Car Hacking

Sérgio António Monteiro e Silva
sergioamsilva@tecnico.ulisboa.pt

Instituto Superior Técnico, Lisboa, Portugal

December 2020

Abstract

The world is more and more digital, the concept of cyberspace begins to surpass the analogical reality at breakneck speed. Therefore, computer systems are the target of an emerging generation of criminals who take advantage of the vulnerabilities of each system in order to have access to secure information or to damage systems to prevent them from functioning. In this context, the automotive industry is forced to provide its vehicles with interconnected features, components and systems, which allow, not only greater efficiency and car safety but also the provision of a series of amenities to the driver and its occupants, that allow them to obtain real-time information, accessing the Internet and remotely control the operation of the vehicle. Besides the usual mechanical components, a modern vehicle is also composed of communications networks, protocols, processors and source code. It is in this technological component that vulnerabilities arise and can be exploited by hackers. This work consists of identifying the main attack surfaces of a vehicle and mapping the associated attack vectors, with the aim of building a car hacking model. Starting from 3 attack vectors: Wifi, Bluetooth and OBD-II, the model was applied to 3 vehicles and the vulnerabilities were classified according to the CVSS classification system. Even in less than a year old vehicles, several vulnerabilities were found, like the possibility of tracking the car via WIFI and Bluetooth, as well as the exploitation of the internal communications system with packet injection that leads to the remote control of components such as disabling signals or the horn. The WIFI system is undoubtedly the most permeable, a consequence of the adoption of encryption protocols with identified vulnerabilities, as well as the lack of isolation of the equipment that connect to this network. In conclusion, the security flaws in the automotive construction are evident, enhancing car hacking, and emphasise that it is not necessary a very high level of knowledge to execute these attacks, considering the current existing tools, which manage to execute some of these explorations automatically. There is a clear need for exhaustive exploration tests, as well as the adoption of cybersecurity standards and procedures by the builders, and the greatest difficulty is the backward compatibility with some protocols such as CANbus. Keywords: Cybersecurity, Vehicle, CanBus, Hacking
Keywords: Cybersecurity, Vehicle, CanBus, Hacking

1. Introduction

It was in the 1990s, shortly after I got my driving license, that I was able to purchase a fourth or fifth hand *Citroen* Zx 1.6, at great cost. This acquisition completely transformed my life, since I stopped being dependent on public transport and could get anywhere faster, as long as I had money for gas.

And the personal impact of purchasing a car is exactly the same kind of the impact that the automotive industry has had on the lives of millions of people for centuries, looking back as far as 1679, when a Belgian named *Ferdinand Verbiest* [1] [16], presented a prototype of the first steam car to the Chinese emperor. However, due to its small size, it was unable to transport passengers, being almost a proof of concept.

the following centuries, there was a constant evolution of the automobile. In 1770, *Nicolas-Joseph Cugnot* [2] developed a steam-powered vehicle in order to transport cannon and, although this vehicle had several operational problems, it made the basic idea for other projects.

For more than 100 years the car has evolved tremendously. In the past, there were almost no electronic components, like the famous *Volkswagen* beetle [3] , which was almost always repairable with wire and pliers. But the new vehicles are simply computers with wheels, where dozens of controllers communicate with each other in real time and make decisions that influence driving, in order to make cars safer and, in some cases, autonomous.

[1] Astronomer, mathematician, scientist, Jesuit and Flemish Catholic missionary

[2] French Military Engineer

[3] This was the first model manufactured by the German company *Volkswagen*, tense been the best selling car in the world,

1.1. Motivation

Nowadays, car safety depends on cybersecurity. However, OEM parts manufacturers[4] tend not to implement safe components. Hardware, software and communication channels are fraught with vulnerabilities that can be exploited by malicious actors.

When computers were first used in cars, it was unthinkable that they could be attacked and their communications tampered with, causing the vehicle to be led to perform strange actions, such as turning to the left when driving at 120 km/h.

There is a huge community involved in *hacking* automobile [5] , and many vulnerabilities and respective exploits have been discovered. This is a very worrying scenario, considering that many models can not be updated, that is, we currently have 8 to 10 years old cars with identified vulnerabilities that can be easily exploited. These vehicles will always be vulnerable, since the manufacturer has no way to update the systems outside its workshop network.

Thus, this document has as its main motivation the identification of attack vectors and awareness, so that the automotive industry designs more resilient systems from the point of view of cybersecurity. Awareness always involves the practical demonstration of vulnerabilities, so an attack model against various models will be explored and the results of these attacks will be reported.

1.2. Goals

Automotive *hacking* is a brand new area and each manufacturer uses its own protocols and function tables that often vary from model to model. Therefore, mapping is time-consuming and economically expensive as they have to have access to each car model to validate their vulnerabilities.

The purpose of this dissertation is thus, to define a methodology for attacking a car, or *hacking*, which can quickly find vulnerabilities in a given vehicle, using Wi-Fi, BlueTooth or ODB-II as the attack surface, in order to inject or change the data within the CANbus network.

Being able to manipulate the CANbus network, the next step is to perform lateral movements so that the most critical areas of the vehicle are compromised, e.g. the engine, the steering and the brakes.

2. Contextualization

2.1. Modern cars

As previously mentioned, in a modern car, there are hundreds of systems that exchange information with each other, and, on average, each current vehicle has more than 80 processors. So, the automotive industry felt the need to develop communication protocols between these various components, ensuring that critical actions such as braking and changing direction were protected by fast, safe and resilient protocols.

Although each manufacturer decides which components and protocols are suitable for each vehicle, often with variations in the same model, and with great reluctance to publish the way in which communication is performed between each component, there is a communication standard called CANbus. This protocol can be analyzed through an existing connector in all vehicles, called ODB-II.

2.1.1 CANbus

CANbus is a protocol developed by Robert Bosch GmbH[6] . It was born in 1986, but the first vehicle with this technology was marketed only four years later, the Mercedes Class S [7] model w140 [4].

CANbus is an extremely resilient protocol for inductive spikes, electric fields or other noises, minimizing the possibility of transmission error, thus ensuring the quality of communication, a very important factor in a car, since there are hundreds of parts that produce numerous electrical interferences in its operation.

One of the peculiarities of this protocol is that any device connected to the network can see all communications, there is no encryption or validation of the message senders, which makes this system [6] extremely vulnerable.

2.1.2 ECU

The ECU, is an embedded system that controls the operation of the vehicle, it can be said that it is the heart of the car, there are several types of ECU in a vehicle namely:

- ECM, engine control module. item. module controls the articulation between the transmission and the engine.
- TMC, transmission control module
- BCM, confort control module and air conditioning among others
- SCM, suspension control module
- EBCM, brake control module

The main elements that make up an ECM are: A microcontroller, memory [8], signal inputs, CAN connections, and built-in software

[4] *Original Equipment Manufacturer*

[5] An example of these communities is *Car Hacking Village*,available at https://www.carhackingvillage.com

[6] Robert Bosch GmbH is a German multinational engineering and electronics company based in Gerlingen, near Stuttgart, Germany.

[7] Top of the range Mercedes and the most technologically advanced model

[8] Can be of the type SRAM, EEPROM or Flash

2.1.3 OBD-II

One of the major issues in the early 90s was that car diagnostics were an expensive process and could only be done at the brands dealers. So, the need for a standard for detecting errors and possible problems that were accessible and inexpensive, was one of the main reasons why OBD-II came about, an evolution of OBD-I [9], which today is available in all modern vehicles.

The OBD-II system is accessed via a DLC - Data Link Connector, which is a 16-pin J1962 female connector and allows access to vehicle data. The location of this connector varies between manufacturers and often between models of the same brand. However, the most common place to find it is under the driver's side instrument panel and, according to the specifications, the OBD-II connector must be up to 60 cm away from the steering wheel.

There are two types of code in the OBD-II [13], namely:

- Diagnostic Trouble Code (DTC), code related to a problem in the system, here each code can be unique or defined by the manufacturer
- Parameter ID (PID), code used to extract data from the ECU such as engine temperature or speed of rotation.

2.2. Car Cybersecurity

The complexity of a car system is enormous, there are more lines of code in a current car than in a 2013 f35 fighter, or even in the latest version of Google Chrome. Given this immensity of source code, it is easy to deduce that there will be a lot of vulnerabilities to be exploited. This complexity can also have its effects in the launch of new models, as was the case with the new ID3 [10] where several faults in the software [7] forced almost 20,000 vehicles to be updated manually with all the logistical and brand image problems that this entails.

Car cybersecurity focuses on all systems that support the modern car, from the simple USB connection to the most complex OTA updates [11]. Several successful attacks over the past few years, have demonstrated that there is an urgent need to implement more restrictive security measures, as well as the abolition of protocols used in the past, which design incapacitates them to be provided with security measures as simple as the communication number between the components..

[9] Initially designed to control gas emissions, it only supports vehicles prior to 1996

[10] New all-electric model of the VW group

[11] Method of distributing application or firmware updates over wireless networks

2.2.1 Vulnerabilities

A vulnerability is a flaw that allows an attacker to compromise a system, which causes it to behave unexpectedly by the developer. Considering the exponential growth of systems as well as their complexity, it is expected that there will also be an increase in vulnerabilities.

2.2.2 Common Vulnerabilities and Exposures (CVE)

Until the end of the 90s, there were no standards to identify vulnerabilities, each manufacturer had their lists and it was impossible to know if there were duplicate vulnerabilities or not. In 1999, David E. Mann and Steven M. Christey of MITER [12], published an article entitled "Towards a Common Enumeration of Vulnerabilities" [13],where they proposed the unification and normalization of the publication process of a vulnerability. It was here that CVE emerged and the whole industry adopted it as a norm and so, in September 1999, the first CVE list was created, with 321 vulnerabilities.

CVE, or Common Vulnerabilities and Exposures, has the primary objective of identifying vulnerabilities, that is, each vulnerability has assigned a unique identifier.

2.2.3 Common Vulnerability Scoring System (CVSS)

National Infrastructure Advisory Council (NIAC) [14], launched CVSS, which is a method of grading the degree of risk of a vulnerability by its characteristics.So far, the CVSS is already in its 3.0 version [2] and, in this classification, the risk is numeric and can vary between 0 and 10, where ten is the most critical value. CVSS is calculated based on evaluation criteria divided into three groups: Base, temporal and environmental.

CVSS is calculated based on evaluation criteria divided into three groups: Base, temporal and environmental. covers characteristics that do not vary with the time variable. It is one of the most important three metrics and the one that has the greatest impact on the final CVSS score. In turn, this metric is divided into two other categories: the impact and exploitation. Exploitation assesses the ease to exploit the vulnerability and represents four metrics:

- Attack surface, where the attack is performed.

[12] The Miter Corporation, is an American non-profit organization

[13] Article available at https://cve.mitre.org/docs/docs - 2000 / cerias.html

[14] United States agency whose main area of action is security, its website can be visited at https://www.cisa.gov/niac

- Attack complexity, time and effort required to exploit the vulnerability.
- Privileges, what privileges are needed to execute the attack.
- User interaction, level of interaction with the user required for exploration.

In turn, the impact group measures the data caused in the attacked system through the permeability of the integrity, availability and accessibility of the system.

In the temporal group, we have the assessment of how the risk of vulnerability can vary with time, as well as the basis, this metric is also divided into the following metrics:

- Exploit code maturity, measures the state of the vulnerability exploit source code.
- Remediation level, measures the solution to the vulnerability, namely whether it is temporary, definitive and official, among others.
- Degree of confidence, measures the credibility of the vulnerability issuer as well as its technical specifications.

Lastly we have the environmental group, it is about the importance of the system, considering the requirements of confidentiality, integrity and availability as well as the security mechanisms that exist in the ecosystem where the vulnerability exists, the metrics that contribute to this group are as follows [14]:

- Security requirements, helps the characterization of CVE as a basis in the scenario in which it is inserted.
- Modification of the base metric, as the environment in which the attacker moves can be influenced by the organization's security measures, helps to adjust the base metric.

2.2.4 Hacking Cycle

By definition, a hacker is an individual who dedicates himself, with unusual intensity, to know and modify the most internal aspects of devices, programs and computer networks.. Thanks to this knowledge, a hacker is often able to obtain extraordinary solutions and effects that go beyond the limits of "normal" operation systems as envisaged by their creators; including, for example, bypassing barriers that are supposed to prevent control of certain systems and access to certain data.

Currently, hacking plays a crucial role in determining security levels of systems and organizations, even contributing to save human lives. Hacking is a well-defined process and, whatever the target of the intrusion in a cyber attack, the cycle of the hacking process is well defined and broken down into five phases, each of which is associated with specific techniques and tools.

The initial phase is called recognition and this is where all the information about the systems we are going to test is collected, and several local or remote processes can be used, most of the time supported by OSINT [15], as different as mapping external and internal networks with tools such as theharvester [16], Shodan [17] or even google dorks [18]. to collect information about the systems. At the local level, one of the passive tools that can be used is Netdiscover [19]. The recognition phase must be mostly passive, so that no type of alarm is triggered on the side of the system being tested. A possible analogy is to look at a door and identify the manufacturer and the model. So, when trying to open the door we already have as much information as possible about it, thus increasing the possibility of success and reducing the number of failed attempts.

The scan aims to identify services and possible ports of entry into the system. Here, we can use tools such as nmap[20], at this stage of the hacking, more aggressive techniques are used that can trigger alarms on the side of the system being tested. We will discover machines or services that are working on the network, as well as possible vulnerabilities and operating systems. is the stage where, based on the previous recognition and detected vulnerabilities, access to the system is obtained. After the access, it might be necessary for the attacker to elevate his privileges to administrator of that system, in order to be able to read, modify or delete information

Maintaining access ensures the persistence of access to the system by the attacker, thus being able to continue to interfere with the operation of the system. So, the attacker has to find a way to maintain access even if the system is rebooted, for example, associated with a backdoor [21] to a legitimate process.

Finally, when the objective of the attack is accomplished, or the attacker feels that he can be dis-

[15] Collection process information in open sources

[16] Software that collects information about a particular organization based on open sources

[17] Search engine, which allows locate computers and services connected to the internet, the platform is available at www.shodan.io

[18] Operators that allow you to fine-tune your searches at www.google.pt

[19] Software used for discovering active IP addresses that can be downloaded at https://github.com/netdiscover-scanner/netdiscover

[20] Software that scans several ports and IP addresses on a given network.

[21] Method that the attacker uses to remotely access the compromised system

covered within the network, we have the phase of deleting the trail, where server logs, temporary files, command line history, emails or any other type of information might link the attacker to the attack

2.2.5 Attack Surface

By definition, the attack surface is where the hacker can exploit attack vectors. Very simply, we can imagine a house with doors, windows, chimneys, etc., where each of these points can be used as an entrance, using a different technique. For example, you can break a window glass or simply try to force the lock on the entrance door.

We can define the attack surface as the set of ways which an attacker can compromise a system. The larger the attack surface, the greater the risk of the system being successfully attacked.

2.2.6 USB ports

USB ports are used for supplying power to other devices such as cell phones, upload files to the multimedia system, such as music in MP3 format and can also be used for system updates.

2.2.7 Bluetooth connections

They are used primarily for pairing with mobile phones to allow the driver to make calls. For example, to read and respond to messages without taking hands off the wheel or for the multimedia system to function as an extension of the phone and enable access to the multimedia system display to various applications, like Android Auto and Apple Car.

2.2.8 Wi-Fi connections

They can be used to provide a HOTSPOT to the occupants of the vehicle, but also the reverse ie the vehicle uses wi-fi to connect to a hotspot. Often the wifi is directly connected to the multimedia system.

2.2.9 GSM Connections

There are several uses of GSM technology in a car. Most recent vehicles have a GSM card built into the hardware that allows communication with the manufacturer and can thus send and receive various types of information and even allows remote OTA updates.

2.2.10 Tire pressure monitor sensor

This system, which can be called TPMS [22], allows you to send information about the condition of the tires, so that if there is a pressure loss in a of the tires he is immediately informed. TPMS are installed inside the tires and ensure communication with the ECU via radio signals.

[22] Tire-Pressure Monitoring System

2.2.11 Diagnostic port

The diagnostic port, or ODB-II, allows the external reading of Canbus traffic, as well as the injection of CAN frames. The operation of this port was described in the automotive operation section of this dissertation.

2.2.12 Apps

The apps of a car can be installed directly on the infotainment system or on the driver's smartphone which, in turn, connect remotely to the infotainment system and many of which connect externally to a cloud for storage and exchange of information. Most current cars provide their customers with an application where they can consult all kinds of information such as consumption, distances covered or even if the doors are closed or not. In turn, the driver can send commands to the vehicle through these applications to perform tasks like horn, open doors, turn on the air conditioner or even start the engine.

2.3. Attack vectors

Considering the aforementioned attack surfaces, we can move on to the attack vectors that will be the gateway to compromise and exploit the vehicle. These are based on design or coding vulnerabilities of the components of each technology. In other words, there will be a breakdown of each attack vector into its smallest components in order to find the vulnerability.

2.3.1 WIFI exploitation

There are several vulnerabilities in WIFI networks that allow attacks on these networks. One of which is the fact that there is no validation of the SSID to which the device is connecting, so it is possible to clone that SSID and put a network on the air with exactly the same name. This attack is called evil twin, and it is based, not only on the premise that devices only look for the SSID to connect, but also that they prefer the network with more power, in case there are two identical SSIDs.

Now, starting from the two modes of operation of the vehicles in wifi mode, it is easy to understand that, in both, it will be possible to attack the evil twin, either to take the car to connect to an attacker wifi network with the same name as the network original or to make external devices think they are connected to the vehicle network and, instead, are connected to the attacker network.

Next we have the deauthentication attack, where we use a deauthentication frame to force the devices to disconnect from the AP [3], it can also be considered a DOS attack since if the WIFI network is continued, it simply leaves to work, this is a protocol design vulnerability that allows an unauthenticated user to issue these disauthentication frames.

Another type of attack is the cracking of the WIFI network password by bruteforce. In simple terms, a certain message is intercepted between the AP and the client and then based on a word dictionary. Each of these words is validated if you get the correct password, in case of success, or reach the end of the dictionary, in case of failure. This method depends on the quality of the dictionary.

Lastly, we have a type of attack that allows two things. First, to analyze where the vehicle has been and also connect it to the attacker's network passively. This is due to the fact that the devices that have already been connected to a wifi network, maintain a list of these networks and regularly issue a probe request, that is, ask if the SSID, to which they have already been connected, is available to them. The attacker in turn can analyze these probe requests [12] and see which SSID the vehicle has already been connected to. This has two purposes: Analysis of the movements of the vehicle and its geolocation or the availability of a network wifi with the same SSID that the car is looking for, thus establishing a connection[11].

2.3.2 Bluetooth exploration

Bluetooth is a low-consumption, wireless communications standard, uses the 2.4GHz frequency, where 79 radio channels are defined [23] spaced 1 MHz

There are several vulnerabilities in bluetooth, although some may have been fixed in new versions, the connection between two devices via bluetooth is as strong as whichever is most vulnerable, meaning older devices can be excellent attack vectors [**?**]. This is a very important fact, considering that there are many vehicles with old bluetooth versions that will never be updated

2.3.3 Scanning USB Ports

There are two types of exploitation of USB ports: the destructive ones and those that fall within the scope of sabotage and those that attempt to exfiltrate the system.

Destructives are based on a device called USBKILL [24], this piece of hardware works in a very simple way, when connected to the USB port it stores energy that it then returns to the machine that is connected to a high voltage discharge. The result is the destruction of the electronic components of the system and their inevitable destruction [25], USBKILL can cause a car to stop responding completely, or in specific cases the USB ports will be burned [1].

From the system exploration perspective, the USB port can be used to update a compromised firmware that will provide an attacker with administrative access, this is because there is often no validation of the firmware signature through the port. USB may also be possible to attack with ransomware [26] where the vehicle's systems are encrypted by the attacker, only after a ransom request are the systems deciphered. [9]

Some systems also allow the connection of usb-to-ethernet devices [27], so it is possible to explore the system through the IP address.

2.3.4 Exploration of the diagnostic port

The diagnostic port, or OBD-II, is considered one of the best points of attack for exploring a car, as it is directly connected to the CANbus and allows not only reading but also writing on the communication channel [17]. To perform the attack and taking into account that the OBD-II is a local port, two techniques can be used: Remote connection using an ELM327 [28]dapter OBD plug for simple diagnosis and reading by bluetooth connection, in that the attacker can be up to 10 meters away. Or using a USB-CAN adapter, which allows direct connection to a computer.

One of the most used techniques in this attack vector is the interception of all traffic on the CANbus and the detection of values that vary when a certain action is performed. For example, when the flashing on which the change in the CANbus frame is connected, makes this mapping it is possible to replicate these frames and inject directly into the CANbus and obtain an action on the part of the vehicle. We must not forget that there is no validation of the origin of the frames in this protocol and that all components can see all the traffic

2.3.5 TPMS exploitation

TPMS sends information on tire pressure, wheel speed and temperature every 60 to 90 seconds as well as a warning about the battery status of the

[23]designated RF channels

[24]Can be purchased at https://usbkill.com/

[25]A demonstration of USBKILL can be seen at https://usbkill.com/blogs/news/usb-kill-vs-car-are-you- at-risk

[26]Ransom malware, or ransomware, is a type of malware that prevents users from accessing your system or personal files and requires them to pay a ransom to return access. [10]

[27]Plug-and-play devices that connected to the USB port provide an ethernet connection

[28]a

sensors themselves, the data is then transmitted to the ECU and presented to the driver on the dashboard of instruments [15], each TPMS has a unique identifier so that there is no interference from nearby vehicles with the same system [8], depending on the vehicle the information exists, TPMS systems that only send data when it is reached the 50 km/h and there are others that even with the vehicle stopped, emit the information, thus enhancing the possibility of a tracking [29]ttack Passive attack that allows the tracking of a certain system based on unique identifiers.

A very important aspect of the design of the communications of TPMS systems is the fact that there is no figure in the data transmission, thus leaving the door open for anyone to explore these systems. On the other hand, the deactivation of TPMS requires some knowledge and specific tools to disassemble the tire, which are not available to anyone.

2.3.6 GSM exploitation

Most current cars have a GSM connection in order to be able to perform a series of functions, ranging from remote updates to providing internet access to vehicle occupants.

To explore GSM the most used technique is to use a fake antenna called a rogue base station [5]. The concept of this attack is to connect the vehicle equipped with GSM technology to this antenna, instead of connecting it to a reliable antenna of the telecommunications operator. The attacker is then able to intercept and analyze the GSM traffic obtained and, in some cases, can even change the contents of the transmitted data.

Bearing in mind that many manufacturers use OTA updates, it is easy to understand that this type of attack can cause permanent exploitation of the vehicle when the attacker is able to rewrite its firmware.

2.3.7 Application Exploration

The exploitation of applications can be supported by various techniques, these techniques are categorized as those in the OWASP [30] in order to enumerate the ways to explore a web application. One of the main OWASP projects is the OWASP TOP 10 [31], which is a list of the 10 most common flaws in web applications, this is an excellent starting point for exploring the applications used by a given vehicle.

[29] a

[30] Non-profit organization whose main objective is to provide reliable and independent information in the area of cybersecurity

[31] Project available at https://owasp.org/www-project-top-ten/

The manufacturers have exponentially increased the attack surface of the cars by using applications, and there are several ways to try to explore these applications and gain control of the vehicle.

3. Methodology

Taking into account the variety of attack surfaces on a car, the exploration model presented in this dissertation will focus on four attack vectors, two local and two remote. The locations will be the connection to the OBD-II and exploitation of the USB connection and, in turn, the remote attacks will exploit the vulnerabilities of communications using WIFI and bluetooth

The method used is to collect information from the vehicle, namely available attack surfaces, such as possible CVE assigned to the vehicle or components that are part of the car's systems.

The first data to be collected will be the year of manufacture, the make, the model and the version.

With this information, the first step will be to search for possible CVE, in order to compromise the vehicle under analysis, Common Vulnerabilities and Exposures [32] will be used, the importance of this step comes the fact that there may be unpatched vulnerabilities in the vehicle.

Next, the attack surfaces defined in this model will be mapped, each one will be assigned an Y or N value where Y means that the attack surfaces are present and an N means that the vehicle does not have that attack surface.

Table 1: Vehicle's attack surfaces

Attack Surface	Value (Y / N)
Are there CVE available?	
Does the car have WIFI?	
Does the car have bluetooth?	
The vehicle has ODB-II	

If the car is equipped with WIFI wireless communications technology, then we will have the following sequence of exploration and it will be possible to explore the various possible attacks, namely: WPA CRACK, DEAUTH, Evil Twin, DOS, Probe.

Regarding the Bluetooth exploration, the visibility of the car in a given location will be tested with its unique identifier of the Bluetooth card, the services it offers through Bluetooth and its resilience to a denial of service.

The exploration of the OBD-II port within this model of car hacking, will aim at intercepting CANbus traffic, identifying a certain packet and injecting that packet directly into the CANbus,

[32] https://cve.mitre.org

4. ODB-II Exploration

As we saw earlier through ODB-II we have direct access to CANbus, however, in order to be able to analyze packages, it is necessary to use some hardware and software. On the hardware side and within the scope of this dissertation, the Korlan USB2CAN [33]

Bearing in mind that the Linux operating system kernel supports CAN using the SocketCAN framework [34], this will be the operating system chosen for OBD-II scanning

The software used to operate the OBD-II is canutils in its version v2020.11.0 [35]

4.1. WIFI exploitation

Within the WIFI exploit, several attack techniques will be used, namely:

4.1.1 WIFI DOS

To execute DOS attacks, the software used will be mdk3 version 3.0 v6, [36] This application allows you to run several of DOS attack namely:

- Beacon Flood Mode
- Authentication DoS mode

4.1.2 DEAUTH

Using the "d" option in the mdk3 software, it is possible to perform a mass deauthentication attack, that is, all workstations connected to the AP will lose their connection. Thus, it is possible to permanently affect communications via wifi if the attack has an indefinite time.

4.1.3 WPA CRACK

In this exploration the objective is to intercept a handshake, so that using the brute force technique based on a dictionary, the password of the WPA network is obtained

The software used will be WIFITE in its version 2.2.3 [37] This application allows the entire process to be done in an automated way, simply identifying the target attacking and waiting for the handshake to be captured and the password cracking process for the WIFI network started.

4.1.4 EVIL TWIN

For the evil twin attack we will use wifiphisher software version 1.4 [38]. Wifiphisher allows you to perform evil twin attacks on WIFI networks in an automated way.

4.1.5 PROBE SNIFFING

In order to run a vehicle snnifing probe, and to know which networks have already been connected and where, the software used will be probeSniffer version 3.0, [39]

4.1.6 Exploration of the internal network

After the success of compromising the WIFI network and the consequent association with that network, the next step is to explore the internal network through a scan to find available machines and services.

The nmap software in version 7.80, [40], will be used for this purpose. This tool allows for various types of machine discovery, services and vulnerabilities.

4.2. Bluetooth exploration

For the bluetooth attacks of a vehicle, and within the scope of the exploration model of this dissertation, one of the software to be used is the bluez [41], which contains the tools hcitool [42], sdptool [43] and l2ping [44]

5. Results and discussion

subsection Exploration model application

After the model was created, several vehicles of different brands and models were tested in order to explore the various attack surfaces in different manufacturers in order to validate the model. Bearing in mind that this work may reveal vulnerabilities and attack methods of specific models, the decision was made to hide the make and model of the vehicles tested, and the results were communicated to the manufacturers.

5.1. Sample results

5.1.1 Car A

Scanning the OBD-II port

[33] Technical specifications can be seen at https://www.8devices.com/media/products/usb2can_korlan/, this device allows connection to windows and linux systems, on the product support page there is even a plugin for wireshark so that packet capture is easier.

[34] Volkswagen Research's contribution to the Linux kernel

[35] The source code is available at https://github.com/linux-can/can-utils

[36] The source code can be found at https://github.com/charlesxsh/mdk3-master

[37] Available at https://github.com/derv82/wifite2

[38] Available at https://github.com/wifiphisher/

[39] source code can be found at https://github.com/xdavidhu / probeSniffer.

[40] Available at https://github.com/nmap/nmap.git

[41] Official stack of the Bluetooth protocol in linux and which is available at http: // www.bluez.org/

[42] For scanning nearby devices, discovering the type of device.

[43] for discovering services running on nearby devices.

[44] Used to make a ping. Send an echo request and receive a reply to a bluetooth device

Table 2: Attack surfaces

Vehicle	WiFi	Bluetooth	OBD-II	CVE
A	No	No	Yes	No
B	Yes	Yes	Yes	No
C	No	Yes	Yes	No

Through the CANbus traffic analysis it was possible to isolate the packet that connects the turn signals that have the value of 612#6230007F00000000

Table 3: Vehicle A OBD-II Vulnerabilities

OBD-II Exploration	Value (Y / N)
CANbus vulnerable?	Y
Interception of frames?	Y
Frame injection?	Y

5.1.2 Car B

WiFi exploitation This vehicle has a password protected hotspot and SSID cannot be changed.

Table 4: Vehicle B WiFi vulnerabilities

Exploration WiFi	Value (Y / N)
Vulnerable to WPA crack?	Y
Vulnerable to Evil Twin?	Y
Vulnerable to DOS?	Y
Vulnerable to PROBE	N
Vulnerable to DEAUTH	Y

Exploring Bluetooth Vehicle B showed a permeability to Bluetooth attacks revealing its identity, the services it offers as well as its location in a given space.

Table 5: Vehicle B Bluetooth Vulnerabilities

Bluetooth Exploration	Value (Y / N)	CVSS
Visible on a scan?	Y	4.3
Discovery of services?	Y	4.3
Do you answer l2ping?	Y	4.3

Exploration of the OBD-II port Through the CANbus traffic analysis it was possible to isolate the packet that connects the turn signals that have the value of 348#001A2249C1210000

Table 6: Vehicle B OBD-II Vulnerabilities

OBD-II Exploration	Value (Y / N)
CANbus vulnerable?	Y
Interception of frames?	Y
Do you accept frame injection?	Y

5.1.3 Car C

Exploring Bluetooth Vehicle C is vulnerable to all exploits of the hacking model

Table 7: Vehicle C Bluetooth vulnerabilities

Bluetooth Exploration	Value (Y / N)
Visible on a scan?	Y
Discovery of services?	Y
Do you answer l2ping?	Y

Exploration of the OBD-II port Through the CANbus traffic analysis it was possible to isolate the packet that connects the turn signals that have the value of 348#0001A2249C1210000

Table 8: Vehicle C OBD-II Vulnerabilities

OBD-II Exploration	Value (Y / N)
CANbus vulnerable?	Y
Interception of frames?	Y
Do you accept frame injection?	Y

5.2. Conclusions

The automotive industry is experiencing difficult times, with regard to cybersecurity. The complexity of the systems, combined with the need for compatibility with older systems, makes it difficult for this ecosystem to manage the older protocols. In this ecosystem CANbus become standard, it is present in all modern vehicles and presents a high risk, since it is an insecure communication protocol and can easily be manipulated without any security mechanism.

Regarding the other attack surfaces explored in this dissertation, and within the samples collected, the vulnerabilities inherited from insecure technologies are notorious. For example, the adoption of WPA ciphers in the WIFI networks provided by the vehicles, makes it possible to reveal the password due to a well-known vulnerability. On the other hand, the impossibility of changing the MAC ADDRESS of the WIFI and Bluetooth card, allows the passengers of the vehicle to be followed and located.

Even in recent vehicles, from the year 2020, it was possible to manipulate the CANbus and extract information from Bluetooth. In other words, it would be mandatory that manufacturers have other types of implementations and endow their vehicles with effective measures that increase the level of security. It was possible to identify the same vulnerabilities in a 2005 vehicle, which means that, in 15 years, nothing has evolved in this matter.

It is important to note that all vehicles presented vulnerabilities in the attack surfaces that existed. In all, it was possible to explore the CANbus, in vehicle B and C, the attacks on Bluetooth were successful and in vehicle B all explorations of WIFI were also successful.

There is also a lack of efficient mechanisms for updating a car's systems, as well the notification to its owners of the need to upgrade.

In conclusion, it is necessary to include cybersecurity specialists in car development teams, as well as to define bug bounty programs of the manufacturers, so that the vehicles are constantly tested. And, above all, the production cycle and availability of corrections are quick to minimize the window of opportunity for the attackers.

References

[1] O. Angelopoulou, S. Pourmoafi, A. Jones, and G. Sharma. Killing your device via your usb port. 07 2019.

[2] CFIRST. Common vulnerability scoring system v3.0: Specification document. Acedido em 2020-02-01.

[3] R. B. V. P. D. D. Chintan Kamani, Dhrumil Bhojani. De-authentication attack on wireless network. *International Journal of Engineering and Advanced Technolog*, 2019.

[4] CIA. Mercedes w140: First car with can. Acedido em 2020-08-01.

[5] A. Dubey, D. Vohra, K. Vachhani, and A. Rao. Demonstration of vulnerabilities in gsm security with usrp b200 and open-source penetration tools. 08 2016.

[6] S. Fassak, Y. Idrissi, N. Zahid, and M. Jedra. A secure protocol for session keys establishment between ecus in the can bus. pages 1–6, 11 2017.

[7] M. Freitag. Volkswagen kämpft mit massiven softwareproblemen beim id.3. Acedido em 2020-07-01.

[8] N. N. Hasan, A. Arif, and U. Pervez. Tire pressure monitoring system with wireless communication. In *2011 24th Canadian Conference on Electrical and Computer Engineering(CCECE)*, pages 000099–000101, 2011.

[9] A.-D. S. T. E. Marko Wolf, Robert Lambert. Wannadrive?feasible attack pathsand effective protectionagainstransomware inmodern vehicles. *International Journal of Engineering and Advanced Technolog*, 2017.

[10] Marlwarebytes. Tudo sobre ransomware. Acedido em 2020-08-01.

[11] L. Oliveira, D. Schneider, J. Souza, and W. Shen. Mobile device detection through wifi probe request analysis. *IEEE Access*, PP:1–1, 06 2019.

[12] W. Pattanusorn, I. Nilkhamhang, S. Kittipiyakul, K. Ekkachai, and A. Takahashi. Passenger estimation system using wi-fi probe request. pages 67–72, 03 2016.

[13] D. Rimpas, A. Papadakis, and M. Samarakou. Obd-ii sensor diagnostics for monitoring vehicle operation and consumption. *Energy Reports*, 6:55 – 63, 2020. Technologies and Materials for Renewable Energy, Environment and Sustainability.

[14] B. Security. Cvss explained. Acedido em 2020-08-01.

[15] C. Smith. *The car hacker's handbook : a guide for the penetration tester*. No Starch Press, San Francisco, CA, 2016.

[16] M. Tutor. Ferdinand verbiest. Acedido em 2020-03-01.

[17] Y. Zhang, B. Ge, X. Li, B. Shi, and B. Li. Controlling a car through obd injection. In *2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud)*, pages 26–29, 2016.