tracker
Infotainment Unit	Responsible for handling the user interaction with various services including the media player and the map	Multimedia Platform WiFi USB port Voice recognition

Table 1: Mapping of ECUs to sensors

hardware components that exist in a car, mainly the Electronic Control Units (ECU) for each system of the car for example the Coordinator(COO)[2] or the Tyre Control Unit(TCU) along with a range of antennas for 3g/4g or WiFi signal. Sensors such as the one assisting in parking or more advanced like the LIDAR(Light Detection And Ranging) and USB ports are also included in this category. In order to facilitate the reading of the report, each hardware component will be addressed as the equivalent sensor and not by the corresponding ECU that may encompass more than one sensors. Table 1 lists all the relevant ECUs along with the sensors it handles that will be used as assets in this assessment.

The second category is the software components that exist not only in the car, like the multimedia platform used by the occupants of the vehicle, but also in our back-end infrastructure that help serve the various functions of the vehicle. Third category is the databases and data warehouses. All information about each car is stored in the back-end infrastructure and various data collected from the car in each period help extract useful information about the usage of the car, the strain on components and the share of the market in each city in the country.

2 Business value of System

Our company is not alone in the autonomous car industry and should always strive to be one step ahead of its competitors. To accomplish this, it is important to set clear goals that will continuously attract new customers with the intention to outsell our competitors. These goals must in turn be separated into smaller ones that can be reached through our systems. A complete overview of this decomposition can be seen on Figure 1.

2.1 Goals and Architecture

At this point it is better to show how this separate business goals can be fulfilled by employing some use cases.

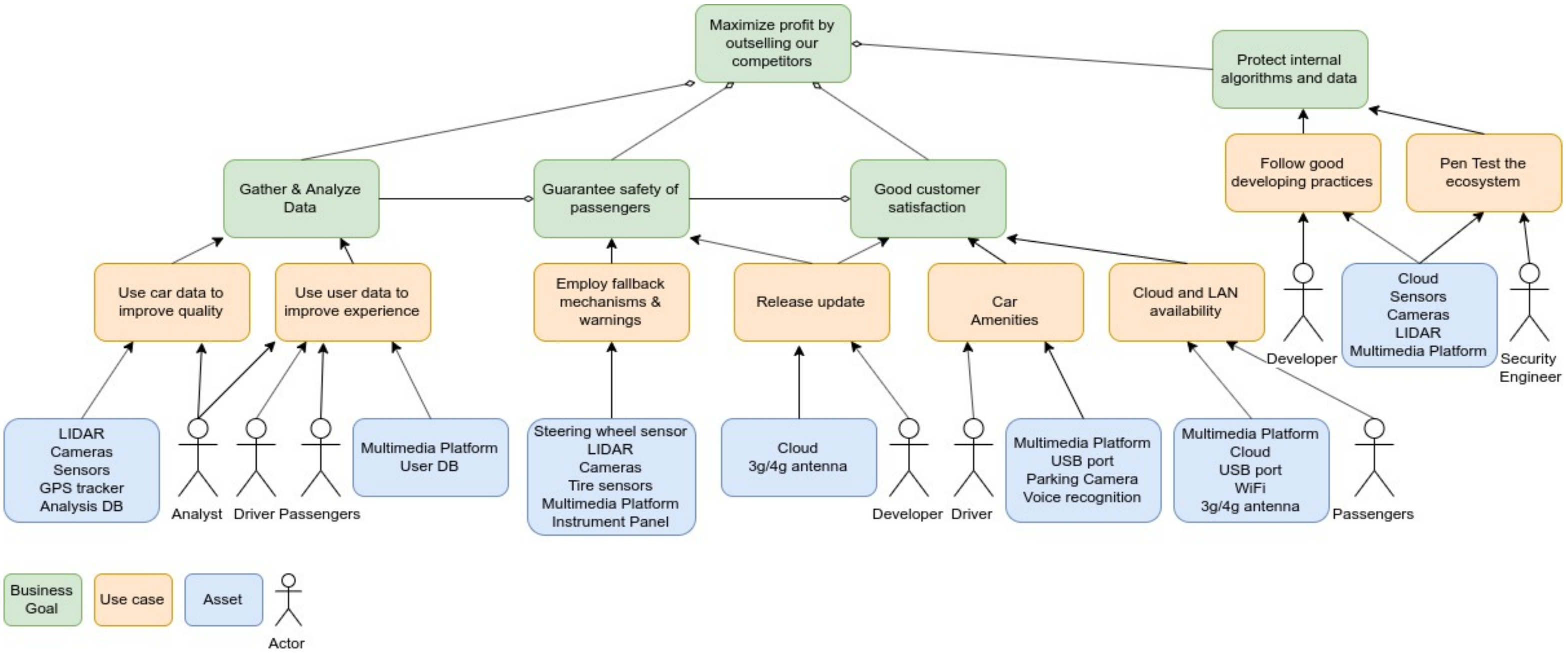
- Gather and analyze data
  This goal is a very important one not only because it provides our company with useful data that can be used to refine our business strategies but it also directly helps to get to the most critical one, safety. For example, by analyzing the tyre behaviour of the car in snowy conditions can help us improve the next generation of our vehicles or apply an upgrade on the same line of cars. An extra benefit, this one aimed at the consumer, can be the fine-tuning of the voice recognition system of the car, to find an address or plan a route, without the need for a mobile device. Another use case would be the logging of real data of fuel consumption inside an urban environment where stops are frequent which are needed to improve our engine or its controller.

- Guarantee safety of passengers
  Because our cars can function in multiple levels of automation it is necessary to have fallback mechanisms when a level of automation can no longer be sustained. When, the LIDAR sensor malfunctions,for any reason malicious or not, the car should continue to function and alert the driver in order for him to take control of the vehicle if necessary. Another critical service that must always function is the pressure sensors on the steering wheel. If the driver falls asleep while driving, the car must notify him not only through an auditory signal but also through vibrating the wheel. If for some reason the driver does not wake up the course of action will be to gracefully take control and direct the car into parking position on the side of the road. The same result should apply in the instance of the tyre sensors detecting critically low levels of pressure.

- Good customer satisfaction
  Guaranteeing the safety of the customer is a good way to make him stay with our brand. Additionally, the car itself should provide some comfort options, like the voice recognition mentioned above, that can enhance the satisfaction of the passengers. Streaming and sharing musing through wireless means with the built-in player, storing music on the personal

cloud of the customer or using a live map is an easy way of providing an enjoyable experience. A pleasant customer experience can also be met by introducing a simple parking camera with an auditory warning when in reverse as an extra safeguard. These systems, though, can not always function perfectly especially when they are first introduced, thus updating the car systems is a required service and not only for satisfying the customer but also for guaranteeing his safety when a security update is needed.

- Protection of internal algorithms and data
  This goal should always be pursued with great consideration because of its ramifications. The first step to achieve it is to make sure through training, supervision and code review that the best practises are followed when developing both our software and hardware. Also, it may seem expensive to conduct a thorough penetration test to our product, both to the car and the cloud service, but proactively mitigating attacks will be proven beneficial in the end. User data or intellectual property theft or perhaps a malicious attack aiming to injure a customer can lead to extreme setbacks not only in terms of monetary value by loosing customers and facing legal action but also by strengthening our competitors if proprietary software falls onto them.



Maximize profit by outselling our competitors
Protect internal algorithms and data
Gather & Analyze Data
Guarantee safety of passengers
Good customer satisfaction
Follow good developing practices
Pen Test the ecosystem
Use car data to improve quality
Use user data to improve experience
Employ fallback mechanisms & warnings
Release update
Car Amenities
Cloud and LAN availability
Developer
Cloud Sensors Cameras LIDAR Multimedia Platform
Security Engineer
LIDAR Cameras Sensors GPS tracker Analysis DB
Analyst
Driver
Passengers
Multimedia Platform User DB
Steering wheel sensor LIDAR Cameras Tire sensors Multimedia Platform Instrument Panel
Cloud 3g/4g antenna
Developer
Driver
Multimedia Platform USB port Parking Camera Voice recognition
Multimedia Platform Cloud USB port WiFi 3g/4g antenna
Passengers
Business Goal
Use case
Asset
Actor

Figure 1: System architecture

2.2 Negative business impacts

At this point, it is crucial to discuss how potential breaches can negatively affect our business. Every breach or more precisely their end result, signified as a loss event, will be tied with the assets involved along with the people, actor, negatively affected by it. Actors can be categorized into internal and external depending on their position related to our company and each loss event will also be given a type for easier categorization[1][7]. There are several things that can be targeted by a malicious actor with a range of impact on the company. In our case, every loss event will be tied with a monetary value for an easier understanding of the impact, value that is calculated based on several factors[3][15]. The cost of *Reputation* loss, for medium and high, is calculated based on replacing the faulty part and up to two times the price of the car[16] due to the same person and a possible friend not buying the same or similar models from our brand while in the case of information leakage it can be greater depending on the scale of the disclosure. The following are some of the malicious attacks that can be performed that lead to the events provided in Table 2 but the list is not exhaustive as these will be discussed later in the report.

- The visual sensors of the car can be tricked by placing stickers on signs, thus, misidentifying them or creating color patterns on the road making the car swerve on a different lane.[6]
- The cloud ecosystem is always online and susceptible to SQL attacks to extract private data, for example daily routine, home address, phone etc.
- A jammer on a rooftop in an urban environment can disrupt wireless communications

3 System definition and decomposition

Before delving deeper, it is crucial to meticulously describe each of the assets listed above. Not all the assets can be directly addressed by either the driver or our company's developers. For the latter, most of the subsystems reside outside the strict boundaries of the business, the car is sold to a customer and the developer can not access its internal components. Furthermore, not everyone should have access to the whole structure, accounts need to be set up with specific permitted operations depending on the target asset. All these intricacies create a complex system that needs to be carefully examined in order to be fully understood and ultimately lead to a productive result.

Firstly, we will separate the assets into three categories, Functions, Data and Networks. Functions is a broad term grouping several categories which in our case complicates things because most of the car sensors and the relevant ECUs are embedded systems that can not only be consider one type, namely hardware. In this report, sensors will be regarded as hardware and ECUs which are responsible for handling them as platforms for the purpose of differentiating

Loss event	Asset	Actor	Type	Cost low k€	Cost mid k€	Cost high k€

Sensor Failure, customer injuries	LIDAR sensor/Cameras	Customer(external)
		CEO(internal)
			injury/death
			Fines
				30
				5
					350
					50
						2500
						500

Sensor Failure	LIDAR sensor/Cameras	Customer(external)	Reputation Replacement	2,5	35	70
User data leaked	User DB	Operations(internal)	Response Fines Reputation	10	50	200
Company data leaked	Analysis DB	Operations(internal)	Response Competitive advantage	10	50	300
Proprietary algorithms leaked	Analysis DB Sensors/ECUs	Operations(internal)	Response Competitive advantage	10	20	100
Analysis DB destroyed	Analysis DB	Operations(internal)	Response	50	375	750
WiFi is down	WiFi	Customer(external)	Reputation	0	5	10
Cloud is down	Cloud service	Operations(internal)	Reputation	0	35	200
Connection to the Cloud fails	3g/4g antenna	Customer(external)	Reputation	0	5	10
Car amenity misbehaves	Multimedia platform Voice recognition USB port	Customer(external)	Reputation	0	5	70

Table 2: Loss events

them. Data and Network represent information residing either in a Database or in transit and means of transmitting data respectively. Table 3 recounts all the assets and assigns to them an actor, there may be multiple, that will use them with an account tied with a set of authorized operations in the form of Create/Read/Update/Delete(CRUD)[19]. In Table 4 only Functions are listed along with their type, their ownership in relation to the business and their ability to send(Server) and receive(Client) data which is important from a security point of view.

Because the reading of Table 3 especially for the cases where there are multiple actors can become a bit obscure, the assets are also presented in a grouped manner in order to make their comprehension easier. Finally, a special actor also exists in Table 3, specifically the Security Engineer. He is responsible for evaluating the robustness of the whole setup, all assets, and is only placed as an actor for the Cloud platform for the purpose of saving space.

- Simple cases
  Some of the assets can only interact with their respective ECU, for example LIDAR, which is used as part of the autonomous functionality of the vehicle while others like the multimedia platform is solely used by the passengers.

- Electronic Control Units

It may seem strange but the only actor that interacts with those subsystems is the Coordinator. The connection between them is facilitated by the Controller Area Network(CAN), a special vehicle bus indented to connect microcontrollers which is not represented as an asset in this document[11].

- Multiple Actors per Asset
  In the interest of disambiguation these assets are also presented in Figure 2, Figure 3, Figure 4, Figure 5, Figure 6 and Figure 7.

Asset	**Type**	**Actor**	**Account**	**Authorization**
LIDAR	Hardware	Vision Control Unit		RU
Parking Camera	Hardware	Driver	Vision Control Unit	RU
GPS tracker	Hardware	Vision Control Unit		R
Vision Control Unit	Platform	Coordinator ECU		RU
Multimedia Platform	Service	Driver & Passengers	Infotainment Unit	CRUD
WiFi	Network	Driver & Passengers	Infotainment Unit	CRUD
USB port	Hardware	Driver & Passengers	Infotainment Unit	CRUD
Voice recognition	Service	Driver & Passengers	Infotainment Unit	CRUD
Infotainment Unit	Platform	Coordinator ECU		RU
Instrument Panel	Service	Driver	Instrument Cluster	R
Instrument cluster	Platform	Coordinator ECU		RU
3g/4g antenna	Hardware	Driver & Passengers Coordinator ECU	Telematics Control Unit	RU
Telematics Control Unit	Platform	Coordinator ECU		RU
Steering Wheel sensor	Hardware	Driver Steering System	Steering System	R
Steering Wheel vibrator	Service	Steering System		U
Steering System	Platform	Coordinator ECU		RU
Tyre pressure/traction sensor	Hardware	Tyre Unit		R
Tyre Unit	Platform	Coordinator ECU		RU
Cloud	Platform	Driver & Passengers Developer Security Engineer	Telematics Control Unit DevWorker SecWorker	RU CRUD CRUD[*]
Analysis DB	Data	Coordinator ECU Analyst	Telematics Control Unit DataWorker	U RU
User DB	Data	Driver & Passengers Analyst	Telematics Control Unit DataWorker	CRUD R
Coordinator ECU	Platform	Driver Coordinator ECU		U RU

[*] Special case where authorization may or may not exist but can potentially be gained.

Table 3: System Components and authorization

Asset	Type	Ownership	Role
LIDAR	Hardware	External	Server
Parking Camera	Hardware	External	Server
GPS tracker	Hardware	External	Server
Vision Control Unit	Platform	External	Client/Server
Multimedia Platform	Service	External	Client/Server
USB port	Hardware	External	Client/Server
Voice recognition	Service	External	Server
Infotainment Unit	Platform	External	Client/Server
Instrument Panel	Service	External	Client
Instrument cluster	Platform	External	Client/Server
3g/4g antenna	Hardware	External	Client/Server
Telematics Control Unit	Platform	External	Client/Server
Steering Wheel sensor	Hardware	External	Server
Steering Wheel vibrator	Service	External	Client
Steering System	Platform	External	Client/Server
Tyre pressure/traction sensor	Hardware	External	Server
Cloud	Platform	Internal	Client/Server
Coordinator ECU	Platform	External	Client/Server

Table 4: Asset Roles and Ownership

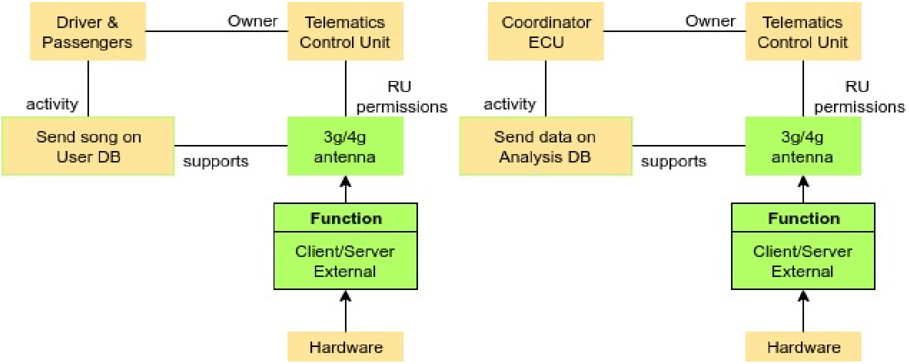


Figure 2: 3g/4g Antenna - Driver(left) - Coordinator ECU(right)

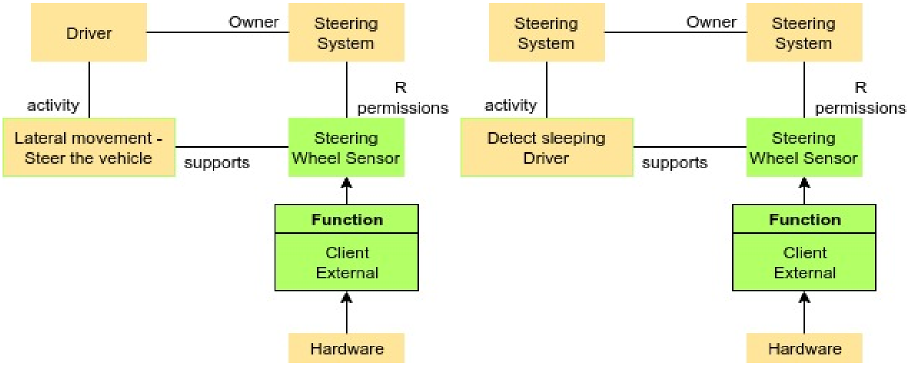


Figure 3: Steering Wheel - Driver(left) - Steering System(right)

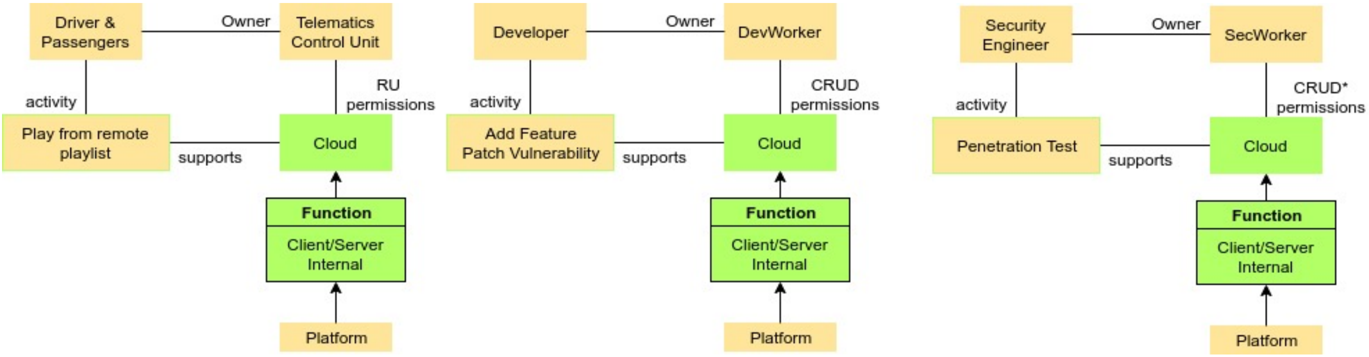


Figure 4: Cloud - Driver(left) - Developer(center) - Analyst(right)

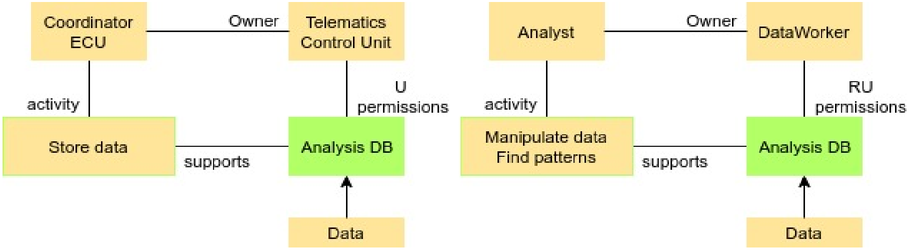


Figure 5: Analysis DB - Coordinator ECU(left) - Analyst(right)

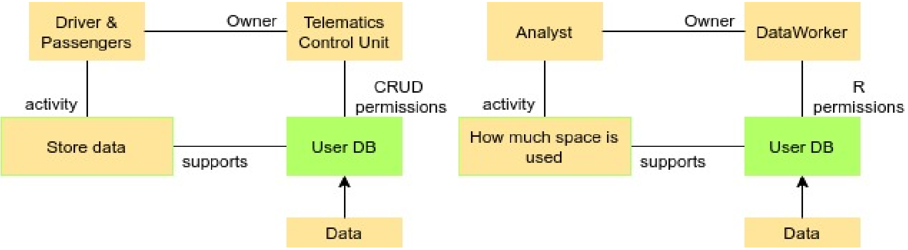


Figure 6: User DB - Driver/Passengers(left) - Analyst(right)

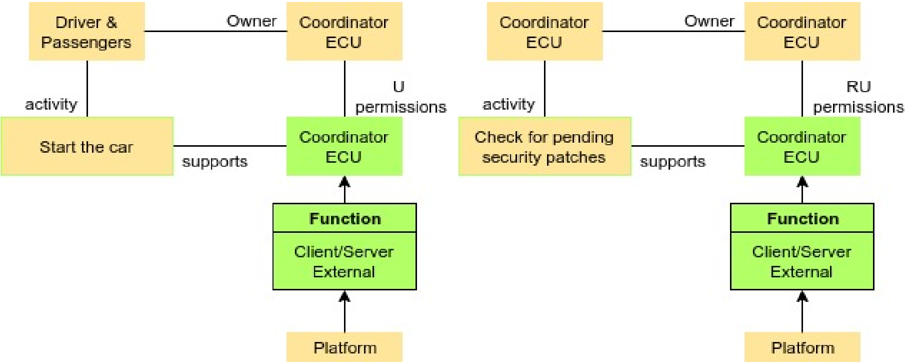


Figure 7: Coordinator - Driver/Passengers(left) - Coordinator ECU(right)

3.1 Data flow

So far we have discussed the business goal of our enterprise along with potential setbacks and we connected the portrayed assets with use cases but we have yet to show a full overview of our setup. We will do that by presenting several data flow diagrams using the notation depicted in Figure 8. By trust boundary we signify the extra precaution needed in dealing with data that traverse over it because their source or their content can not necessarily be trusted. Figure 9 presents a macroscopic view of our architecture showing the flow of information between each vehicle and our back-end infrastructure. On the other hand, Figure 10 contains all the relevant information from the perspective of the automobile.

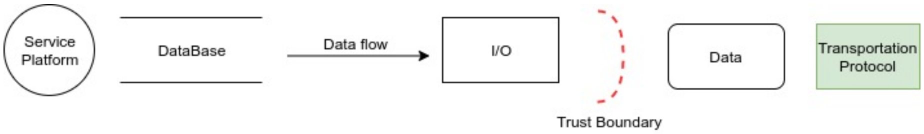


Figure 8: Data flow Diagram notation

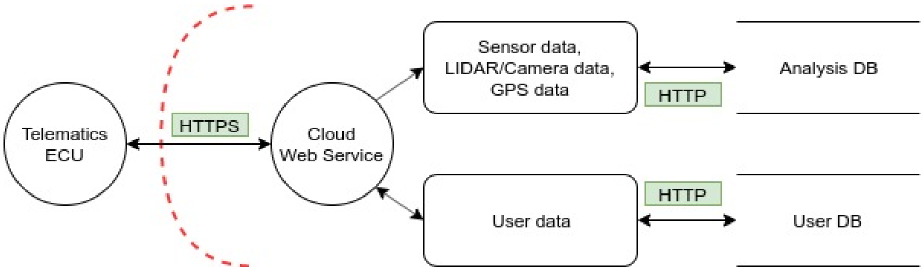


Figure 9: Macroscopic view

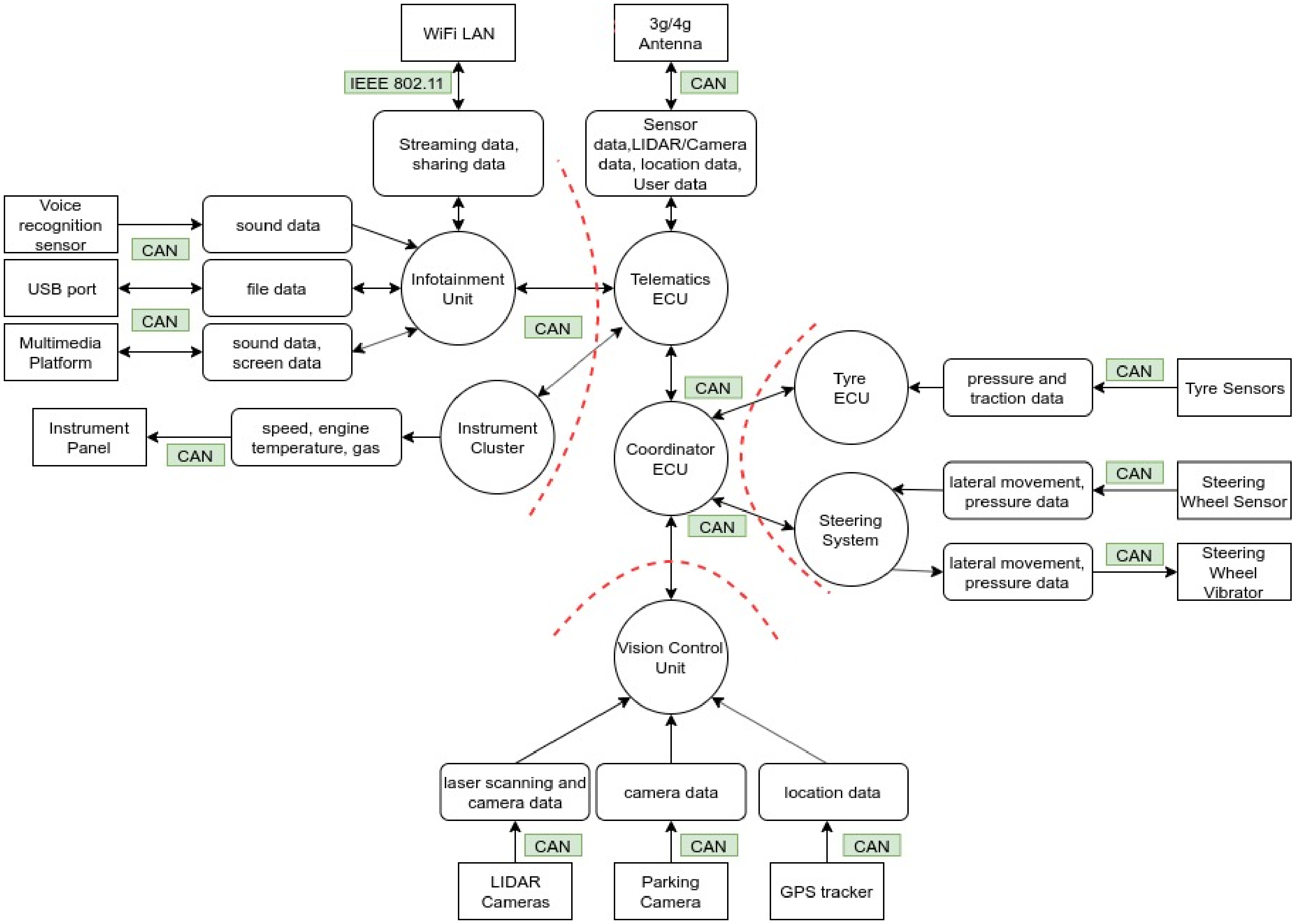


Figure 10: Vehicle view

4 Threat Analysis

Every company that exists in our digital society faces cyber threats regardless of its nature of business stemming mainly from the fact that that data have intrinsic value. They can then be sold, used as blackmail or used as a stepping stone for further attacks. This is the main reason for the ever expanding cyber crime industry[12] which consists of a plethora of individuals, from amateurs to highly skilled. But data are no the sole targetable asset of an enterprise. The very same infrastructure that fuels our organization, especially with its inherent distributed setup, can be used as a position to perform Distributed Denial of Service attacks(DDoS)[9], that is, to saturate the resources of a target thus rendering him inoperable. Such a network of otherwise benign device or in our case cars can be a valuable target for individuals or criminal organizations that seek to either undermine a third party or even us through bad publicity.

4.1 Attacker Profiling

With that in mind, we have to first define the various groups that can pose a risk to us and assign them a level of threat based on certain attributes like their personal risk tolerance and their concern for collateral damage particularly in our case where the consequences can also involve peoples' lives. On the other hand, availability of resources both in terms of money or knowledge is crucial because of the difficulty of exploring internal characteristics of vehicles. These actors are listed in Table 5 and they are given a threat capability percentage that will be used later when assessing the overall risk.

- Script kiddies
  This category of hackers is consisted of people who are either amateurs in the field or have no programming expertise, hence the name, but are able to use preexisting tools to mount their attacks. They may not be perceived as the biggest threat but the low level of knowledge needed makes this group a numerous one. They usually act alone without large resources behind them and more of than not are more cautious when taking risks.

- Hacktivists
  This group of people are most of the time motivated by their ideologies for social change and do not have malicious intend for performing their attacks[14]. Therefore they will not be further analyzed here but are included for completeness.

- Employees
  This class is noteworthy mostly because of their first hand knowledge of our ecosystem. Depending on their skills and background this can offer them a huge advantage, both in terms of finding vulnerabilities and bypassing defenses, and should be reflected when giving them their threat capability. Because their motive can vary, for example a disgruntled employee may not concern himself with the fallout of his actions, their threat is also adjusted to accommodate that.

Actor	**Script Kiddie**	**Employees**	**State Hackers**	**Competitor Hackers**
personal risk tolerance	low	medium	high	medium
concern for collateral damage	high	medium	low	medium
skill	low	medium	high	high
resources	low	medium	high	high
sponsorship	none	none	high	none
Threat Capability	5%	40%	95%	60%

Table 5: Profile of Attackers

- State sponsored Hackers
  State sponsored hackers consist of individuals with advanced knowledge of their craft with the added advantage of huge resources and backing from their country. These kind of hackers do not necessarily have any industry preference and have been found attacking a plethora of targets from media and law firms to governments[4]. It is also not unheard for these kind of groups to go to great lengths to target infrastructure[10] and their volume of operations should not be ignored compared to other types of parties[17]. In our case, this means that there should be a constant concern in securing our assets against adversaries that exceed the typical kind of hackers. From all the actors listed, these adversaries are the only ones with the sponsorship attribute which also includes legal backing.

- Competitor backed Hackers
  Considering the market size of the automotive industry, every advantage that can be gained over a competitor can lead to great profits or loses, for the victim, which provides a great incentive to perform trade secret theft. Also, depending on their goals, consequences can be disregarded leading them on taking greater risks to achieve them.

4.2 Abuse cases

Abuse cases like use cases are a form of interaction with the system but contrary to the latter the intent is malicious and the result is often a loss event. In the same manner, they are tied to an asset and require a point of entry(Attack Surface) in order to reach it. In order for the abuse cases to have any value to our assessment they need to produce a metric that corresponds to how often they can be realized. This metric, we call it Threat Event Frequency and it is generated based on the *Contact Frequency* and the *Probability of Action*,via multiplication, from the view of the intruder. Contact Frequency denotes the number of days the attack surface is available to an attacker while the Probability of Action is derived from several factors like the perceived easiness of performing the attack and the benefits that will be gained combined with the characteristics pertaining to the actor.

Abuse case	**Trick LIDAR**		
Target asset	LIDAR		
Attack Surface(AS)	Vision Control Unit		
Accessibility to AS	Always, being in the vicinity of the car		
Window of opportunity	Car passes		
Resources	Stickers		
Contact Frequency	104	365	365
Chances to protect ourselves	Refine recognition algorithm		
Perceived deterrence	Low, the stickers can be placed when no one is around		
Perceived feasibility	low	medium	high
Perceived benefit	Fines/Reputation	Injury/Death	Fines/Reputation
Probability of Action	2	15	10
Threat Event Frequency	2,08	54,75	36,5
Loss event	Sensor failure		
Threat Agent	Employee	State sponsored	Competitor sponsored

Table 6: Trick LIDAR

In order to promote comparison abuse cases that can be performed by more than one parties are depicted in a table fashion while cases that are probably to be performed by single groups will be presented as graphs.

- Trick LIDAR
  This abuse case can give rise to an unexpected observation when it comes to the aggressor. The rogue employee has the least resources leading to a smaller contact frequency(twice per week) with the asset. Depending on his background, the feasibility of knowing how to perform the attack is closer to a lower value which affects his action prospects as depicted in Table 6, with the state coming second as the state actor is not necessarily knowledgeable in the field but has the resources and contacts to make the attack attainable. On the other hand, the competitor is possible to have a system functioning in a similar manner thus making the attack easier. Lastly, the probability that the employee will carry on with the plan is again the smallest with the state coming first despite the ease of performing the attack because of their unique characteristic, no concern for collateral damage.

- Extract DB data
  Here, all the groups described previously can take action and shown in Table 7. Most of them have different reasons to exfiltrate data from our company but user specific data are a valuable target even for the state, for example to correlate them with other information to identify a spy. The script kiddie has the least probability mainly because of his risk tolerance with the employee coming second. Both the state and the competitors have the same probability for different reasons, the state is less likely

to perform such an attack while the competitor is more concerned with avoiding getting caught.

- Jam signal
  In this occasion the script kiddie and the competitor are the ones who are probably going to utilize this form of attack. The first one most likely for fun while the latter for damaging our reputation. The state is addressed here because it may affect us unintentionally by using jamers for reasons unrelated to us and is noted as such in Table 8.

- Reverse engineer asset
  Two actors are relevant in the case of reverse engineering, the state and a competitor of ours. The target in this case can be any ECU as they contain the useful data and the decision making code used in our cars. The cost limited to buying the car and the tools and cables to connect to the ECUs thus making this attack feasible while its nature makes a possible deterrence from our part harder. Clearly, the goal of our competitors is to gain an unfair advantage and this is reflected in their probability of action over us while for the state it could be to gain insight of inner systems that can be used as nodes in a botnet or perhaps as a staging step for another exploitation. The illustration of this is shown in Table 9.

- DDoS Cloud Service
  A common attack scenario for every business,Table 10 lists the relevant information regarding the parties involved, script kiddies and our competitors. The motivation for the former would be gaining experience and building a reputation, hence also the bigger probability of performing that action, while the latter to disrupt our normal business functionality leading to imperfect user experience.

- Alter amenity behaviour
  The last abuse case is given in Figure 11 and showcases an interesting attack that can be performed upon our assets by state backed people in a standalone fashion,after reverse engineering certain neighboring components and using them as a point of entry or even through the software update functionality reserved for security patches. The Contact frequency depends on the way the attack happens and is assigned a medium to low value to reflect that physical access may be necessary. Such an attack has a high probability of being executed because of its high reward.

Abuse case	**Extract DB data**			
Target asset	User DB			
Attack Surface(AS)	Cloud			
Accessibility to AS	The service is always running			
Window of opportunity	All the time			
Resources	Hacking skill or specialized tools			
Contact Frequency	365			
Chances to protect ourselves	Code inspection/Penetration Testing/Encrypted data			
Perceived deterrence	high	medium	low	medium
Perceived feasibility	High, even for amateurs exploits are available.			
Perceived benefit	Sell for money	Reputation/Fines Sell for money	User data Reputation loss	Competitive advantage
Probability of Action	5	15	20	20
Threat Event Frequency	18,25	54,75	73	73
Loss event	Sensor failure			
Threat Agent	Script Kiddie	Employee	State sponsored	Competitor sponsored

Table 7: Extract user data

Abuse case	**Jam signal**			
Target asset	3g/4g Antenna or WiFi			
Attack Surface(AS)	Telematics Control Unit, Network			
Accessibility to AS	Always			
Window of opportunity	Car passes from the area			
Resources	Specialized tool, jammer			
Contact Frequency	104	104	365	365
Chances to protect ourselves	Low, it is not feasible to have specialized anti-jamming technology in each car			
Perceived deterrence	Low, actor can hide in plain sight/station jammer on roof			
Perceived feasibility	High, toolkits already exist or can be made easily			
Perceived benefit	Fun	Reputation	Unintentionally	Reputation
Probability of Action	10	5	1	10
Threat Event Frequency	10,4	5,2	3,65	36,5
Loss event	Cloud connection failure/WiFi down			
Threat Agent	Script Kiddie	Employee	State sponsored	Competitor sponsored

Table 8: Jam signal

Abuse case	**Reverse engineer component**	
Target asset	ECUs	
Attack Surface(AS)	ECUs	
Accessibility to AS	Requires access to a car	
Window of opportunity	Always, because the car needs to be bought	
Resources	Low, price of specialized tool and cables	
Contact Frequency	365	
Chances to protect ourselves	Low, code obfuscation	
Perceived deterrence	Low	
Perceived feasibility	Medium, time and knowledge of the underlying systems is needed	
Perceived benefit	Infrastructure knowledge	Competitive advantage
Probability of Action	10	30
Threat Event Frequency	36,5	109,5
Loss event	Proprietary algorithms leaked	
Threat Agent	State sponsored	Competitor sponsored

Table 9: Reverse engineer component

Abuse case	**DDos attack**	
Target asset	Cloud	
Attack Surface(AS)	Cloud	
Accessibility to AS	Always reachable	
Window of opportunity	Always	
Resources	Low	
Contact Frequency	365	
Chances to protect ourselves	Medium/High, traffic analysis and honeypots are valid options	
Perceived deterrence	Medium	
Perceived feasibility	Medium	High
Perceived benefit	Experience	Reputation
Probability of Action	10	5
Threat Event Frequency	36,5	18,25
Loss event	Cloud is down	
Threat Agent	Script kiddie	Competitor sponsored

Table 10: Cloud DDoS

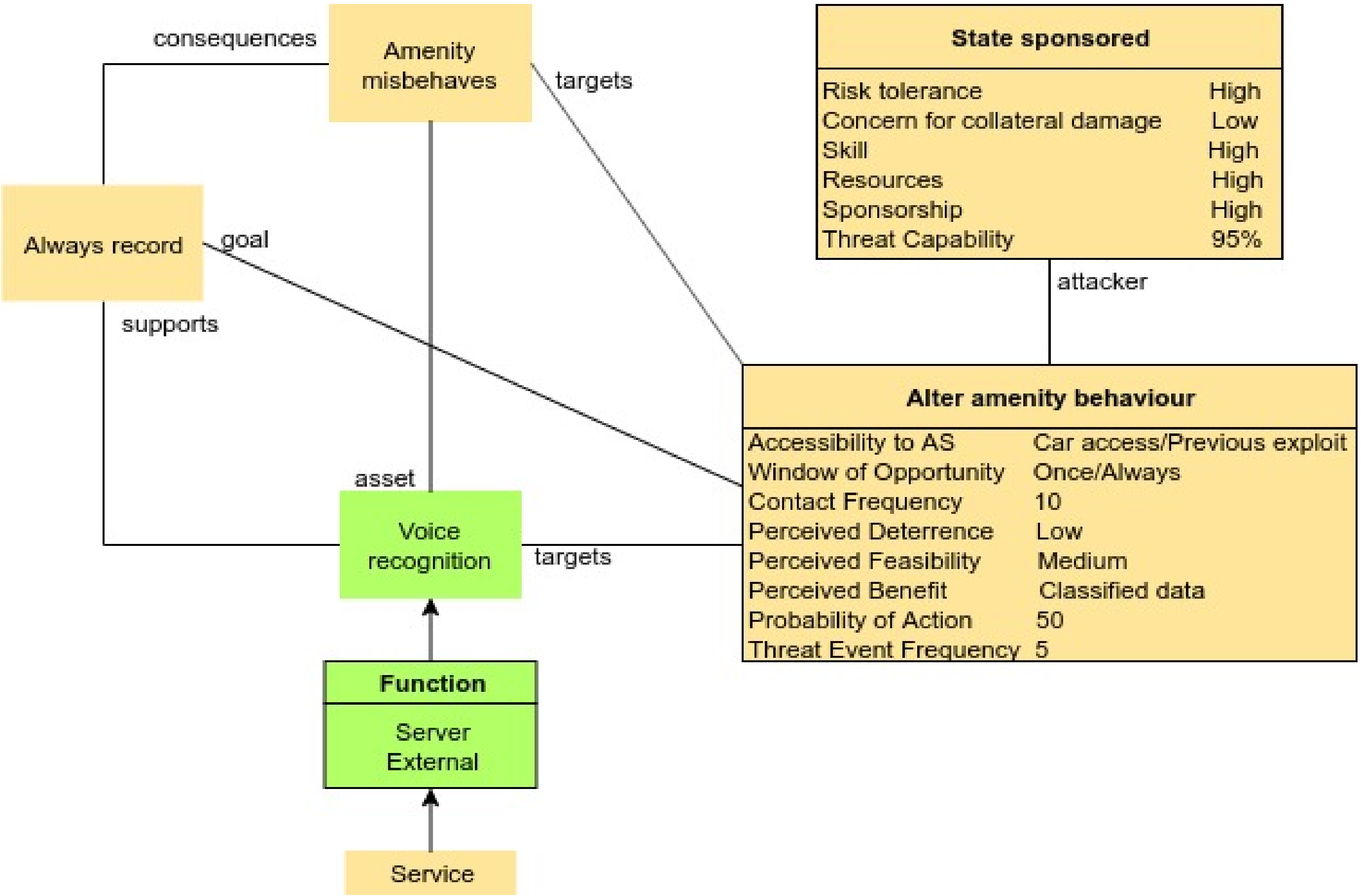


Figure 11: Alter amenity behaviour

Vulnerability	**Severity**	**Asset**
Remote code execution(CVE-2018-9318,CVE-2019-13980)	10	Telematics Control Unit/Cloud
Improper certificate validation(CWE-295)	10	Cloud
Neural network input perturbation(CWE-1039)	9	LIDAR
Local code execution(CVE-2018-9320)	9	Infotainment Unit
SQL injection(CWE-89)	8	Analysis/User DB
Improper Authentication(CWE-287)	8	Cloud - Analysis/User DB
Weak Passwords Requirements(CWE-521)	7	Cloud - Analysis/User DB
DDoS Vulnerability(CWE-410)	6	Cloud
Security through obscurity(CWE-656)	6	ECUs/Multimedia Platform/USB port
Bad developing practises(CWE-395)	4	Cloud
Signal jamming(CVE-2018-15181)	3	WiFi - 3g/4g antenna
Insufficient logging(CWE-778)	3	ECUs

Table 11: Vulnerabilities

5 Attack and Resilience Analysis

Now that we have identified potential aggressors and listed several abuse cases it is crucial to understand how an attacker can reach the attack surface. More often than not this is done by exploiting some form of weakness or vulnerability in the system, either in the form of a software bug or one created by a design flaw. Table 11 demonstrates some of them coupled with a severity value ranking them, in descending order, based on the qualitative levels given by the Common Vulnerability Scoring System(CVSS)[13].

To demonstrate how the attacker can reach his end goal, illustrated as abuse case, we present several attack trees where each node corresponds to a single step forming a path from the starting point, the first hurdle for the attacker, all the way to his objective. Each step is assigned an intrinsic cost, best, expected and worst case, that is aggregated after each step to signify the total cost needed at the end. The attack trees will follow the notation given in Figure 12 and will also depict the right countermeasures related to the attack steps. The DDoS case is a special one because all the actions required to perform it lie outside the boundaries of our setup thus it is not presented as an attack tree but as a graph. Two things need to be mentioned here before we delve into the trees, finding a vulnerability was set to the numbers of twenty in order to give room both below and above and already discussed vulnerabilities are set to low numbers to signify that they are known and can be used by everyone without too much knowledge. That, however, means that paths building from these steps are not necessarily the best regardless of their preference in the attack trees.

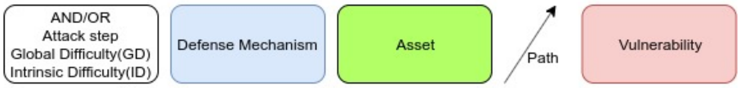


Figure 12: Attack Trees notation

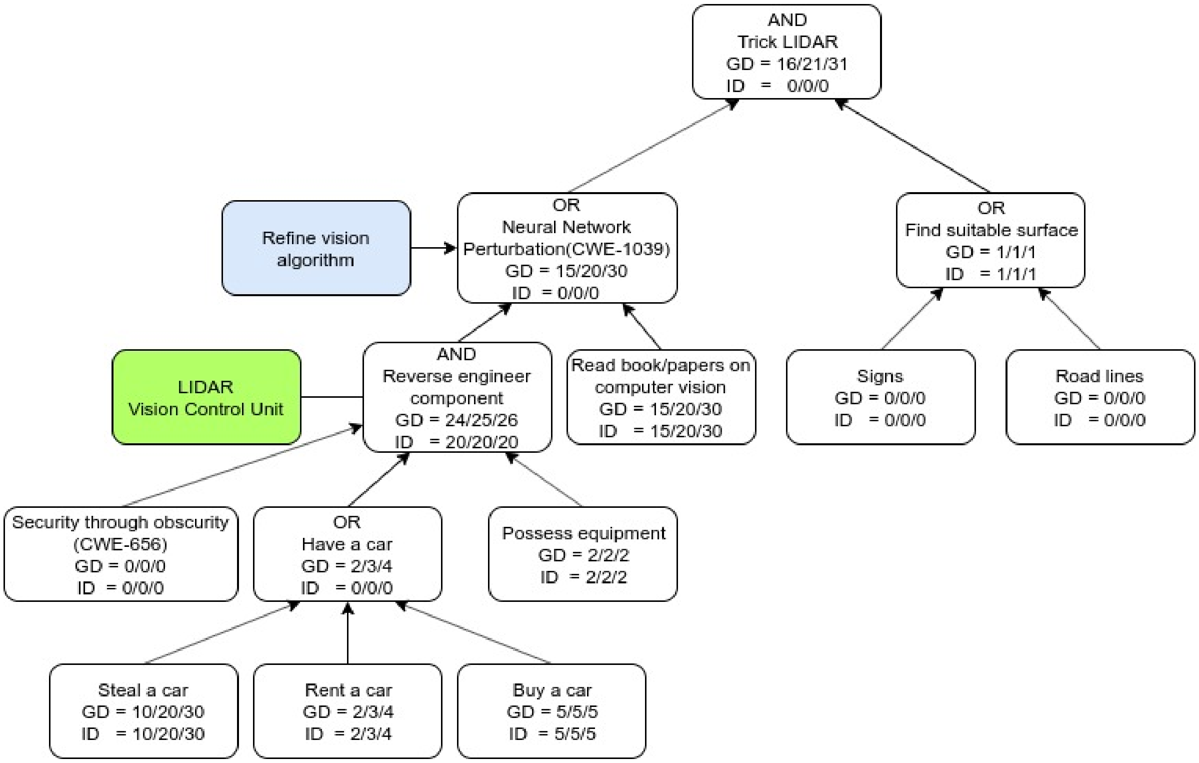


Figure 13: Trick LIDAR tree

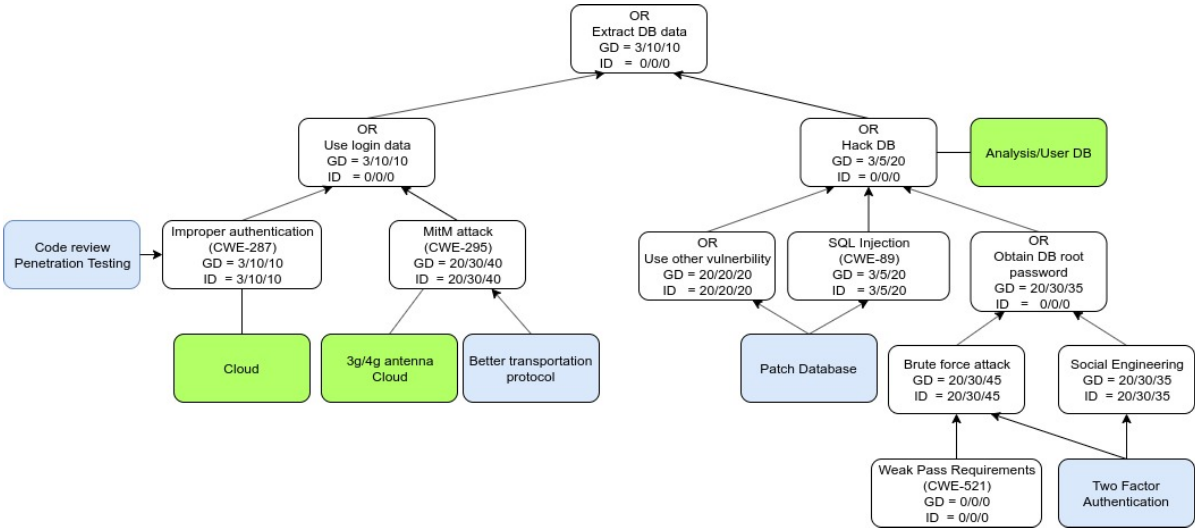


Figure 14: Extract DB data tree

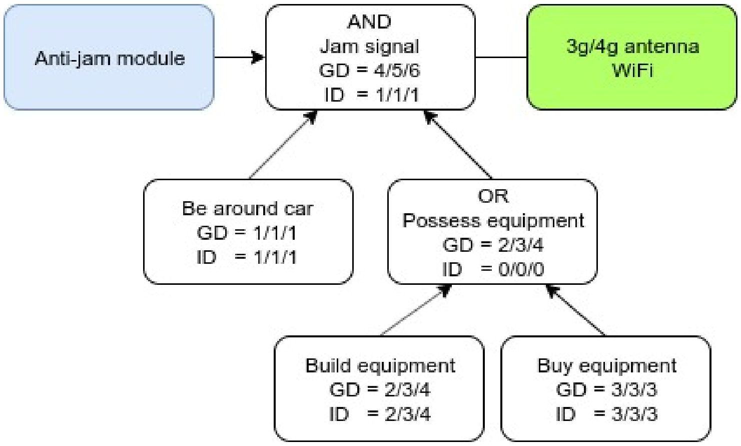


Figure 15: Signal jamming tree

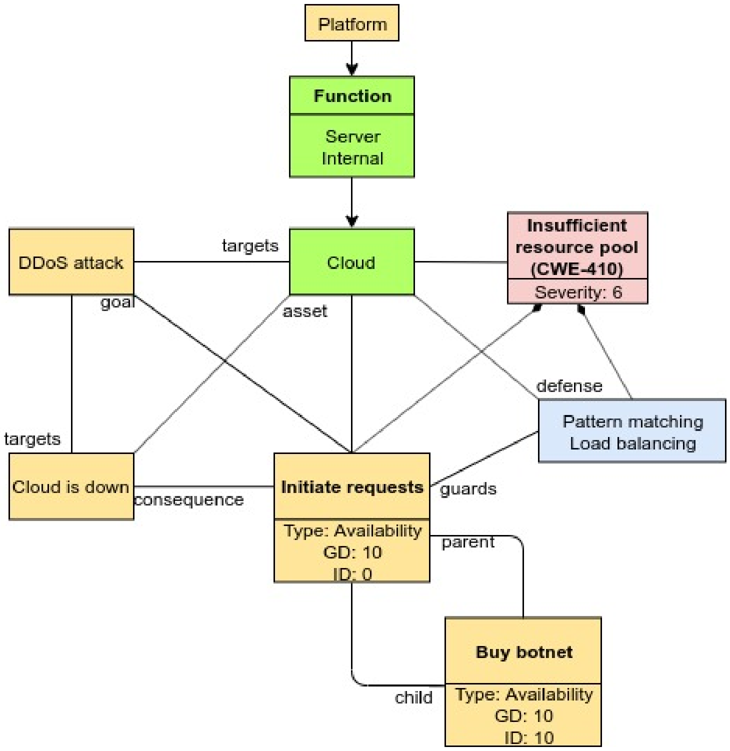


Figure 16: DDos attack graph

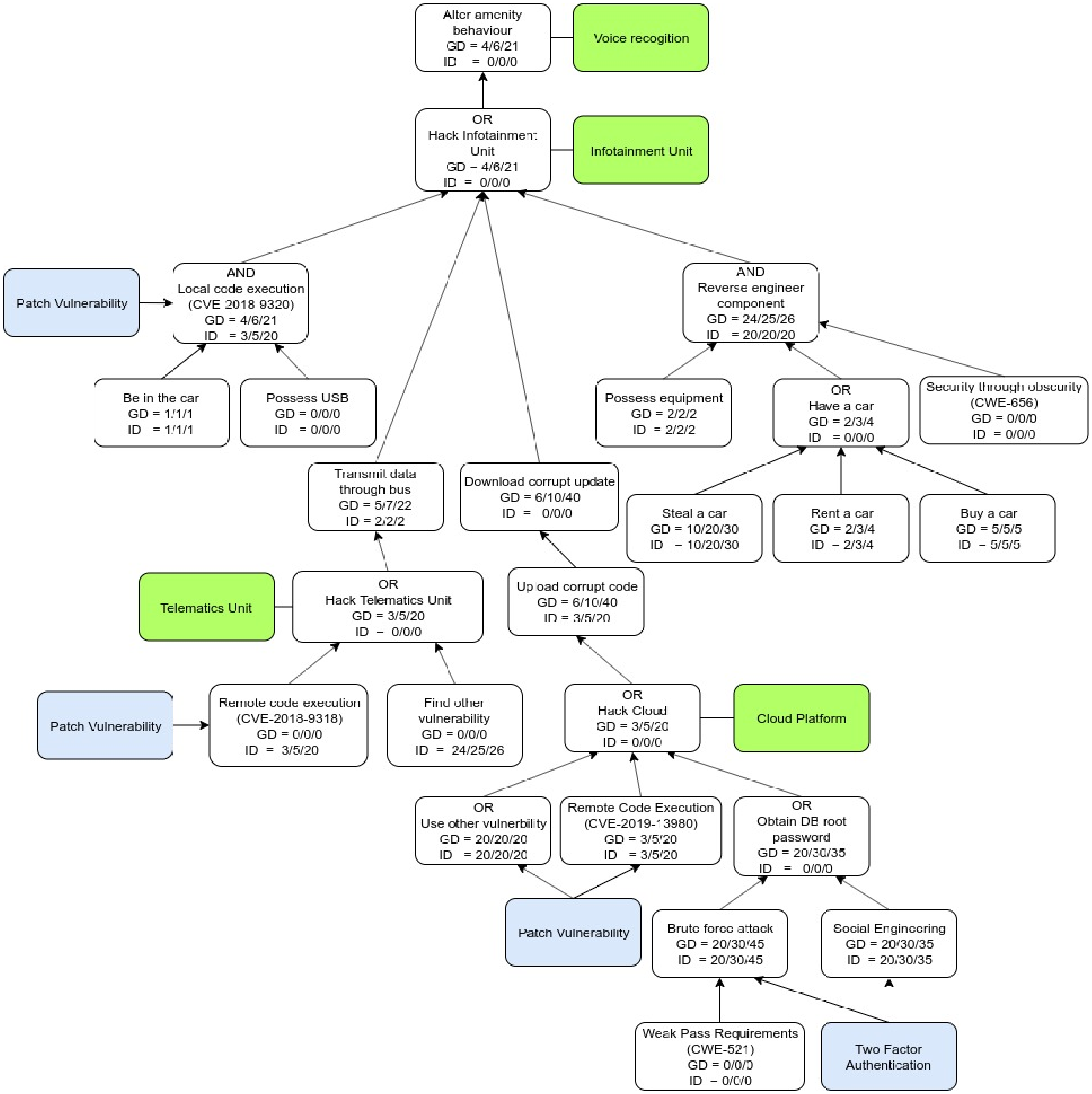

Alter amenity behaviour GD = 4/6/21 ID = 0/0/0
Voice recogition
OR Hack Infotainment Unit GD = 4/6/21 ID = 0/0/0
Infotainment Unit
Patch Vulnerability
AND Local code execution (CVE-2018-9320) GD = 4/6/21 ID = 3/5/20
AND Reverse engineer component GD = 24/25/26 ID = 20/20/20
Be in the car GD = 1/1/1 ID = 1/1/1
Possess USB GD = 0/0/0 ID = 0/0/0
Possess equipment GD = 2/2/2 ID = 2/2/2
OR Have a car GD = 2/3/4 ID = 0/0/0
Security through obscurity (CWE-656) GD = 0/0/0 ID = 0/0/0
Transmit data through bus GD = 5/7/22 ID = 2/2/2
Download corrupt update GD = 6/10/40 ID = 0/0/0
Steal a car GD = 10/20/30 ID = 10/20/30
Rent a car GD = 2/3/4 ID = 2/3/4
Buy a car GD = 5/5/5 ID = 5/5/5
Telematics Unit
OR Hack Telematics Unit GD = 3/5/20 ID = 0/0/0
Upload corrupt code GD = 6/10/40 ID = 3/5/20
Patch Vulnerability
Remote code execution (CVE-2018-9318) GD = 0/0/0 ID = 3/5/20
Find other vulnerability GD = 0/0/0 ID = 24/25/26
OR Hack Cloud GD = 3/5/20 ID = 0/0/0
Cloud Platform
OR Use other vulnerbility GD = 20/20/20 ID = 20/20/20
Remote Code Execution (CVE-2019-13980) GD = 3/5/20 ID = 3/5/20
OR Obtain DB root password GD = 20/30/35 ID = 0/0/0
Patch Vulnerability
Brute force attack GD = 20/30/45 ID = 20/30/45
Social Engineering GD = 20/30/35 ID = 20/30/35
Weak Pass Requirements (CWE-521) GD = 0/0/0 ID = 0/0/0
Two Factor Authentication

Figure 17: Alter amenity behaviour tree

6 Risk assessment and recommendations

6.1 Risk assessment

In order to measure the overall risk, a combination of all the above measurements will be used. Risk will be calculated in the manner depicted in Figure 18. The only missing value is the *Probability of success* which is derived from the attack difficulty and the effort spend from the attacker which we will address here. The effort spent is influenced by the same parameters that *Probability of Action* was when we were discussing the abuse cases. It depends heavily on the personal risk tolerance of the attacker and the perceived benefit from following through with his actions, the results are introduced in Table 12.

- Trick LIDAR
  There is an inherent difficulty in performing this attack but a rogue employee has elevated chances of succeeding especially if his position is close to the asset at hand making the endeavor worthwhile. The other two actors, have both the means and the time to realize it giving them better changes of a positive result.

- Extract DB data
  In this case, all the actors have elevated probability because these kinds of attack are common for a reason, easy to miss bug and many exploits floating around. With that in mind, the script kiddie has the least because he does not have the expertise to develop an exploit from scratch thus if one does not exist already he will halt. The rest, are capable and motivated to succeed and again in this case the rogue employee has better chances because he is already inside the trust boundary and can potentially have relevant passwords.

- Jam signal
  Because this attack is not hard to implement and one can find similar products on the market the chances of success are considerably high. The state actors and the competitors backed hackers are guaranteed to succeed here.

- Reverse engineer components
  This one is one of the hardest because it requires good knowledge of several underlying systems that exist inside a car. Also, the benefit here would be either a competitive advantage or the creation of an exploit which is not the goal of every actor. Both the state and the competitor backed groups are guaranteed high percentages here because of their resources and knowledge of the designs.

- DDoS
  Relative similar to the signal jamming, this attack is not necessarily hard to perform. Apart from that, not everyone is interested in disrupting

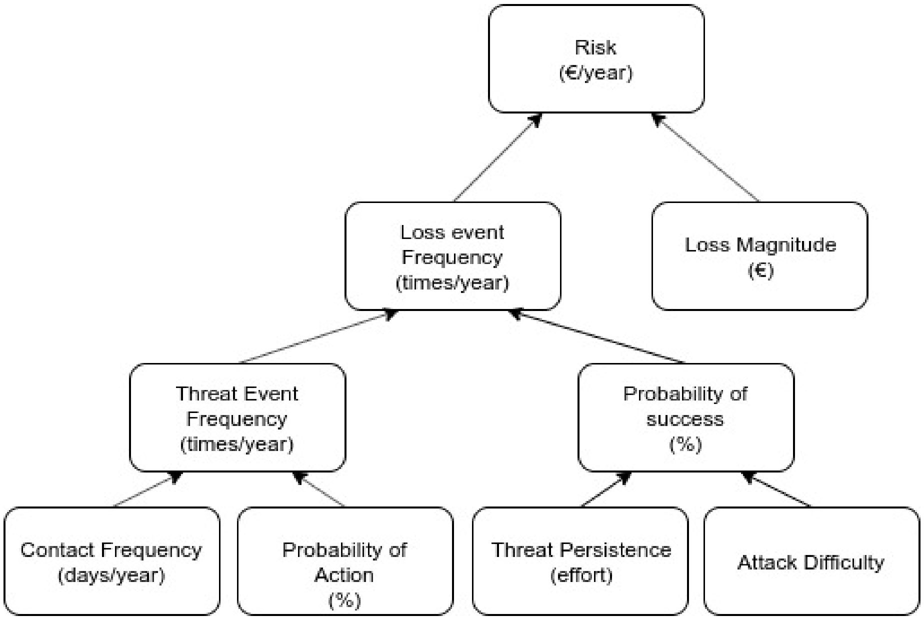


Figure 18: Risk calculation strategy

the operation of a service such as ours leaving only script kiddies and competitors to pursue it.

- Alter amenity behaviour
  Equally here, as in reversing the components, the knowledge needed is a prohibiting factor and without an already known weakness the chances of success are slim for amateurs. Depending on the circumstances and the end goal of doing such a sophisticated attack the chances of paying off are moderate.

Now that we have computed the Probability of success it is time to calculate the risk for the actors affected in our loss events. We have three, the customer, the CEO and the operational cost from loss of reputation, fines and response

	Script kiddie	Employee	State	Competitor
Trick LIDAR	-	30	60	70
Extract DB data	35	60	70	50
Jam signal	70	70	100	100
Reverse engineer component	-	-	90	80
DDoS attack	60	-	-	90
Alter amenity behaviour	-	-	75	-

Table 12: Probability of Success

Sensor Failure with injury	1.770.720	2.065.840	147.560.000
Sensor Failure	147.560	2.065.840	4.131.680
Wifi down/Failed Connection to Cloud	0	255.350	510.700
Car amenity misbehaves	0	18.750	262.500
Customer Risk	1.918.280	4.405.780	152.464.880

Table 13: Customer's risk

User data leaked	1.268.375	6.341.875	25.367.500
Company data leaked	1.268.375	6.341.875	38.051.250
Proprietary algorithms leaked	602.250	2.409.000	12.045.000
Cloud is down	0	18.750	262.500
Operational Risk	3.139.000	16.434.125	83.128.750

Table 14: Operational risk

teams. Table 13 lists the customer's risk while Table 14 and Table 15 the business and the CEO respectively. It should immediately strike as strange the max cost for all three actors. This is due to the event involving death where the worst case scenario consists of 96% of the total cost. This is primarily because both the state and the competitor are able to have a vehicle all year long leading to a high Threat Event Frequency. Having said that, even in the case where the LIDAR sensor fails unexpectedly the autonomous functionality will continue to be in control of the car by using the other cameras until the driver is able to resume driving the vehicle thus the value does not necessarily tells the whole truth.

6.2 Protection scenarios

We have identified several protection scenarios already when describing the attack trees. Additionally, because the bulk of our setup relies outside of our immediate control it is of great importance to have some form of control of those assets, through the use of logs. Table 16 gathers all those mechanisms in a single place for faster reference.

- Refine vision algorithm
  This particular mechanism is of great importance because of the impact this weakness can have.The fact that we have an in-house department focusing on neural networks and computer vision is a plus when considering the cost, but nevertheless, research and development in this sector is a

Sensor failure with injury	295.120	2.951.200	29.512.000
CEO risk	295.120	2.951.200	29.512.000

Table 15: CEO risk

Defense mechanism	**Asset**	**Cost**
Refine vision algorithm	Vision Control Unit	Medium
Code review	ECUs/Cloud Platform	Medium
Penetration Testing	ECUs/Cloud Platform	Medium/High
Better transportation protocol	3g/4g antenna - Cloud	High
Patch DB vulnerabilities	Databases	Low/Medium
Two-Factor Authentication	Cloud Platform - Databases	Low
Anti-Jam module	Telematics Control Unit	High
Pattern matching	Cloud Platform	Low
Load balancing	Cloud Platform	Low
Patch Car Vulnerabilities	ECUs	Low/Medium
Patch Cloud Platform Vulnerabilities	Cloud Platform	Low/Medium
ECU data logging	ECUs	Low/Medium

Table 16: Defense Mechanisms

time consuming process.

- Code review
  This approach to resolving bugs before they appear in a production environment has many merits if done correctly. Bugs are an unavoidable consequence of writing code and can emerge in the most unexpected places leading to potential big security flaws. The cost of performing this this activity constantly is of medium value because it inadvertently requires developer work hours to be spend.

- Penetration Testing
  Huge potential in finding vulnerabilities but with the cost of hiring engineers to do it or outsourcing it to third parties with the accompanying cost. A possibility here would be to promote bounty programs as a low cost alternative. The results can vary depending on the scrutiny of the process and it requires continuous application especially when there are architectural and design changes.

- Better transportation protocol
  This is solely the focus of the research department along with hiring security experts in order to setup protocols that suit our needs without sacrificing security. Its cost is high because of the time scales that are needed for its deployment cycle, design, implement, review and finally test.

- Patch Vulnerabilities
  The price can vary depending on the number of vulnerabilities that are already known to us but are not yet fixed because of time constraints and resource scarcity.

- Two-Factor Authentication

A relatively low cost solution that solves several problems in regards to user authentication on our web platform.

- Anti-Jam module
  This mechanisms is one of the most cost ineffective one because of the cost required to integrate into our vehicles, the low cost of the exploiting device and finally the low severity that poses as a weakness.

- Pattern matching/load balancing
  This defensive technique is already supported by many third parties suppliers and can easily be integrated into our infrastructure. The sole negative of this approach is that we have to rely on an external party to avoid DDoS attacks.

- ECUs data logging With that mechanism we refer to further collection of logs from our vehicles during their operation. This can help us find attack pathways previously unknown after an incident; currently our control units log errors for diagnostics purposes only. Because these changes can interfere with time critical functionalities of our cars it is crucial that they are implemented and tested thoroughly before being shipped.

6.3 Course of action

Thus far, we have described our architecture and our assets and we have presented several attacks against them with the relevant cost that they impose on our business. We have also listed several defenses that can stop a lot of these exploits and discussed their cost in a qualitative scale. The connection that needs to be done now in order to choose the best solution for our business is to pit the defensive cost both from a monetary perspective and a time one with the calculated risk. Code reviewing and integrating two factor authentication would be a good start with their medium and low cost but they can benefit us greatly in the long term while patching certain of the vulnerabilities first, the ones with high or critical level of severity, is a good attitude going forward. Outsourcing the pattern matching and the load balancing is also a good start because it requires little effort from our part while giving us an immediate security boost. In the same manner, a bounty program can be run freeing our resources while simultaneously achieving some of the goals of performing penetration tests.

The refinement of the vision algorithms is something that must not be neglected but its nature makes it time consuming consequently it can be placed in the queue after the above mechanisms. Similarly, formal penetration testing is time consuming with uncertain results so it can be scheduled at a later time.

References

[1] Ep2790 security analysis of large-scale computer systems. 2019.

[2] Alexandros Asvestopoulos. Intrusion protection of in-vehicle network: study and recommendations. 2015.

[3] European Commission. *Handbook on the external costs of transport.* 2019.

[4] The MITRE Corporation. Technical report. `https://attack.mitre.org/groups/`.

[5] Arturo Davila, Eduardo Dios, Enric Aramburu, and Alex Freixas. Environmental benefits of vehicle platooning. 5, 01 2013.

[6] Ivan Evtimov, Kevin Eykholt, Earlence Fernandes, Tadayoshi Kohno, Bo Li, Atul Prakash, Amir Rahmati, and Dawn Song. Robust physical-world attacks on machine learning models. *CoRR*, abs/1707.08945, 2017.

[7] Jack Freund and Jack Jones. *Measuring and Managing Information Risk: A FAIR Approach.* Butterworth-Heinemann, USA, 2014.

[8] Ed Garsten. Sharp growth in autonomous car market value predicted but may be stalled by rise in consumer fear. 13 Aug 2018.

[9] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas. Ddos in the iot: Mirai and other botnets. *Computer*, 50(7):80–84, 2017.

[10] David Kushner. The real story of stuxnet. 26 Feb, 2013. `https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet`.

[11] Scania Technical Information Library. General information on can, 2016.

[12] Steve Morgan. 2019 official annual cybercrime report. Technical report, 2019.

[13] Forum of Incident Response and Security Teams. Technical report, 2019. `https://www.first.org/cvss/v3.1/specification-document`.

[14] Patrick Putman. What is a hacktivist? `https://www.uscybersecurity.net/hacktivist/`.

[15] Dan Swinhoe. The biggest data breach fines, penalties and settlements so far. December 2019. `https://www.csoonline.com/article/3410278/the-biggest-data-breach-fines-penalties-and-settlements-so-far.html`.

[16] Inc Tesla, 2019. `https://www.tesla.com/model3`.

[17] Liam Tung. New zealand: over a third of cyber attacks come from state-sponsored hackers. Nov 18, 2019.

[18] Z. Wang, G. Wu, and M. J. Barth. A review on cooperative adaptive cruise control (cacc) systems: Architectures, controls, and applications. In *2018 21st International Conference on Intelligent Transportation Systems (ITSC)*, pages 2884–2891, Nov 2018.

[19] Wikipedia. https://en.wikipedia.org/wiki/Create,_read,_update_and_delete.

[20] Vladimir Zwass. Information system. December 28, 2017. https://www.britannica.com/topic/information-system.