Assessment of Components Vulnerabilities in Undentified Remote Access

Ph.D. Mario Reyes de los Mozos, Ph.D. Juan Caubet, Samuel Expósito
Fundació Eurecat, Barcelona, Spain

Álvaro Arrue, David Fernández
Applus IDIADA, Spain

Summary

The connected vehicle is already a reality and its penetration rate will enhance exponentially in the next years. It's well known that connected ECUs open the possibility to remote access the vehicle internal network. We must add the emergence of autonomous, connected and collaborative car over the next few years, where the vehicle are exposed to a greater number of threats, becoming one of the main targets for hackers in the very near future. In this communication we assess the options for an attacker to achieve their objectives in a certain vehicle, his motivation, and how to exploit vehicle vulnerabilities. This paper grants a new automotive cybersecurity vision focused on electronic components, their vulnerabilities and how to deal with them from the hacker point of view.

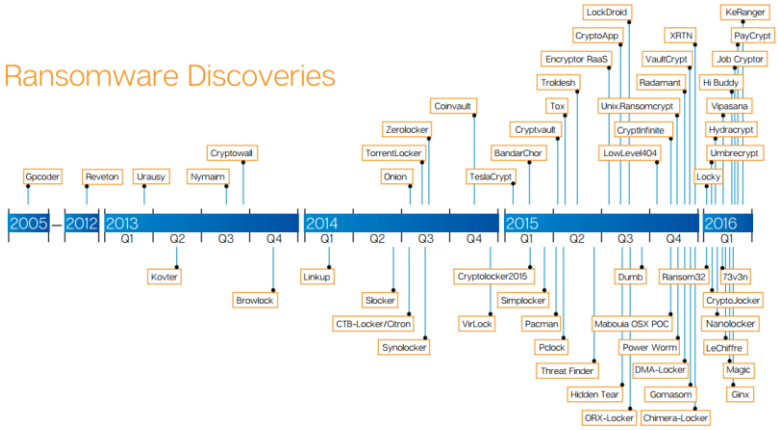
1 Introduction

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. 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 exposed the current vehicle is mainly due to that are parked in places with easy access, and because in the process of designing and manufacturing have not taken into account changes to copes with vulnerabilities vehicle which can be exploited by an attacker. Besides illegally manipulated vehicles threaten drivers and passengers lives, and in the worst case, they damage communities in a large area. There are numerous examples that we can find where a vehicle is compromised (Jeep Cherokee, Volkswagen, Jaguar XFR, Toyota Corolla, Mitsubishi Outlander, Nissan Leaf, etc.). The automotive industry has a new challenge ahead.

Moreover, 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 Iinformation 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 (Figure 1), and so on. The automotive industry and ITS should be prepared to introduce appropriate detection and protection measures.



Source: Blog of Heimdal -- "What is Ransomware ans 15 easy steps to keep your system protected"

Figure 1. Ransomware discoveries.

In this paper we introduce a method for cybersecurity assessment of a vehicle. To do this we will use common methodologies of Ethical Hacking. The ultimate goal of this process is to get an objective assessment of the resilience of the vehicle to attacks that can occur within an Intelligent Transport System. With this cybersecurity assessment, the necessary corrective measures, firmware and software updates, detection mechanisms, prevention, mitigation and recovery of vehicle will be defined (outside the scope of this paper).

2 Ethical Hacking

The car of the future will be an essential object in the future society, not only in terms of mobility of people, but also in other aspects such entertainment, health or insurance. For this reason, the car of the future will be a priority to consider to be attacked. According motivation, we can group and identify the following attacker's profiles:

- **Ethical Hacker.** We call hacker the attacker that has no malicious motivation on target. They do not want to harm the company reputation or the vehicle owner (if not himself). They are characterized by their high level of expertise and achieving their goal is associated with a personal challenge or improving the car performance (tuning).
- **Industrial hacker.** In this case the attacker has a purely economic incentive, which makes him even more dangerous than the previous profile. It is backed by a company, usually competitors, which offer two of the most important factors

in hacking: time and money. The most important goal would be the theft of intellectual property. However, sabotage a particular car model, could seriously damage the reputation of a company for a long time.

- **Professional criminals.** This profile is usually focused on the hacking of high-end vehicles. The main objective of these attackers is theft, therefore they focus on the attack vectors that provide access to the vehicle and disable security countermeasures. Otherwise, the same attacker may not be interested in the vehicle itself, but in the personal information they contain, such as the drivers home address.
- **Terrorists.** This attacker is surely the most dangerous of all. Its main objective is to undermine any measure that might jeopardize the safety of the passengers.

The Ethical Hacker model is that we will adopt during the process of security assessment of a vehicle. The purpose of an Ethical Hacker is to assess the security of the network of a complex system (in this case, a vehicle and its internal networks of ECUs). To achieve this objective, he must analyze the vehicle searching for any vulnerability, trying to exploit the vulnerability in order to determine whether unauthorized access or other malicious activity that may compromise vehicle security and occupant's safety are possible.

It is called Penetration Testing the live test process of the effectiveness of security defenses through mimicking the actions performed by an Ethical Hacker. For the execution of a penetration testing the ethical hacker simulates a criminal attack under controlled conditions:

- **Definition of entry points**. First step is to determine which connectivity devices that may be attacked are.
- **Ability to perform an attack**. Once entry points are identified, these will be tried to compromise using several cyber-attacks, obtaining the possible security breaches.
- **Define the breach level**. If any of the performed attacks succeeds, next step is to determine its level of penetration. Attacks can be passive (attacker only can eavesdrop, intercept messages or resend it) or active (attacker can manipulate data or generate new data), but their impact can have a very broad range.

Bellow, we develop the phases composing a penetration testing on a connected, collaborative and autonomous vehicle.

3 Methodology

ECUs are the most risky components of a modern vehicle, but it is noteworthy that the options for an attacker to achieve his ultimate goal are also given by the remote connection points of the vehicle, the topology of the internal networks, and even by the security measures implemented in its ECUs. A critical cyber-attack on a modern vehicle usually requires three stages: access to the internal networks of the vehicle, access to the ECU that allows an attacker to perform the desired action and

communication with other ECUs. Bellow we describe the different phases of this process.

3.1 Attack Classification

The different kind of attacks could be classified according to a different criteria: depending on the type of attacker, the vulnerability which has been exploited, the result obtained or the attacker's goal. Taking into account those criteria, and focusing on the attacker's goal as the main criteria, we could describe the following examples:

- **Theft.** This goal could be tagged as the most obvious reason. For example, the attacker could exploit a wireless protocol vulnerability to unlock and deactivate the security alarm.
- **Improve performance (tuning).** In this case we try to include all the situations which the attacker is usually the car's owner. The goal is to improve the car performance modifying the source code of certain ECU or the data it receives.
- **Sabotage.** In this type of attack we include all those actions which try to deteriorate the vehicle security and safety features like disabling a certain ECU, altering its source code or deny its service on the internal network. The consequences of this type of attacks can cause minor inconveniences (turn off the air conditioning) or critical accidents (deny the brake pedal response). Another way to make a sabotage is known in the world of computing as Ransomware. This type of attack block and leaves the system unusable until the vehicle owner makes a payment for an unlock code. Sabotage attacks are a threat that could eventually cause serious damage to the brand reputation.
- **Intellectual property theft.** The attacker could attempt to obtain information about the internal network and their ECUs. He could analyze the packets flowing through the data bus in order to determine the communication protocol and try to understand the behavior and functions of all ECUs. From this point, the attacker could publish the detected vulnerabilities or create and sell a cheaper ECU not approved by the manufacturer.
- **Privacy breach.** The relationship between the increment of electronic components in our vehicles increases in parallel with the amount of personal data we keep in the car. A common sample of this could be a call log, contacts linked to the mobile phone, GPS coordinates indicating historic locations or home/work address.
- **Personal challenge.** We should not forget that human curiosity is one of the strongest human aspects that have allowed go forward in the computer history. Having the full control of a vehicle in our hands could be a strong enough motivation.

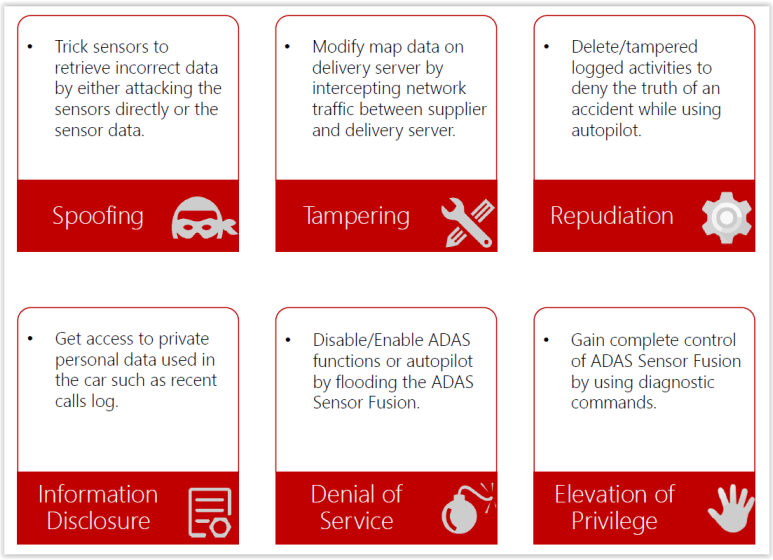
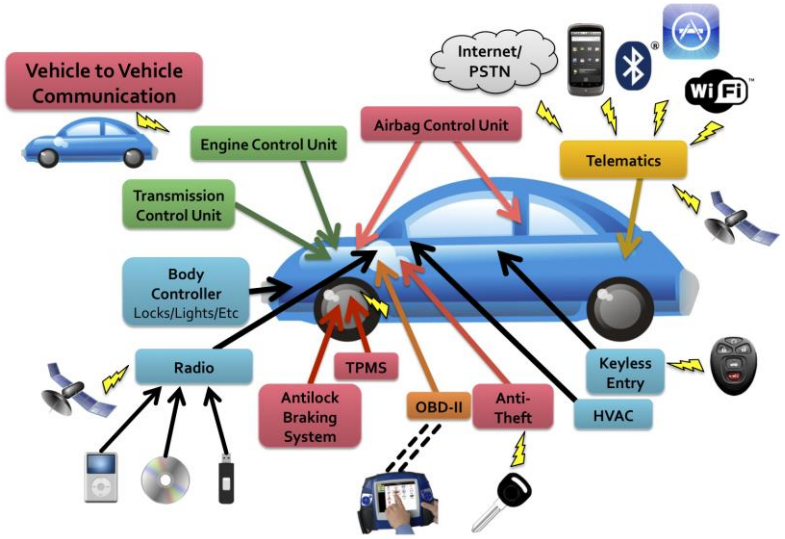


Figure 2. Some of the objectives of a car hacking.

Finally, it is considered that an attack has been carried out successfully if the attacker has achieved to perform one or more actions (Figure 2) within the system for which he was not authorized. Some examples of successful actions within modern vehicles are: denial of service (e.g. blocking the break system), the disclosure of confidential information (e.g. the privacy of the driver may be compromised), corruption of information (e.g. a manipulated ECU could allow sending corrupt information to other vehicle components), or theft of resources (e.g. a cyber-attack may open the inside of a vehicle).

3.2 Attack surfaces

The first objective of a penetration testing is to identify all attack surfaces of the vehicle, characterize those surfaces, identify the affected devices and the components that integrate them, study the existing connections between those components, and finally know the format of the exchanged messages. Attack surfaces can be both physical and remote, and then remote surfaces can be classified depending on the distance from which they can be reached. Some examples are as follows:



Source: Technical paper -- "Comprehensive Experimental Analyses of Automotive Attack Surfaces"

Figure 3. Attack surfaces of connected car.

3.2.1 Physical attack surfaces

On Board Diagnostics (OBD) Port: It is a physical port that allows identifying and reporting infrastructure problems of the vehicle. Once the attacker is connected to the ODB port, he can easily eavesdrop traffic on the vehicle's buses, and even send messages.

CD Player: Playing a manipulated music CD can turn the CD player into a gateway to the internal network of the vehicle. Some successful attacks have used the CD player to play a manipulated song which deceived the system into installing a malicious software update or sending messages to the internal network.

USB Port: The USB port can also be used to perform similar attacks to those explained above. In this case, a USB flash drive storing malicious software to be executed by the media player could be connected to that port. Other attacks can also be performed by the connection of a compromised device. Once the device is connected to the USB port it is ready to launch an attack directed to a certain ECU in order to gain access to the internal network, inject malicious messages or even conduct a denial-of-service.

3.2.2 Remote attack surfaces (short distance)

Passive Anti-Theft System (PATS): The keys of most modern vehicles incorporate a chip to communicate via RF with the steering column. Once the key is turned to start the car, the onboard computer communicates with the key to verify its authenticity. Such systems could be used to perform a denial-of-service attack, which would avoid to start the car even using the right key.

Tire Pressure Monitoring System (TPMS): This system consists of several pressure sensors located on wheels, which send data via RF to a dedicated ECU. Sending malicious messages from a short distance to the vehicle could disrupt the operation of that ECU, which could alert the driver unnecessarily, among other malfunctions.

Remote Keyless Entry / Start (RKE): Modern keys contain a RF transmitter that communicates with an ECU to open/close doors, turn on lights, or even remotely start the car. The key sends its identification data (encrypted) to the ECU so that it can determine whether the key is valid or not. These systems could be used to perform a denial-of-service attack or even get inside the vehicle.

Bluetooth: The Bluetooth stack is considerably large, and unfortunately many vulnerabilities have already been known. Basically there are two different types of attack scenarios that involve the Bluetooth stack. The first involves an unpaired device. And the second occurs when a device is already paired. This second case requires prior user interaction.

3.2.3 Remote attack surfaces (long distance)

Vehicle-to-Vehicle (V2V) Communications: Communications between vehicles allow sending safety alerts, traffic information, etc. to other vehicles. But they are also liable to be misused; an attacker could send false information or even compromise the ECU responsible for such communications.

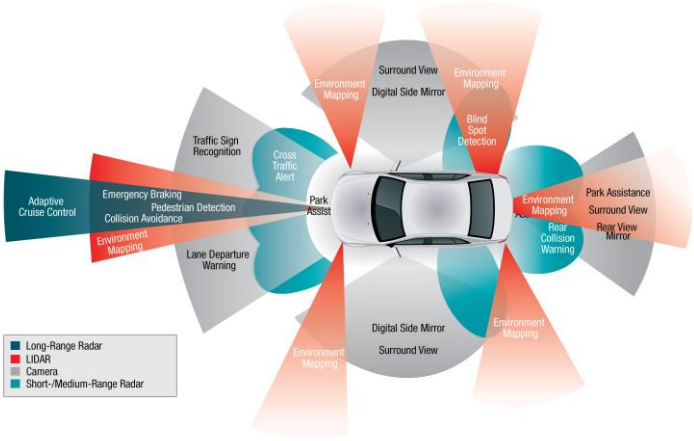
Radio Data System: In the same way that a music CD or USB flash drive may contain manipulated songs to be played by the media player, radio signals (FM, AM, satellite, etc.) can also contain malicious data.

3G/4G/Wi-Fi Connections: Many modern vehicles have an Internet connection via 3G/4G and/or Wi-Fi. This connection is usually used to get diverse information (weather, traffic, etc.), provide Internet connectivity to the vehicle passengers (hotspot), or even make emergency calls. Due to its wide range of applications, these devices are susceptible to many attacks; therefore they should be protected accordingly.

Smartphone Apps: In many modern cars it is now possible to receive information and perform actions through a smartphone application (for example, receiving information of the last route, turning on the lights, or rolling down the windows). And on the other hand, although in less cases, it is also possible to install third-party application in the infotainment system. These scenarios open another gateway to malware, trojans, etc. The use of untrusted application stores, or the manual installation of applications, may cause the existence of malicious software on the system.

3.2.4 Other types of attack surfaces

There are another types of attack surfaces that can be used to compromise a autonomous and cooperative vehicle. Attacks that can be performed in relation to these surfaces are non-invasive to the internal network of the vehicle, and do not alter any of its electronic components and control (ECUs). The attacks exploit functional vulnerabilities of different control systems of an autonomous and cooperative vehicle. Some examples are:



Source: Texas Instruments -- " LIDAR, cameras, radars, ACTION! The road to autonomous vehicles"

Figure 4. Attack surface of the self-driving car.

- Infrastructure sign, road sign (static or dynamic) installed by road operator or government agencies to inform drivers
- Machine vision, video image processing used for object detection (road, obstacles, road signs, etc.
- Acoustic sensor that recognizes a trained/known signal
- Radar, Active system that uses return of microwave radiation (radio waves) to detect objects
- Lidar (light detection and ranging), Active system that uses return of infrared (IR) or visible light instead of radio waves to detect objects.
- Odometric sensors, wheel encoders and inertial sensors (accelerometers, gyroscope, etc.) used for inertial odometric navigation

- Maps, in the case of non-real-time detection of road, maps are used to give longitudinal and lateral directions to the autonomous automated vehicle
- Infrastructure, the infrastructure defines the set of entities involved in the vehicular communication that are not mobile. These entities can broadcast messages such as roadside alert and signal phase and timing
- Security system, the security system includes the infrastructure entities that manage security-related information
- Any other vehicles equipped with a cooperative system and that is capable of sending messages in a comprehensible format for the receiving vehicle

The next step on a penetration testing corresponds to the search and analysis of components vulnerabilities.

3.3 Vulnerabilities identification

One of the main phases in a process of penetration testing is seeking information in order to increase knowledge about the vehicle to hack. The goal is to get information regarding the components of the vehicle, etc. Once we have identified all the components of the vehicle, the buses that interconnect them, how they communicate, and the attack surfaces, we will collect the already known vulnerabilities of those components, buses and protocols.

On the other hand, once known vulnerabilities are documented, we will conduct a process of testing those vulnerabilities and carry out an exhaustive process of discovering new vulnerabilities at different levels:

- **Internal level:** A modern vehicle contains dozens of ECUs. An ECU attack involves modifying its firmware, changing the data that are managed, or modifying its hardware implementation. The main attack vectors to modify a firmware or the managed data are software defects or misused functions. For these reasons we will check the ECUs' vulnerabilities already known and investigate in depth the possibility of new vulnerabilities in those ECUs.
- **Internal communication level:** Although most vehicles implement the CAN bus, note that almost every vehicle has its own network architecture, uses a different number of buses (usually between 2 and 5) and combines several types of them. For this reason we will analyze in depth the bus architecture and protocols used by the vehicle for vulnerabilities resulting from inadequate design and configuration. We will check if already known vulnerabilities of each of the buses and communication protocols used in the vehicle apply in our case. On the other hand we will also check the already known vulnerabilities in sensors that send information to the vehicle via RF, RFID, etc. (very short range) and investigate in depth the possibility of new unpublished vulnerabilities in this type

Figure 5. Exploitation phase.

of sensors. In this sense we will investigate the use of radio signals to steal confidential data.

- **External level:** We will check the already known vulnerabilities of the external communication devices (Bluetooth, GPS, WiFi, etc.) available on the vehicle, and try to find new vulnerabilities that could allow their exploitation. We will also investigate potential vulnerabilities at both software and hardware, and try to use radio signals to obtain relevant information.

3.4 Exploitation

We tend to think that an attacker who wants to break the car security systems is wearing a bumping lock pick in one hand and a crowbar in the other hand. However, the inclusion of electronic components in the safety systems of automobiles has made the profile of these attackers more technical. In this phase of the project we will carry out the last stage of a hacking process. Here we have some hacking actions we will do to try to compromise the security of the vehicle by means vulnerabilities exploitation:

- Probe. To find out the behavior of an ECU with request-response messages (reverse engineering).
- Scan. To discover any element within the internal network of the vehicle which could become a potential access vector.
- Flood. The denial of service can be achieved in several ways. One of them is flooding the ECU receiver with false requests in order to collapse and force it to stop processing legitimate requests.
- Spoof. To send fake packets by pretending to be a legit internal component and causing a false level of confidence to the receiver.
- Bypass. To skip the protection of a service that is protected by authentication.
- Inject. To introduce no legitimate packets in a communication channel that can be interpreted later

3.5 Ethical Hacking Attack Assessment

For the purpose of evaluate objectively the attacks made during the Penetration Testing process, a set of terms that characterize an attack and its impact on the safety of the vehicle is defined. To do this we were inspired by the methodology Failure Modes and Effects Analysis (FMEA):

1. Description of the attack performed,
2. Attack surface, indicating the attack surface on which is carried out the attack.
3. Vulnerability exploited, describes the vulnerability exploited by the attack
4. Feasibility of the attack, describes the level of knowledge and tools needed to perform the attack. This term uses the risk levels low/medium/high, where a low feasibly means that the knowledge and tools needed is not easily accessible.
5. Ease of detection by driver, can the driver detect the attack? This term uses the risk levels low/medium/high, where a low level means that the detection is difficult.
6. Ease of detection by the system, can the system detect the attack? This term uses the risk levels low/medium/high, where a low level means that the detection is difficult.
7. Probability of attack success. This term uses the risk levels low/medium/high.
8. Impact on vehicle, describes the consequences for the vehicle such as lock the vehicle, installation of malicious software, etc. Additionally a value between 1 and 5 is assigned.
9. Impact on safety, describes the consequences for the passenger safety or people from the vehicle environment. Additionally a value between 1 and 5 is assigned.
10. Assessment of the attack, represented by a value of 1 to 5, and which is obtained based on the attribute 4-9.

The results obtained from the set of attacks provide the objective basis for assessing a vehicle on a penetration testing process.

4 Conclusions

In this paper we have presented a method for assessing the cybersecurity of a vehicle, and its impact on passenger's safety. To address this problem, we show that the first action is identify the different adversary models, the different kind of attacks, and the type of attacker. According attacker motivation, we can group and identify several attacker profiles. On the other hand, we have considered that an attack has been carried out successfully if the attacker has achieved to perform one or more actions within the system for which she/he was not authorized: denial of service, disclosure of confidential information, corruption of information, to carry out terrorist acts, or lock the vehicle.

We explained that a critical cyber-attack on a modern vehicle usually requires three stages: access to the internal network of the vehicle, access to the ECU that allows

the attacker to perform the desired action and communication with other ECUs. The assessment procedure that we have presented starts with the identification of the attack surfaces of the vehicle, characterizing those surfaces and identifying the affected components. Attack surfaces can be both physical and remote, and then remote surfaces can be classified depending on the distance from which they can be reached. Once the attack surfaces and the affected components are identified, the vulnerabilities of those components will be assessed. Finally, a classification of different attacks taking into account the vulnerability that could be exploited, will be performed, obtaining as a result, the attacker's goal or the type of attacker that has performed the attack. During the implementation of this procedure, we have drawn a map of attack surfaces (physical and remote) and vulnerabilities of a particular automobile model, determining the depth of different threats. To do this, standard pentesting techniques were used, as well as ethical hacking and other methods of intrusion, both digital and analog.

5 References

[1] Petit, J..; Shladover, S.E.
Potential Cyberattacks on Automated Vehicles
IEEE Transactions on Intelligent Transportation Systems
September 2014

[2] Onishi, H.
Paradigm Change of Vehicle Cyber Security
4th International Conference on Cyber Conflict
Tallinn, 2012

[3] Yadav, A.; et al.
Security, Vulnerability and Protection of Vehicular On-board Diagnostics
International Journal of Security and Its Applications
Vol. 10, No. 4 (2016), pp.405-422

[4] Millet, C.; Valasek, C.
Adventures in Automotive Networks and Control Units
IOActive Report
2015

[5] Kamkar, S.
Drive it like you hacked it (presentation)
DEFCON 23
2015

[6] Millet, C.; Valasek, C.
Car Hacking: For Poories
IOActive Report
2015

[7] Prathap, V.; Rachumallu, A.
Penetration testing of Vehicle ECUs
Department of computer science. Chalmers University of Technology
Gothenburg, Sweden, 2013

[8] McDonnell, A.
Reverse Engineering Embedded Software. An introduction using Radare2
Linux.conf.au
Auckland, 2015

[9] Seeber, B.
Hacking the Wireless World with Software Defined Radio 2.0.
2015

[10] Harnett, K.; Watson, G.; Harris, B.; Clark, J.
Recent Vehicle Cybersecurity Attacks Vulnerability Research and State-of-the-Art Mitigations
October 22, 2015

[11] Ghanem, M.A.
BackTrack System: Security against Hacking
International Journal of Scientific and Research Publications
Volume 5, Issue 2, February 2015

Hoa La, V.; Cavalli, A.
Security attacks and solutions in vehicular ad hoc networks: A survey
International Journal on AdHoc Networking Systems (IJANS)
Vol. 4, No. 2, April 2014