# Attacks to the new connected vehicle: radio-frequency and vehicle internal network

Víctor Jiménez García, Ph.D. Mario Reyes de los Mozos
Fundació Eurecat, Barcelona, Spain

**Summary**

The connected vehicle is already a reality and its penetration rate will enhance exponentially in the next years. Wireless communications will allow the car of the future to interact with other objects in its environment (infrastructures and other vehicles), as well as benefit from the different services that will be emerging in the automotive and mobility sector. The complexity of communication networks, the large number of connected objects, the processing power and decision-making capacity of vehicles, as well as the high number of actors that will be related to the connected car, increase significantly the number and types of attack surfaces. Besides that, it's well known that connected ECUs open the possibility to remote access the vehicle internal network. This paper shows results of three examples of the weakness of a current connected car, specifically in relation to electronic control components (ECU), communications architecture and protocol (CAN) and radio frequency communication.

## 1 Introduction

Cybersecurity for computers has been treated and discussed for a long time, and a considerable number of guidelines, standards and tools have been generated. On the other hand, in recent years, cybersecurity for non-computers (such industrial, transportation, utility, home appliances, and others) has become a serious social concern, mainly because a problem of cybersecurity directly affects the safety of people. The automobile industry is not exempt from problems of cybersecurity. We must consider that the vehicle is not an isolated object, it is part of the so-called Internet of Things, where it requires tight integration of computing, communication, and control technologies to achieve stability, performance, reliability, robustness, and efficiency. The autonomous, connected and collaborative car is part of this new model of transport system, which may be called Intelligent Transport System (ITS). With the introduction of ITS, new challenges must address the automotive industry, challenges that Information and Communication Technologies (ICT) domain are dealing for a long time: privacy, availability, integrity, authenticity, confidentiality, and accountability. We must not forget that the car of the future will be one of the priorities for criminal acts using common techniques in ICT, as Ransomware, APT (Advanced Persistent Threats) and so on.

In the previous edition of FORMForum (2016) we introduced the procedure for evaluating the resilience of a connected car where we described the procedure for an intrusion test on the connected car, where a critical cyber-attack on a modern vehicle

usually requires three stages: access to the internal network of the vehicle, communication with other ECUs, and access to the ECU that allows the attacker to perform the desired action. In this work we have classified the attack surfaces into 4 domains: ECUs, Communication (in-vehicle network), Architecture and Extended Vehicle (external networks), showing the process of exploitation in three specific cases. In the process of exploiting these systems, we first perform a vulnerability analysis that allows us to detect the weakest points of each of them. We will then use the most appropriate tools to exploit the vulnerabilities found and analyse the real impact that an attack would cause.

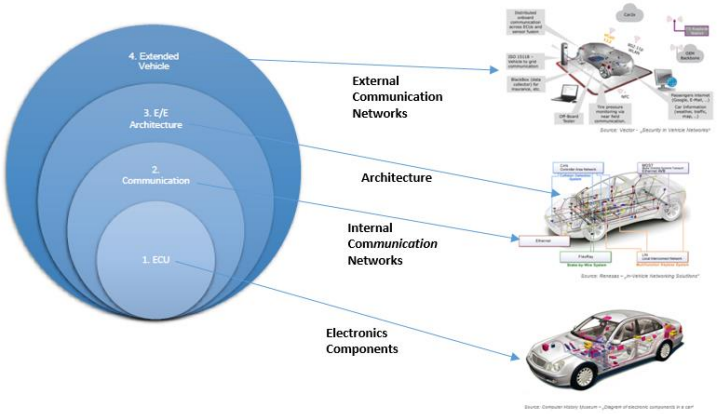


Figure 1. Attack surfaces.

## 2 Electronic Components

The first of the experiments carried out focuses on electronic components (ECU), with the aim of analysing and validating their resilience to attacks. Following the complete process of analysis, detection, definition and attack, relevant information has been obtained that compromises the driver's privacy and can be a target for malicious and fraudulent actions.

The first phase of an ECU analysis focuses on identifying the architecture, detecting each of the modules and their functionality. This process is carried out manually, by visual inspection, detecting 3 types of modules: power, ECU microcontrollers and car interfaces and telematic functions. We proceed in the same way (visual inspection) to detect the connections, where our objective is JTAG connections, that can allow us to access the memory of the ECU (Figure 2). Thanks to JTAG we have access to RAM and Flash memory, but it is not feasible to have full access on a continuous manner. The next step we performed was to try to disable the protection mechanisms implemented in the TCU. Once the protection mechanisms are deactivated, we get full access to the NOR Flash. The information we may have access

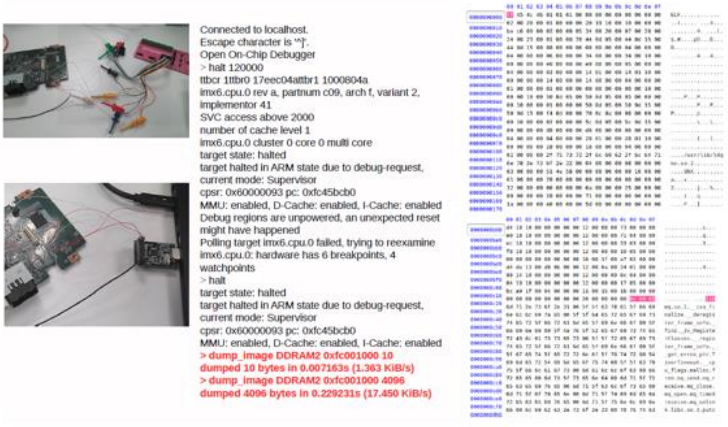


Figure 2. JTAG configuration.

to is very relevant, and can be used as a means to carry out a remote attack or fraudulent action: OS libraries code, application code, calibration data, SMS numbers, server URL's, VIN, ECU Id, GPS position, City address, phone numbers, certificates and privacy key, remote re-flash functions, wifi functions, etc.

The experiment described shows the weaknesses and vulnerabilities of the current TCU of a connected car on the road. The information that has been obtained is of high relevance for a hacker who plans to make an attack addressed to a particular user, but also if she/he wants to perform an attack against the provider of the services offered through the Internet, since it has the URLs of the servers, as well as the certificates and private keys, providing an access to their servers.

## 3 Internal Communication Networks

The second of the experiments, which focuses on CAN architecture and protocol, aims to show the existing risk in the current vehicle fleet, showing how the lack of security features of the protocol may provoke accidents. Specifically, we show the loss of control of the vehicle, launching it at an unexpected speed (and high).

The set of ECUs aimed at addressing safety-critical aspects (impact on the physical safety of people) of the vehicle are transmitted via the CAN bus, and therefore the bus must be robust to both faults and malicious actions. This problem has not been resolved, although initiatives are already beginning to emerge in this direction. With the arrival of technological advances that provide connectivity to the vehicle, the lack of security mechanisms in the CAN protocol has a direct impact on the physical security of the vehicle and people. The CAN bus is exposed to several threats: confidenciality, integrity, authetication, availability, non-repudiation.

We test the lack of security of the CAN protocol, especially when dealing with a malfunction, and the recovery of the service. If the CAN protocol shows unexpected behavior, the affected ECUs may activate their reset process, returning the ECU to an initial state of recovery. In our case, we act on the CAN protocol through the OBD connector, manipulating a certain configuration parameter, forcing a reset to the affected ECUs. During the time of anomalous behaviour of the CAN protocol we accelerate the car (by pressing the accelerator pedal), without any effect, the car does not accelerate or generate any response. We stop pressing the accelerator pedal, and re-establish the correct CAN protocol configuration parameters. At that precise moment, the car accelerates abruptly, at an uncontrolled speed.

The results obtained demonstrate the lack of security of the CAN protocol (internal communication of the critical elements of the car), which can lead to an accident if the configuration parameters are manipulated remotely and when the car is in motion.

## 4 External Communication Networks

Finally, in this third case of vulnerability analysis of the connected car we focus on the RKE (Remote Keyless Entry). The RKE operates at different frequencies depending on the vehicle and the geographical area, as well as in different modulation modes. In Europe, the most commonly used frequency for keyfobs is usually 433 MHz. But there may be other models that have another frequency like 315 MHz. The frequency modulation can be either ASK or FSK. For the tested cars there is the FSK modulation. Note that to decode the car remote control signal we need to know the frequency, the modulation, the frequency deviation if FSK, the baud rate, and perhaps the synchronization value.

Once we have all the information (frequency and modulation type), we proceed to capture and replicate the signal for a keyfob that does not have a rollcode. That is, the signal transmitted does not change, the same token is always used to open or close the doors. Usually this step works on older cars, and allows us to open the door of a car without the need to have the key fob, allowing access to the vehicle for their manipulation.

Figure 3. HackRF & Yard Stick One.

The next step is to implement an evolution of the work done by Samy Kamkar in order to access the vehicle without forcing the lock (Rolljam Attack). We are focused on the capture and analysis of radio frequency signals (HackRF and Yard Stick One hardware have been used for this type of attack). To carry out the rolljam attack it is necessary to perform a jamming attack on the vehicle's receiver, so when the victim tries to open the car by pressing the key button, it will not work but we will record this signal. Seconds later the victim presses the door opening button again, the transmitted signal begins to be recorded and the previous recorded signal is sent. So, the victim can open the car and does not suspect that the attacker has a valid code to be used next time. So we get a valid key code to open the car doors.

The final experiment carried out in relation to the RKE consists of analysing the resilience or robustness of the rollcode1 for a determined car model. In order to perform this analysis it is necessary to decode the various signals that are transmitted each time the open/close button is pressed. In order to decode the packets of a transmitted signal, the following data must be known: frequency, modulation, frequency deviation, baud rate and bit encoding. The signal is decoded and digitized, in order to be

1 The rollcode is a secret, one-time-use code that is transmitted each time a vehicle key's unlock button is pressed.

processed and analyzed by GNURadio or Eurecat's own software. The analysis shows that the rollcode is composed of:

- an initial preamble to the code,
- synchronisation values,
- door opening code or door lock code

allowing to create at any time the necessary code for opening or closing doors. This experiment illustrates the weaknesses in wireless communication in the connected car. The ability to digitize communications and process them with software increases the possibilities of unauthorized access to the connected car.

## 5 Conclusions

The automobile industry is not exempt from problems of cybersecurity. For a long time, with the introduction of a large number of electronic components, vehicles have large security risks. The risks and threats to which is exposed the current vehicle are mainly due to the fact that are parked in places with easy access and because in the process of designing and manufacturing designers have not taken into account an appropiate design to cope with vulnerabilities of the vehicle which can be exploited by an attacker. Besides illegally manipulated vehicles threaten drivers and passengers lifes, and in the worst case, they can provoke big damage and losses. In this paper we show three examples of the weakness of a current connected car, specifically in relation to electronic control components (ECU), communications architecture and protocol (CAN), and radio frequency communication. The impact of each of these attacks is different, affecting the privacy of individuals, the physical security of individuals, as well as the theft or manipulation of the vehicle.

The three examples included in this paper allow us to define a set of procedures and tools to assess a vehicle's resilience to attacks. In such a way, it would be feasible to develop a system for evaluating and managing the risk of a vehicle, determining the real impact in relation to safety, security, privacy, fraud, theft, etc. Likewise, these tools would be of great value to automobile manufacturers, allowing them to introduce the necessary countermeasures for vehicle protection.

Manufacturers need to know how security breaches could affect the car safety and, indeed, the passengers on it. However, this is a reactive response to the problem, requiring a proactive attitude, taking into account safety aspects from the outset. It is necessary to apply methodologies such as Security-by-design, Resilience-by-design, and Privacy-by-design during the design and production process of the connected vehicle.