The Insights into Car Hacking

EEL 6931 – Advanced Ethical Hacking

Group Project – Spring 2014

Mark Bacchus
FIU - Computer Engineering Department
Florida, United States
2394870
Mbacc001@fiu.edu

Maria A. Gutierrez
FIU - Computer Engineering Department
Florida, United States
2227112
mguti023@fiu.edu

Alexander Coronado
FIU - Electrical Engineering Department
Florida, United States
2605672
Acoro012@fiu.edu

***Abstract*— Cars have come a long way. The most important aspect that has been constantly changing in cars is the technology that they are built with. Today, computers are essential and play a big role in cars. Almost everything is controlled by computers, which are as vulnerable as any other computer out in the world.**

***Index Items*— Car, hacking, wireless, ECU, PCM, research**

I. Introduction – Car Technology

Technology is constantly changing. It affects everything in a person's life, including their vehicle of transportation. It does not matter what type of car you may drive, the basic structure of computers in car is the same. Some computers will control almost the entire car; others may just control the main features of the car. In this paper, it will be discussed the different computers a car has, the research that has been done on car hacking, and finally the future expectations.

A. Different Computers

A car is composed by many computers; all these computers are the ECU (Electronics Control Unit). Here is a small list of computers that compose an ECU is: ECU (Engine Control Unit), PCM (Powertrain Control Module), CTM (Central Timing Module), SCM (Suspension Control Module), GEM (General Electronic Module), TCM (Transmission Control Module), BCM (Body Control Module), EBCM (Brake Control Module), CCM (Central Control Module) and others. The two main computers that will be discussed in this paper are the Engine Control Unit and Powertrain Control Module. The Engine Control Units are the most dominant computers the car has. There are also other microprocessors, which are essential for the car engine to run; this is due to the global specifications a car has to meet in order to be able to be sold.

The elements of an ECU are as follows:

1. Core of the computer:
    a. Clocks
    b. Microcontrollers
2. Inputs of the computer:
    a. Supply Voltage
    b. Analog Inputs
    c. Digital Inputs
3. Memory
    a. SRAM
    b. Flash
    c. EEPROM
4. Connector
5. Housing
6. Communication Links:
    a. USB
    b. Serial
    c. Flex ray
    d. CAN Bus
7. Outputs
    a. Logic Outputs
    b. H Bridge Drivers
    c. Relay Drivers
    d. Injectors Drivers

In this section, it will be discussed in detail ECUs, and PCMs.

1) ECU

As previously mentioned, the Engine Control Unit is one of the computers in the car that is most dominant and powerful. This computer works with closed-loop control. This scheme, the closed-loop control, is in charge of monitoring the system's inputs, some parameters such as the fuel economy, and the emissions' management. These

computers gather lots of information that has to do with the sensors located around the vehicle. It works by reviewing tables that exist in the system and making a lot of calculations per second.

It is like a small computer containing 32-bit and a 40 MHz processor, which is enough since the code that it handles is no more than 1 MB of memory in total.

The components that are supported by this processor are:

1. High-level digital outputs: these are the on and off digital outputs that the systems transmits; for example, the cooling fan being on or off.
2. Analog-to-Digital converters: the car's sensors give an output in analog, which the car cannot read because it only reads digital outputs. This way, the ECU converts the output from analog to digital and performs the task that is needed.
3. Digital-to-Analog converters: the same applies here. Whenever the ECU needs to send an output to the sensors or any other computer in the car, it needs to be in analog. The ECU only comes up with digital outputs that need to be converter to analog.
4. Signal converters: these components adjust the inputs and outputs whenever it is needed.
5. Communication Chips: these components are the CAN (Controller-area networking). They are mainly used for the implementation of the communication standards. These standards let the communication have a speed of up to 500 Kbps. The communication is through two wires.

2) PCM

As stated earlier, PCM or Powertrain Control Module is the computer that takes care of the engine managements and driveline components. These are a multi-layered circuit that adjusts and monitors all the mixtures such as fuel and air.

It also uses catalytic converters to reduce the pollution that is created by the engine. Working in two modes, the PCM either is in an open loop or a closed loop. An open loop is when the engine is cold and the computer makes the engine operate on a preset program. The closed loop is when the engine is at right temperature and working. For a closed loop, the computer uses various sensors around the car to operate the engine.

Other of the tasks that the PCM takes care of is adjusting the system's sensors as it is necessary for the car. The sensors that are taken care of by the Powertrain Control Module is mass air flow, crankshaft angle, oxygen, air intake temperature, throttle position, engine hook, coolant temperature, camshaft angle. After adjusting the sensors, the PCM starts sending the necessary feedback to other controls around the car, such as the emission system controls, or the traction controls, etc.

This is how the two main computers in the car work. Their jobs are essential for the car to work. These are the computers that are as vulnerable as any other computer in the world. This is the way hackers get into the car the easiest. In the sections to follow, we will be explaining some of the security aspects that the cars have, the research that has been done by universities, the malware that exists, the different attacks and the governmental restrictions when it comes to cars.

II. Research Done

A. Security on Vehicle Wireless

When it comes to the future of vehicle technology, Bluetooth Is often mentioned and integrated in more and facets of everyday vehicles. By using Bluetooth manufactures are able to cut down on the number of cables and simplify the bus system in a vehicle. Wireless systems give the manufacture a sense of flexibility that will allow them to do things that otherwise cannot be done in a traditional wired bus system that is found in most cars today. To summarize what Bluetooth technology basically is, it is a short ranged wireless system that uses around the 2.4 GHz frequency to transmit data. The reason why most manufactures find that it is the ideal wireless technology to be used in vehicles is because you can operate a Bluetooth signal in noisy environments. Bluetooth has the ability to hop faster and also use smaller packets then most other wireless technologies. This is so efficient that it even limits the impact of microwaves on the signal. The reliability of this does not stop there, as it also supports multi-channel transition so that data can be transmitted even faster. Bluetooth technology is also seen as ideal for vehicle systems because the distances that you need to cover are in most cases very short. There are 3 classes of power when it comes to Bluetooth signals, 1mW, 2.5mW, and 100mW. These power frequencies allow for distances of between 10 to 100 meters.

Frequency Band	- 2.4 GHz ISM Band
Output Power	- 1 mW / 2.5 mW / 100 mW
Range	- 10 m - 100 m (dependent on Power Class)
Modulation	- 2-GFSK
Frequency Hopping	- Up to 1600 hops/s - 79 (23) Hopping-Channels (1 MHz)
Number of Devices	- 8 per Piconet - ~ 10 Piconets in one environment
Services	- Speech (3x64 kBit/s) - Data (DL:721 kBit/s, UL: 58 kBit/s or 433 kBit/s DL/UL)
Speech-Codecs	- LogPCM - CVSD
Module (Q2/2000)	- ~ 25 mm x 15 mm x 4 mm - 3.3 V; Standby: 0.3 mA, Connect: 40 mA

Figure 1. Bluetooth Technical Details

Bluetooth systems biggest advantage that will allow it to work well in vehicle is its ability to support both point to point, and point to multipoint connections. You can have in one piconet; up to 7 devices all connected together, sharing information. Today, you mainly see the use of Bluetooth networks used in vehicle media systems to connect devices such as laptops and phones to your car. We are seeing a change in technology however due to low price and wider availability, that is introducing the use of its Bluetooth technology in providing car status information to the users

mobile device (if there is a CAN bus link between the media system and the car). Even though Bluetooth is an easy system for a vehicle to use, it is also an easy system for an attacker to gain access to through blue jacking. An attacker can perform a variety of attacks such as accessing the phone book of a car or sending audio, or retrieving audio (phone calls) through the cars Bluetooth network. There is even software out there such as 'Car Whisperer' which allow you to tap into a phone or vehicle to access the sound being transmitted with no extra software besides a computer and a Bluetooth driver. Someone gaining access to your media and personal info might not sound that bad, but with the integration to the CAN bus system, where people can actually start their car remotely, unlock doors, etc. It becomes very dangerous for someone to have access to your vehicle.

B. Bluetooth based Attacks

Most modern cars now a days have very complex systems, most have some sorry of keyless entry and key less start that come standard, and this is called a PKES system. While this is a great invention and makes life easier on drivers, it also opens up a new security vulnerability in which attackers can take advantage. A typical attack of a PKES system involves an attacker placing a device near the key and another device near the car. What that does is it carries over the signal from the key to the car without either having to be close to each other. Relay devices such as this one are available online for purchase, many times under 1000 dollars. Before I describe any attacks, I will briefly explain how a PKES system works exactly. First you have the car that occasionally sends out a beacon (or when the handle is pulled) that is recognized by the key, when you key sees the signal; it will demodulate it and interpret it. Then the key replies to the car with the response message and then the car unlocks it. The car starts itself in a similar way, only this time keeping in mind the region that the key is in.

(a) A PKES Key and its backup physical key. (b) Car LF coverage.

Figure 2: PKES Key FOB Coverage

There are several types of relay attacks. A normal relay attack just involves placing a device near the key and another near a car to make it seem as though they are in close proximity to each other. This attack is commonly done in two ways, the first of which is a Relay Over-Cable Attack. This is where the signal from the car to the key and vice versa is transferred via a coaxial cable. There is also a Relay over The-Air Attack, which is used for long distance. It catches the signal from the emitter and boosts it up to around 2.5 GHz and transmits it to another antenna that is near the key that grabs the signal and then down converts it to match the frequency required by the key. Now there are a number of preventive measures one can take to ensure the safety of their vehicle. One could be to shield the key in a metal casing to prevent the RFID chip within from transmitting. One could also remove the battery from the device when not in use. The most viable one in my mind would be a software modification that would allow you to activate and deactivate the key whenever you need it.

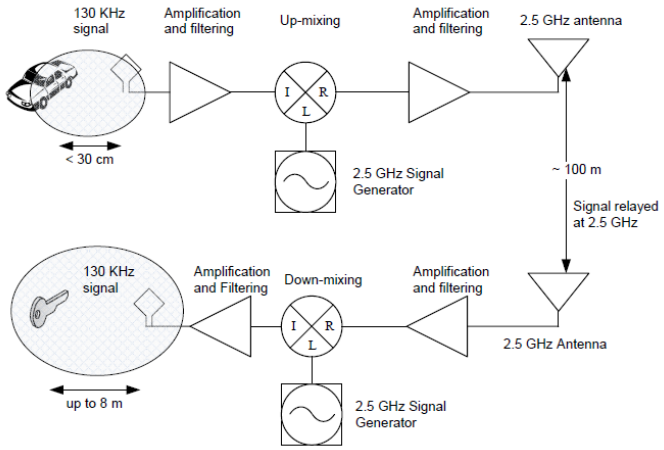

Figure 3: Up and Down Conversion and Modulation of Signal

C. Vehicle Malware

1) Vehicle Malware

Nowadays most of the new cars are integrated with electrical devices that can communicate external devices through the electronic network composed of several Electronic Control Units (ECUs) that are connected to a bus where any information can be broadcast to any connected node. This has lead the vehicles in a security risk and attackers take advantage to access with low cost available tools access to vehicles for exploiting its security vulnerabilities and as successfully access to the automobile [4].

2) Automotive Networks

Among the multiple networks that an unauthorized user can access can be listed as follows:

CAN (Controller Area Network): Is a serial bus designed for Ethernet networks based on CSMA/CD (Carrier Sense Multiple Access / Collision Detection).

LIN (Local Interconnect Network): Based on Master Slave model, where a slave can only send a message if previously asked by the master. This network is common used for controlling elements such as electric windows lifts and windshield wipers.

MOST (Media Oriented System Transport): is used to manage multimedia data via optical fiber. The MOST is in charge of streaming data such as audio or video signals.

OBD (On-Board Diagnostic): Is a standard that monitor statistics of a vehicle such as, speed, low tire pressure, RPM among others. The OBD is connected to multiple sensors in different parts of vehicles to locate abnormal changes in the system.

With this potential networks vulnerabilities in an automobile, attackers has set eyes on these targets make unauthorized modification on the code to lower the miles on a car [4], unlock and deactivate alarms and targeted cars, counterfeit, stole personal information from users or just for the challenge of talking control of somebody else vehicle. With this malicious actions security in the vehicle network has become a serious concern nowadays.

a) Remote Attacks

ODB Port: This diagnostic port has the option of plug a device to remotely control it via Wi-Fi, such as the device ELM327 OBD2 Auto Scanner Adapter Scan Tool Wi-Fi enable [1] which make this port vulnerable to any attack made from a regular computer. This pass-thru device not also can transmit malicious packets onto the network but use this tool as a virus distributor to other automobiles that share the same device, for example a car dealer or an automotive repair center.

USB Port: Since it is an input connected to the network of the car, the insertion of a file with unauthorized malicious software or the possibility of connect a compromised device (smartphone, USB drive) which would perform an attack against the ECU of the vehicle.

Bluetooth: Wireless pairing of mobile devices with the vehicle and use features like sound system or the hands-free devices is very common nowadays. However exploiting a possible vulnerability can lead to access to personal information, eavesdrop into conversations and according to some document, the exploitation of the ECU [2].

Vehicle-to Vehicle communications: this feature will be one of the evolutions of the networking vehicles. The ability of communicate with near cars with the purpose of send alerts to the driver in case of some emergency braking, incoming stop light, accident ahead, e.g. This are very useful tool but at the same time can lend for eavesdropping, emission of corrupt data that could lead the driver to commit an inappropriate reaction.

Wireless Unlocking: Most of the vehicles came with the remote unlocking system to unlock alarms, doors and even to power on the engine. This service is encrypted and can be hacked as demonstrated by [4] where the encryption KeeLoq was compromised vehicles from different manufacturers with an antenna placed close to the key holder to unlock and start a car that use Passive Keyless Entry and Start system [5].

D. Keyless Technology and Relay Attacks

As discussed earlier, most cars today use keyless entry systems. This is either a numerical keypad that contains certain combinations of numbers, or a RKE, which is a remote keyless entry system, through Bluetooth, radio frequencies, or infrared.

The keypad is easily hacked into since it contains algorithms and anyone with time on their hands can decipher the code. In this section, we are going to focus in RKE.

Remote keyless entry contains two main parts: the CID (customer identification device) and receiver located on the inside of the vehicle. The CID is the key that the user holds. The most important aspect of this is that their communication between the parts is unidirectional through either Infrared (IR) or through Radio frequencies (RF); this means that the CID is the only device who sends information.

Since the transmission carries important information about the car, this makes it very vulnerable. From the moment a person holding the CID touches the car, the communication between the devices start. Now, we are going to describe in more detail some of the common attacks for passive entry systems.

1) Message Playback Attack

a) Attack

This attack is the easiest and most common attack for RKE. It consists on having a thief going up the car and recording the transmission that the car sends as soon as you grab the door handle. After having that recorded, the thief would go near the person holding the CID and play the recording. The CID will then identify the transmission and respond to it creating the communication cycle. Finally, once the CID is responding to the recording, the thief records it. He/she is now in control of the communication of your car. This way, the thief goes up to the car, touches the handle and starts the transmission. Then, the thief plays the recording from the CID and gets access to the car.

b) Available Solution

A solution that is available for this attack is creating a random challenge response. This consists on the car creating a random challenge once it is triggered. Then the CID will respond to the certain challenge presented to it. Since the challenges change, the thief recording a certain challenge will not get it right whenever he/she tries to open the car. The challenges can be created from various messages that are either new or have been transmitted already and/or a combination of those as well. The idea here is to make it difficult for the thief to figure out what the challenge is and it can't be a decipherable algorithm.

2) Dictionary Attack

a) Attack

This attack consists on an electronics dictionary created by the thief. This goes hand-in-hand with the message playback attack. The thief develops a dictionary that contains the challenges and their responses that are valid for the vehicle. To do this, the thief plays a challenge next to the person containing the CID, and then records the response and starts developing the dictionary. Then the thief does the message playback attack.

b) Available Solution

For this attack, there is no solution defined yet, other than making even more complicated challenges.

3) Two-Thief Attack

a) Attack

This attack consists of two thieves working together. They need to position themselves in the gap between the person with the CID and the vehicle, then bridge the communication. With receivers, the thieves send one another the communication of both sides. Then, they use a device that amplifies the signal. This is just like the message playback attack without actually recording the signals because they are being streamed live as if the person holding the CID was next to the vehicle.

b) Available Solution

For this attack, there are a couple of ways you can avoid being harmed. The best one is to detect the repeater. The vehicle itself can detect if a repeater is near the vehicle's range. This is done through measuring the loop time delay that it takes the signal to reach the CID. If the delay is larger than a certain value, the car will notice the repeaters. This is done through electronic devices that have high-speed.

These are the different attacks that can be done to a vehicle through the remote keyless entry systems. Since it is common in cars to have this technology, this is a big window for attackers to hack the car.

E. Governmental Restrictions

With the advancement of technology in automobiles and the increased research in these areas according to the United States Department of Transportation [1], several organizations have been established in order to regulate, standardize and innovate in the automotive arena. Participating organizations in this research can be named as follows:

AASHTO (American Association of State Highway and Transportation Officials)
USDOT (United States Department of Transportation)
ANSI (American National Standards Institute)
APTA (American Public Transportation Association)
ASTM (American Society for Testing and Materials)
IEEE (Institute of Electrical and Electronics Engineers)
ITE (Institute of Transportation Engineers)
NEMA (National Electrical Manufacturers Association)
SAE (Society of Automotive Engineers)
IETF (Internet Engineering Task Force)
W3C (World Wide Web Consortium)
ISO (International Organization for Standardization)

Of the organizations previously mentioned have been selected three documents that are of interest for this research.

a) IEEE Standard for Wireless Access in Vehicular Environments (WAVE): Security Services for Applications and Management Messages.

The purpose of this IEEE standard is to protect the messages or data from attacks such as alteration, spoofing, eavesdropping among others in wireless technology. The document describes the security services that should be aware in order to certify the Confidentiality, Authentication, Authorization and Integrity in the communication between devices in the automotive network, preventing unauthorized users have access to it.

WAVE proposes a communication protocol stack for vehicular environment, using the architecture illustrated in Figure 1.

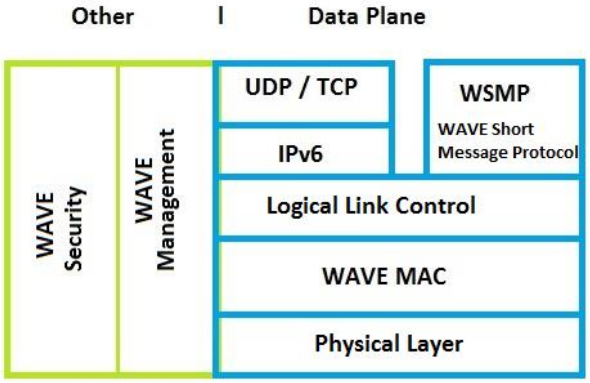

Figure 4. Wave Protocol Stack

The WAVE security block is in charge of accepts secure input requests from calling entities. The WAVE security block will respond to each request with a corresponding output confirmation containing the request as long as the private keys, public keys or certificates are valid. An implementation of WAVE security services block should include at least one of the following security processing services:

- Generate signed data
- Generate encrypted data
- Verify signed data
- Decrypt encrypted data

The WAVE Management block allows the WAVE security block to determine the trustworthiness of the certificates and received data defined on IEEE standard 1609.3 [2] required to provide WAVE networking services. Among the services provided by the management block is maintain the information of the certificates that correspond to the private keys. In this block is located the Certificate Revocation List. For the WAVE security management block it will need some of the following operations:

- Generate certificate request
- Verify response to certificate request
- Verify certificate revocation list

One of the certificates that may be use according to this standard is an explicit certificate to verify that is a trusted user illustrated in the figure 2. In Figure 3 is illustrated implicit certificate which must contain one of the following rules:

– At least one public key for a cryptosystem belonging to the certificate holder
– A list of the permissions associated with that public key
– An identifier for the issuer

A cryptographic demonstration that the issuer authorized the linkage between the public key and the permissions

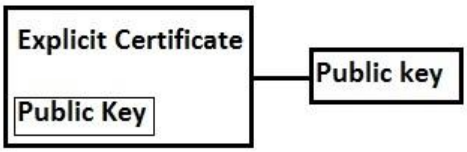

Figure 5. Explicit Certificate

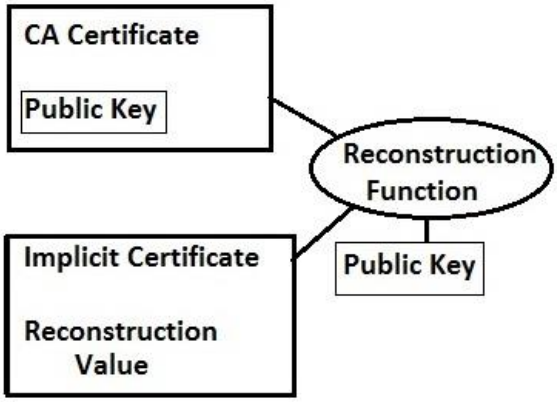

Figure 6. Implicit Certificate

Taking into consideration these parameters previously explained, it will warrantee more security in the wireless automotive transportation. Being this not the only security standard for vehicles, the U.S. Department of Transportation (USDOT) sponsors a group dedicated to the innovation in vehicles technology.

b) USDOT Research and Innovative Technology Administration

This organization focuses on intelligent vehicles, intelligent infrastructure and the creation of intelligent transportation system through integration that has been divided in: connected vehicle technology, connected vehicle applications, connected technology policy and institutional issues of which can be named the following projects:

1. Connected Vehicle Technology
   - Harmonization of International Standards and Architecture around the Vehicle Platform
   - Human Factors Research
   - Systems Engineering
   - Connected Vehicle Certification
   - Connected Vehicle Test Bed
2. Connected Vehicle Applications
   - Vehicle to Vehicle Communications for Safety
   - Vehicle to Infrastructure Communications for Safety
   - Real-Time Data Capture and Management
   - Dynamic Mobility Application
   - Applications for the Environment: Real-Time Information Synthesis (AERIS)
   - Road Weather Applications for Connected Vehicles
3. Connected Vehicle Technology Policy and Institutional Issues
   - Connected Vehicle Policy and Institutional Issues

Progress of these projects are demonstrated with Vehicle-to-Vehicle communication has been approved by the U.S. Department of Transportation's (DOT) National Highway Traffic Safety Administration (NHTSA) in Washington the last third of February of 2014 and announced that it will begin taking steps to enable vehicle-to-vehicle (V2V) communication technology for light vehicles. This technology would improve safety by allowing vehicles to communicate to each other and ultimately avoid many crashes altogether by exchanging basic safety data, such as speed and position, ten times per second.

III. Conclusion

Conclusion

In conclusion we have discussed the different systems within a car, also the types of know attacks and some ways you can defend yourself from such attacks. We have also gone into a potential in-car network that is possible with Bluetooth technology that links the car CAN bus system and the media system for a reliable all in one system. Although Bluetooth technology has made large strides over the years, there is still a of room to progressive until we have a system that is full proof and safe enough to make universal in all vehicles. In order to make significant progress and deter vehicle hacking we must analyze critical flaws in out vehicles and propose countermeasures to minimize the risks of many of the known attacks. You can never make any system full proof but the plan is to stay one step ahead of the attackers.

References

[1] Nice, Karim, “How Car Computers Work”, April 2011. HTTP: http://auto.howstuffworks.com/under-the-hood/trends-innovations/car-computer.htm

[2] Lavacot, Ken, “Computer PCM”, August 2009. HTTP: http://www.2carpros.com/articles/how-a-car-computer-works-pcm-ecm-bcm

[3] I. Studnia, V. Nicomette, “Survey on Security Threats and Protection Mechanisms in Embedded Automotive Networks”. Dependable Systems and Networks Workshop (DSN-W), 2013 43rd Annual IEEE/IFIP Conference. Budapest, Hungary, 2013

[4] Z. Fellow, “Defending Connected Vehicles against Malware: Challenges and a Solution Framework”, Internet of Things Journal IEEE. Issue 99, Fort Lee NJ USA, 2014

[5] M. Lee, “User-Level Network Protocol Stacks for Automotive Infotainment Systems". International Conference on Embedded and Ubiquitous Computing, Hong Kong, 2010

[6] J.A. Cottle, “Exploiting the Synergetic Relationship between Automobiles and Wireless Communications”. Automotive Electronics, 2007 3rd Institution of Engineering and Technology Conference, U.K, 2007

[7] R. Nusser and R Pelz, “Bluetooth-based Wireless Connectivity in an Automotive Environment”, Vehicular Technology Conference, 2000. IEEE-VTS Fall VTC 2000. 52nd, Boston, USA, 2000

[8] S. Masud and S. Shanker, “In-Vehicle Secure Wireless Personal Area Network (SWPAN)”, IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 55, Detroit, USA 2006

[9] T. Yang, “Resisting Relay Attacks on Vehicular Passive Keyless Entry and Start Systems”, Fuzzy Systems and Knowledge Discovery (FSKD), 2012 9th International Conference, Sichuan, China 2012

[10] I. Rouf, R. Miller, H. Mustafa, T. Taylor, S. Oh, W. Xu, M. Gruteser, W. Trappe, and I. Seskar, “Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study”, the 19th USENIX Security Symposium, 2010

[11] http://www.dot.gov/research, U.S. DEPARTMENT OF TRANSPORTATION, 1200 New Jersey Avenue, Washington, DC.

[12] IEEE standard 1609.3