Data Security in Modern Cars

Pedro Martins

Lusofona University of Porto, Portugal
pedro.miguel.martins9@gmail.com

Abstract. As the automotive industry progresses there's been a growing investment in connected cars. With it the need for ensuring secure communications inside of, from and to said cars has also become a growing focus. This paper will talk about the known threats, how they are identified and their impact on systems, ways to avoid them, as well as methods to contain and resolve them in order to raise interest and awareness over these matters, using as means of reference, a case study from the industry.

Keywords: Communication, Vehicle, Automobile, Data Security, Car.

1 Introduction

With advancements in technology, daily use objects have steadily and increasingly become more connected in networks in order to give them more flexibility and to adapt to the users' needs. Vehicles have also followed this trend, and although it brought very useful features, it also brings with it some risks.

Data security and mainly personal data security have been subjects of extreme importance with the development of digital technology. We live in a time where information can be easily shared and extracted, as such, the need to keep a person's personal data private has become the focus with the recent push to develop security measures and methods of prevention.

After the introduction of the Electronic Control Unit (ECU) to the commercial car, the access to vehicular telemetry has become more common place, firstly used to monitor the engine and to control variables such as the injector on time in order to improve efficiency [1], it soon expanded to many more areas of the vehicle and quickly more types of ECUs followed and made the vehicle's information easily accessible.

Nowadays, after the introduction of parking assist and other technologies, information such as the steering angle, braking and displays can now be tampered with [2]. This means that someone with physical access to a vehicle, can use the ECU's functions to gain control of the vehicle.

With the advance of current communications technologies however there's been a growing push to connect the vehicles to a network, sharing information between vehicles to avoid common problems such as vehicle blind spots and information on what's coming ahead.

With some vehicles having the need for software updates using wireless networks, some of which being more important to the vehicle's safety than others, the importance for secure communications becomes evident as well as the risks associated.

This paper will be structured in two main parts, in-vehicle connections and mobile connections. In the first topic the in-vehicle connections will be separated in two kinds, the wired and the wireless, after a brief introduction, some common attacks will be described followed by some mitigation and prevention methods. The second topic will be about mobile connections, describing first how the vehicle uses such connections, followed by the results of an interview in the field.

2 In-Vehicle Connections

Starting with the last line of attack on a connected vehicle, we have ECUs, these devices are capable of processing signals and are usually coupled with sensors, other ECUs or even interfaces connecting to the users or even outside systems [3]. They create a network of data, responsible for tracking the vehicle's components' status and process them in order to maximize efficiency, safety and even to aid and inform the driver and its passengers.

It's clear why attackers might want to get access to the ECUs' data. Gaining access to one or more interfaces would be a gateway to the vehicle's control and information on its users. As such, security in these interfaces is critical for the whole system's security.

To understand how data flows in a network of ECUs, we must first investigate how the various nodes are connected and how the communication is established between them.

Below, some of the more common possible attacks on the in-vehicle network will be described, all of which require either physical access or very close proximity to the target vehicle.

2.1 Attacks over wired networks

In a vehicle there are one or more serial buses and gateways connecting the various nodes together and ensuring they can send and receive information. One such system is called Controller Area Network (CAN) [4]. The CAN is a broadcast protocol as such, all nodes receive a sender's message, but only the receiver will accept them [5].

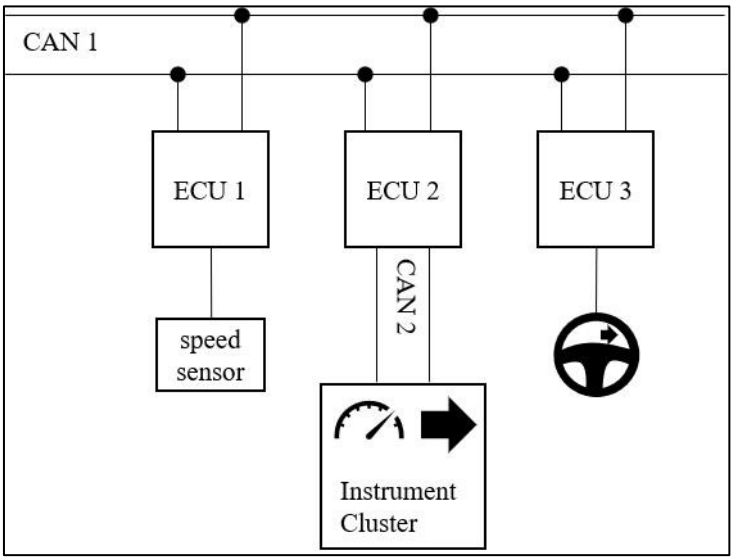

Fig. 1. CAN Architecture example [4]

2.1.1 Denial of service

The first and most basic of attacks across networks is the Denial of Service (DoS). This attack consists of overloading the bus so that the communication between nodes becomes obstructed and no packets can be delivered. The effects and results of the attack however vary between networks and ECUs, in some cases even disabling power steering and limiting the wheel's range of motion. [2]

A DoS can be achieved in several ways, ranging from sending false Request to Send (RTS) packets to repeating packets it sniffs in the CAN bus [6].

The damage of the attack can't however be considered the same for every vehicle, while some vehicles are older and make less use of the processing capabilities of said networks, newer vehicles are filled with sensors and ECUs but are also more developed in terms of data security as the technology got more time to mature.

Some ways to mitigate the damage caused by a DoS can be:

- Checking for excessive packets during a time frame, this can be achieved by programming the ECU to drop requests it has already responded from the same source for a limited time frame [6], since the frequency of normal packets is predictable [2];
- Ensuring minimal safety when one or more ECUs lose control avoiding cases such as the reduced steering range [2].

2.1.2 Packet Sniffing and Data Injection

Data injection is a more complex attack as it involves the attacker sending packets impersonating nodes in the bus and sending potentially malicious information requiring knowledge of the network structure which in most if not all cases implies that the attacker needs to reverse engineer the target vehicle's CANs [2].

To aid with this process the attacker would need to analyze packets in the buses (sniffing), this however is similar across vehicles' CANs and there's already a wide variety of tools for this purpose easily accessible to most. To achieve this, some ECUs allow you to do diagnostic operations requiring an authentication key. While in some cases it might be necessary to extract its firmware and reverse engineer the key to gain access to the mentioned mode, in some cases, depending on the system you can get away with brute force since some use a fixed seed while authenticating. [2]

Although sniffing by itself already poses a privacy concern, when used for the purpose of packet injection it poses a much bigger threat, in some cases even making it possible to gain control of the vehicle's steering by resending packets used in park assist used to control the steering wheel. Some other attacks range from sending misleading information to the vehicle's dashboard which includes the speedometer and door signals causing confusion and misleading the driver. [2]

Suggested methods to avoid these attacks, some of which already used in commercially available vehicles include:

- Random seeds for authentication purposes, lowers the chance of a successful authentication by brute forcing as described previously [2];
- Physical network separation, although most systems use CAN buses, some manufacturers avoid possible attacks on other systems such as the cruise control by connecting them directly to the Powertrain Control Module (PCM) where the accelerator is also connected [2];
- Message obfuscation, it tries to maintain messages known only to authorized parties, although it doesn't stop all attacks it adds an extra layer of difficulty, forcing the attacker to reverse engineer in order to decode proprietary messages [7]

2.2 Attacks over in-vehicle wireless networks

With the increase of sensors in the car, wired connections across sensors directly affect the weight and the wire complexity of these networks. To avoid this, wireless networks are thought to become increasingly used across the vehicle and although vehicle-tovehicle and vehicle-to-infrastructure connections have been getting much attention, the first wireless network widely installed in every new vehicle has been the Tire Pressure Monitoring System (TPMS). [8]

This system consists of one sensor per tire that periodically broadcasts the tire's variables such as temperature and pressure over to a receiver fitted to an ECU which after filtering the received packets processes the sensors' data [8].

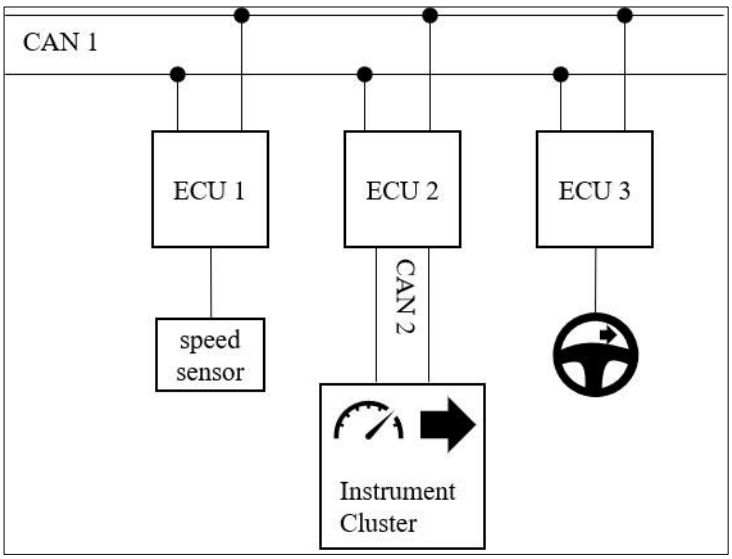

Fig. 2. TPMS Architecture with four antennas [8]

The TPMS's lack of security however doesn't get much attention since the car's metal body works as a shield shortening the maximum connection distance, and because a third--party getting tire pressure seems harmless [8].

Furthermore, having most modern vehicles pushing for handsfree interaction with the vehicle using Bluetooth [9] which is nowadays also common across smartphones and even fitness devices, a whole new vector of attack is possible.

Although some of the previous attacks over wired connections still apply over invehicle wireless networks, attacks unique to these connections will be given more attention.

2.2.1 Indirect attacks (Trojans)

For an attacker it's much harder to physically pair a device to the vehicle, instead, using an app the target will likely have installed in one of his devices paired connected over Bluetooth, the attacker can send harmful information to the vehicle's system over the target's phone (Trojan) [9].

These sorts of attacks where harmful payloads are sent to the vehicle's ECU responsible for the Bluetooth communication could potentially exploit security flaws only available over paired devices [9].

Some possible ways to avoid these attacks start with:

- Increasing safety measures in phone application stores, this will only get you so far however, since there are exploits that can compromise devices through malicious Web sites [9];

- User awareness, education on methods of prevention and the risks of visiting rigged websites [10] or installing harmful software;

2.2.2 Tracking

Even though the TPMS doesn't seem to contain much information on its own since its purpose is to be used to track tire pressure and due to its lacking security measures, the sensor's IDs can be used to identify a vehicle [8].

Coupled with the reported possibility of eavesdropping the system over ranges of over 10 meters using a strategically placed receiver make it a viable way of locating a car. Although some similar systems exist, such as the automatic license plate identification this system and the toll tags, this method is can prove to be more reliable against the usage of fake license plates since the system is hard for drivers to deactivate [8] and doesn't need the vehicle to be equipped with an extra equipment.

This method doesn't make it possible to track a vehicle with much precision due to the high cost of placing receivers along a stretch of road. However, by well thought out placements the receivers could track the frequency of highway entrances and exits' usage [8].

It is however possible to avoid this by:

- Adding cryptographic measures to the wireless communications, making it more difficult to decipher and obtain information such as the sensors' IDs in the TPMS;

- Better insulation of radio frequencies, avoiding the possibility of sniffing on the wireless networks, lowering the maximum distance at which the attack can occur.

3 Mobile Connections

With the European Union making eSIM based system eCall mandatory, modern vehicles are now always connected via mobile networks.

Although by itself the system doesn't pose security risks, many manufacturers are now pushing to give more functionality to the vehicle over mobile networks, enabling intractability with the vehicle wirelessly over mobile networks.

The most common and used mobile communication system today is the Global System for Mobile Communications (GSM), first used mainly for voice communications it is now the most

widely used wireless technology worldwide and although technologies like 4G LTE (Long Term Evolution) have gained popularity, GSM still handles a great amount of voice calls as systems without access to Voice over LTE (VoLTE) usually fall back to it. [11]

The main problem with mobile communications however is the fact that they use an unprotected medium such as air. To mitigate this problem, current technologies such as 2.5G now using cryptographic techniques, and 3G having new authentication systems. [12]

3.1 Attacks over Mobile Networks

Since GSM is the most common, has some similarities over the other alternatives and is the one that all systems will roll back to when needed, it's going to be described in greater detail.

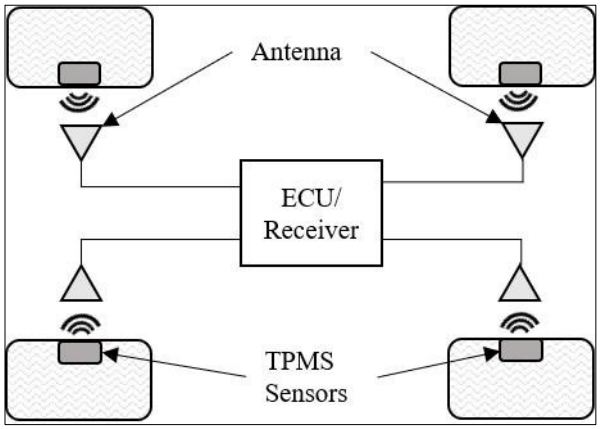

Fig. 3. GSM Network Architecture Simplified [14]

This technology is structured in three major subsystems:

- The Mobile Station (MS), which is all the equipment and/or software required for the subscriber to communicate with the network. It includes the mobile equipment, such as a mobile phone, and a Subscriber Identity Module known more commonly as a SIM card;
- The Networking and Switching Subsystem (NSS), responsible for connecting calls from one end to another, to manage mobility of the subscribers and the communication with the telephone network and the internet;
- The Base Station Subsystem (BSS), that manages the radio transmission between MSs and other subsystems. [13]

3.1.1 Man in the middle

The man in the middle attack as the name suggests, is performed by being an intermediary in the communication of two systems. In the case of GSM this attack can be achieved by the attacker impersonating a Base Station to the Mobile Statin and impersonating the Mobile Station to the Base Station. [14]

Although these kinds of attacks can be used in the systems above, in the case of mobile networks they appear to get more of a focus, since multiple protocols such as GSM and UMTS operate simultaneously.

These attacks over GSM and UMTS connections target encryption keys which would grant the attacker access of the content of the message as it is, this could mean text messages such as SMS could be read, the attacker could also send messages impersonating the target and even manipulate them. [14]

Attacks like this can and have been mitigated using:

- Better authentication mechanisms, as has been proved to be critical in resolving some threats such as the A5/2 attack on GSM [14];
- Use of Certificate Authorities, even if the message is read and deciphered, another cypher will be behind, this as will be described ahead, is a technique already in use.

4 Security Measures in use

As an interview revealed, some manufacturers use mobile networks in conjunction with APIs to provide functions to the user via smartphones and other smart devices. These APIs limit and control the access an outside system has over the vehicle, avoiding the risk of an attacker controlling a function outside of the API.

Although the eSIM could be used for tracking, it can be disabled, leaving only the functionality of emergency calls available.

A system can be further secured from possible man in the middle attacks, by means of certificates where asymmetrical keys are used to keep the communication private and that, besides communications, all stored data is also encrypted in the systems, keeping the users' information private.

Furthermore, it has also been revealed that to avoid indirect attacks such as trojans mentioned above, all workers in the working place take part in mandatory training, to alert them over risks, such as the use of unknown USB devices, and possible threats of human engineering.

5 Conclusion

We see the world and the vehicular industry growing each day with newer developments, bringing with it much more flexibility over how we interact with our daily vehicles. A great amount of data is now used for our comfort in cars, going to the extent of using wireless methods to avoid cable complexity. With the modern car being so connected to the end user, some security risks surface, namely some privacy concerns and health hazards.

The industry and governments however seem to be steadily adapting to this new age of technology where so much information is connected between devices and has so much control over our daily life, with laws like the European Union's General Data Protection Regulation (GDPR) and some businesses investing in cybersecurity awareness of their workers.

It could be seen from this work that threat awareness is also vital, given that one form of attack, the trojan, can be mitigated by properly educating the population over possible risks caused by some common actions we deem harmless, can lead to serious security flaws.

From the results we've seen it's clear that the technology we use is in a constant wrestle between security methods and new attacks, which leads me to believe that a problem with the industry in the future could be the end of life support of the software in these vehicles.

References

1. Honda Motor Co Ltd: Engine control unit, (2003).
2. Chris Valasek, Charlie Miller.: Adventures in Automotive Networks and Control Units, IOActive, (2014).
3. Siemens Aktiengesellschaft: Electronic control unit for a motor vehicle, (1999).
4. Robert Bosch GmbH: Bosch Automotive Electrics and Automotive Electronics. Springer, (2014).
5. Lin, C., Sangiovanni-Vincentelli, A.: Cyber-Security for the Controller Area Network (CAN) Communication Protocol. International Conference on Cyber Security. IEEE (2012).
6. Mukherjee, S., Shirazi, H., Ray, I., Daily, J., Gamble, R.: Practical DoS Attacks on Embedded Networks in Commercial Vehicles. 12th International Conference, ICISS (2016).
7. Zhang, T., Antunes, H., Aggarwal, S.: Defending Connected Vehicles Against Malware: Challenges and a Solution Framework. IEEE Internet of Things Journal. 1, (2014).
8. Rouf, I., Miller, R., Mustafa, H., Taylor, T., Oh, S., Xu, W., Gruteser, M., Trappe, W., Seskar, I.: Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study. 19th USENIX conference on Security (2010).
9. Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., Kohno, T., Comprehensive Experimental Analyses of Automotive Attack Surfaces. SEC'11 Proceedings of the 20th USENIX conference on Security (2011).
10. Luo, X., Liao, Q.: Awareness Education as the Key to Ransomware Prevention. Information Systems Security. 16, 195-202 (2007).
11. Sauter, M.: From GSM to LTE-advanced pro and 5G. Wiley (2017).
12. Corallo, A., Cremonini, M., Damiani, E., Vimercati, S., Elia, G., Samarati, P.: Security, Privacy, and Trust in Mobile Systems (2015).
13. Ochang, P., Irving, P.: Evolutionary Analysis of GSM, UMTS and LTE Mobile Network Architectures (2016).
14. Meyer, U., Wetzel, S.: On the Impact of GSM Encryption and Man-in-the-Middle Attacks on the Security of Interoperating GSM/UMTS Networks. IEEE 15th International Symposium on Personal, Indoor and Mobile Radio Communications (2004).