Journal of Theoretical and Applied Information Technology
30th November 2014. Vol. 69 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

HARDWARE-SOFTWARE SYSTEM FOR MALICIOUS LOGIC DETECTION IN HARDWARE INFRASTRUCTURE OF CARS

[1] NIKOLAY KALINTSEV, [2] DMITRY MIKHAYLOV

[1,2]Engineering Centre of the National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Kashirskoye highway 31, 115409, Moscow, Russian Federation

E-mail: [1] nick.ingenium@gmail.com , [2] mr.mdmitry@gmail.com

ABSTRACT

Electronics control almost all vehicle systems. Such systems have a serious vulnerability problem at the hardware level and can be subjected to unauthorised actions by an attacker. This paper deals with the issue of security of car infrastructure. The article gives the basic information about Controller Area Network bus system, describes security problems of embedded automotive systems and the “bug” capable of intercepting driving that was developed as an example of the hardware attacks described in the paper. To solve the problems caused by the bug the special hardware-software complex was designed to detect the bug in the onboard vehicle system that can be insert for example during tech inspection. There are two main options for detecting and protecting against unauthorised connection: monitoring of resistive and capacitive condition of buses and blocking commands, which introduce one or more blocks in the service mode. The article presents an algorithm of this defence mechanism. The effectiveness of the proposed hardware-software complex was proved experimentally.

Keywords: *Vehicular Networks, Networked Control Systems, Data Buses, Car Data Security*

1. INTRODUCTION

The domain of automotive safety has been getting a whole new meaning lately due to the fact that the management systems of modern cars are becoming increasingly autonomous. Electronics control all vehicle systems now: engine, brakes, directional stability, airbags, climate control, wipers and others [1-7] and cars electronisation is still underway [8].

Nowadays a lot of cars are equipped with starter buttons, which have replaced the usual ignition key. Instead of the usual key turn the driver only needs to push the button [9]. More than half of these systems could not be implemented if not for the advanced electronics.

However, such systems have a serious vulnerability problem at the hardware level. If all possible risks had previously been limited to external or human factors, a modern car can be a source of threat in itself.

One possible threat is based on modern communication technologies. Modern cars can contact with external media through a variety of wired and wireless technologies (port USB, Bluetooth, Wi-Fi, 3G). Such interaction may jeopardise the internal network, making it vulnerable to attacks [10].

This article focuses on automated control systems in cars and suggests techniques for protecting them from the unlawful influence of a third party (namely encryption when transmitting) as well as integrity-breach and anomaly-detection methods for built-in on-board computer software.

2. SECURITY PROBLEMS OF EMBEDDED AUTOMOTIVE SYSTEMS

2.1 CAN-Bus System

Today almost all car manufacturers use electronic control units [11-15], due to the widely used standard J1939. This is a standard for communication and diagnostic networks applied to different kinds of transporting machinery, originally developed by the Society of Automotive Engineers (SAE). This standard is the source of technical information and expertise, used in designing, manufacturing, maintenance and motor vehicle driving of all U.S. vehicles. Any network, created in compliance with J1939, uses the CAN-bus (Controller Area Network) standard CAN 2.0b as a link layer. Since a large majority of operated vehicles in the United States and the European Union meet this standard, they have the CAN-bus in their structure [16].

CAN stands for Controller Area Network or Network Controller. This is a serial bus, which chains input-output devices, detecting elements and actuators in a single network. This system has a protocol that allows to put several bus masters. Those bus masters provide real-time data transmission, error correction and high noise immunity. Initially CAN-buses were used to transfer data from the engine control module to the computer for diagnostic purposes. Now each block inside the car is linked to another through this interface: the engine control unit, the unit body control, anti-lock and anti-slip blocking systems, the climate control unit, power airbags, the immobiliser, the audio system and others. All the units and systems communicate via the two wires [17].

An average car has four different bus types, each of different speed and relevance of data transmission:

- HS-CAN – high-speed bus, data transfer rate of 500 kbit/s;
- MS-CAN – medium-speed bus, data transfer rate of 100 kbit/s;
- LS-CAN – low-speed bus, data transfer rate of 33 kbit/s;
- MM-CAN – multimedia bus, data transfer rate of 500 kbit/s [15].

2.2 CAN-Bus Vulnerabilities

Like any other automatic control system, the CAN-bus system has its vulnerabilities [18-21]. Modern research on the subject defines a classification of possible attacks on a bus CAN. The classification is based on the aim of the intruder. According to the research of Dennis K. Nilsson, the electronic control units (ECU) of the car can be divided into five categories, depending on their areas of responsibility: transmission, vehicle safety, comfort, infotainment and telematics. Further, the author develops the EEC classification by four levels, depending on the potential impact on safety while driving. As a result, a classification of security threats is drawn up, based on the potential extent of any damage. That is how the author made the final attacks classification [22].

Pierre Kleberger's scientific group also studied the potential security problems of embedded automotive systems. In his work, the author highlights the vulnerability of CAN-buses and the urgent need to develop practical solutions to protect this system [23].

Among the possible attack scenarios involving the introduction of malicious code into the protocol, we can list deactivation of emergency lights, turning off the airbag system, spontaneous lowering of windows, creating the effect of surprise and loss of concentration at high speed, and other dangerous failures [24-25].

Moreover, some authors have proposed methods to detect and certify evidence in order to expose attacks, as in the near future digital and remote offences are likely to replace physical crimes in the automotive sector [26].

An advanced alternative to the CAN-bus protocol is a new protocol called FlexRay. However, it was no less vulnerable and failed to solve the problem of security in the vehicles which were equipped with this system [27].

Thus, the relevance of practical solutions to protect vehicles from attacks is important.

One of the major vulnerabilities of CAN protocols is that if an intruder manages to connect to any of the buses, he or she can subsequently gain control of the rest of them, as the body control module (BCMi) acts as a gateway for all buses (Figure 1).

In Figure 1 the following abbreviations are used:

- PCM – Power Control Module;
- ESP – Electronic Stability Program;
- OBDII – On-Board Diagnostics slot;
- IPDM – Intelligent Power Distribution Module.

All systems of this type have vulnerabilities in hardware: an attacker only has to forge one or several commands to make one block fulfill a new task.

For example, if an attacker sends the network a command to open the door, he can forge an immobiliser message, which is normally issued when deactivating the regular security system. If the restart command to the immobiliser is made cyclical, i.e. converted into a constant reboot, the engine can be blocked.

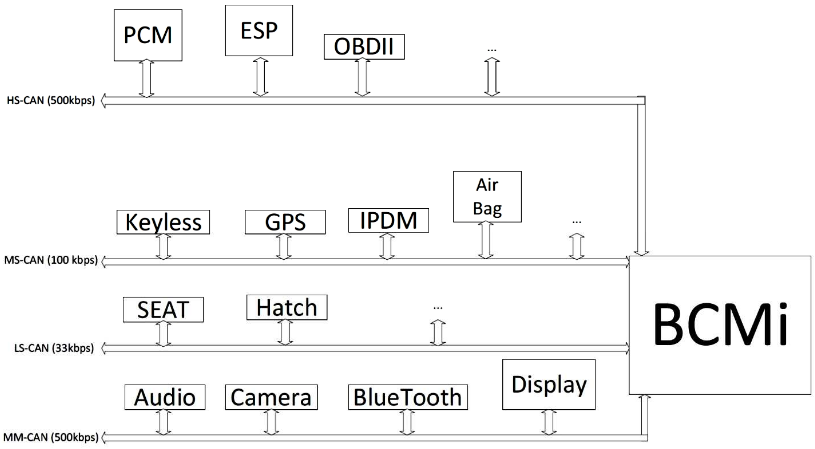

Figure 1: The System of a Vehicle Control

Furthermore, there are sets of service commands used by diagnostic equipment in troubleshooting and monitoring of the system. For example, an intruder could refer to anti-lock and anti-slip system block, put the engine into service mode and forcibly close the valves (this mode is used to replace the brake fluid). In this case, it will be impossible for a driver to depress the brake pedal.

In the same way it is possible to close one or more valves and enable the fluid pump at the same time. This act would result in the wheel steering uncontrollably. If driving at high speed, the vehicle would veer to one side.

More than that, it is possible to send commands to a medium-speed bus, triggering the shock sensor, which will activate one or more airbags. This list of examples can be very long.

A “bug” capable of intercepting driving was developed as an example of the attacks described above. This bug can be put in and powered from a standard diagnostic OBDII socket, or it can be hidden in any place with access to one of the buses and power. For example, minimising the size of the bug, it could put inside the motor wiring harness (Figure 2).

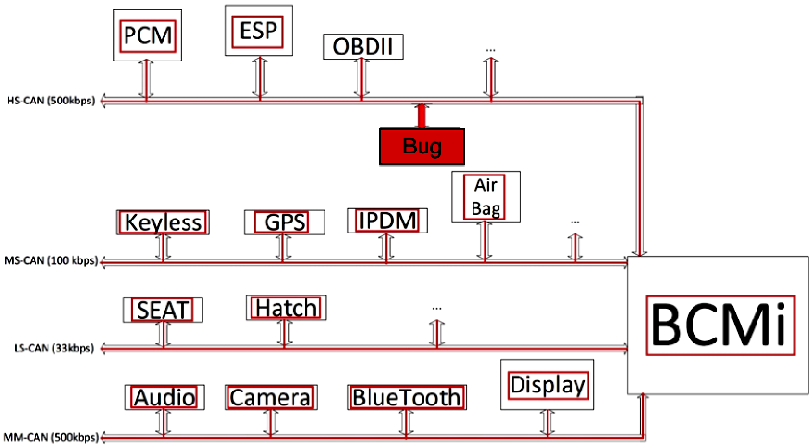

Figure 2: A Possible Bug Placement

Figure 2 shows that while connected to a single bus, you can gain control of all the others through the body control unit, which is the gateway for all buses. You can control the bug remotely with a mobile phone via Bluetooth, but it could also be equipped with any other communication module (3G, Wi-Fi, LTE, etc.).

Several solutions were proposed to protect the CAN from intrusion. For example, In-vehicle Intrusion Detection System by SeVeCom proposes monitoring of the vehicle’s system to detect possible attacks on CAN [28].

In [29] an introduction of anomaly detection systems to the automotive in-vehicle network is discussed. Based on properties of typical vehicular networks, like CAN, a set of anomaly detection sensors is proposed allowing recognition of attacks during vehicle operation without causing false positives.

However, these decisions provide only monitoring of unauthorized connection to CAN.

CAN Scanner is another equipment of ISO-11898 standard providing real time CAN-bus monitoring by an intelligent module – CAN USB-bridge. CAN Scanner software features allow to view in real-time any messages (all chosen from the list of specified range or group) passing through the CAN-network to identify their frequency, for any given connection speed. [30]

The disadvantage of CAN Scanner is that it requires manual settings and data input as well as PC presence where the software can be run.

Another device that can control a car CAN-bus is Automatic which is an auto accessory for car's onboard computer to upgrade the car's capabilities [31]. However, it works only in the USA and provides only general information about the car.

As we can see today there is no means to protect the car from the hardware vulnerabilities. Although existing software can provide a sort of protection from malware it cannot give a comprehensive CAN-bus security. Accordingly, a method and system for protecting a vehicle data transmission bus from intrusion attacks and bugs is desired. This system is described below.

3. SECURITY HARDWARE-SOFTWARE SYSTEM

A specially designed hardware-software complex (HSC) can be used to detect, control and block the bug in the onboard vehicle system. It is connected to the vehicle's CAN-buses and scans radio waves for possible data transmission to the bug (Figure 3).

This complex is a self-teaching CAN-system used to monitor and block harmful commands in the vehicle. Each vehicle (of each model, type and settings) has its own reference bus data (parameters), which is used to detect added modules and a harmful data sent over the vehicle CAN-bus. The harmful modules (bugs) can be attached to the CAN-bus or to a wire bundle.

There are two main options for detecting and protecting against unauthorised connection:

- monitoring of resistive and capacitive condition of buses;
- blocking commands, which introduce one or more blocks in the service mode.

Let us focus on each of the methods.

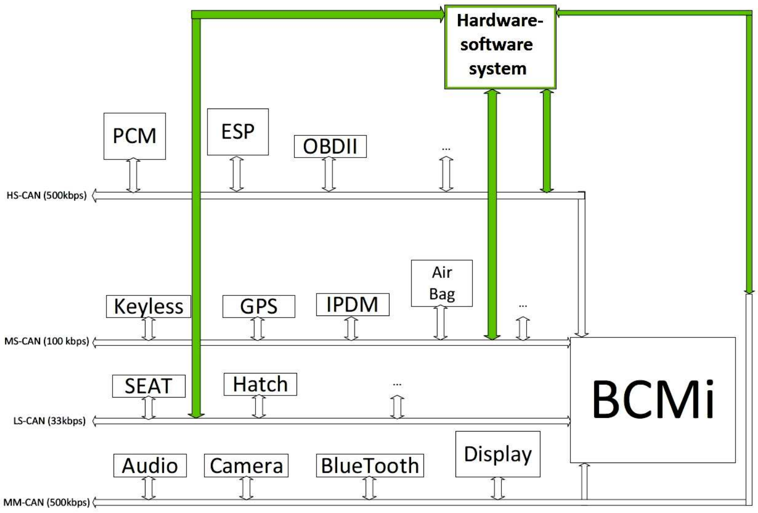

Figure 3: Integration of Software-Hardware Complex

3.1 Monitoring the Resistive and Capacitive Condition of Buses

This method is based on the fact that the connection of an additional device to the bus leads to resistance reduction and capacitance increase therein. A transceiver has to be introduced in the system for such monitoring. The layout of such a transceiver is shown in Figure 4.

The resistors (25 kOm each) are used for correlation of voltage levels CAN_H CAN_L and for noise resistance. The transistors with diodes are used for reaching a voltage level – in this case to 2.5V (0.5Vcc). The receiver is used for summing the signals CAN_H and CAN_L. The transistor assembly is used for signal level transformation of the TX Time-out Timer for waiting for transmission permission. The driver separates signals CAN_H and CAN_L (the voltage level on both buses is reached by the transistors).

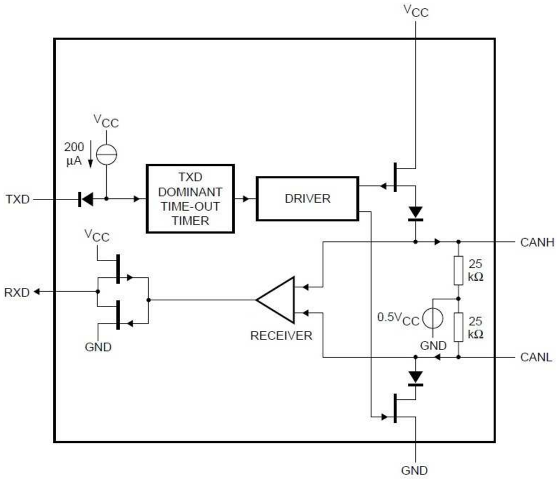

Figure 4: Transciever's Work Layout

The efficiency of this first method has been applied to the Nissan Teana J31 of 2006. The resistance (R_{total}) on the CAN- bus was measured and equaled 4.6 kOm. Each transceiver of the bus has a resistance R≈50 kOm (Figure 5).

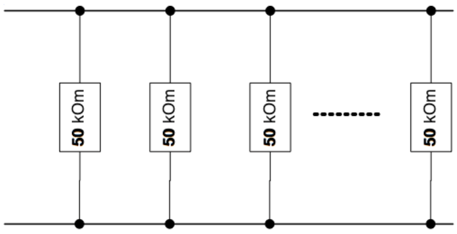

Figure 5: CAN-bus with Transceivers

Now we want to identify the number of devices connected to the bus:

R_{total} = R/N => N ≈ 10.8 ≈ 11 devices. The number meets the specification of the vehicle (see Figure 6) [32].

Next we connect a bug to the bus (R_1≈50 kOm) and measure the total resistance of the CAN-buses: R_{total1} = 4.3 kOm.

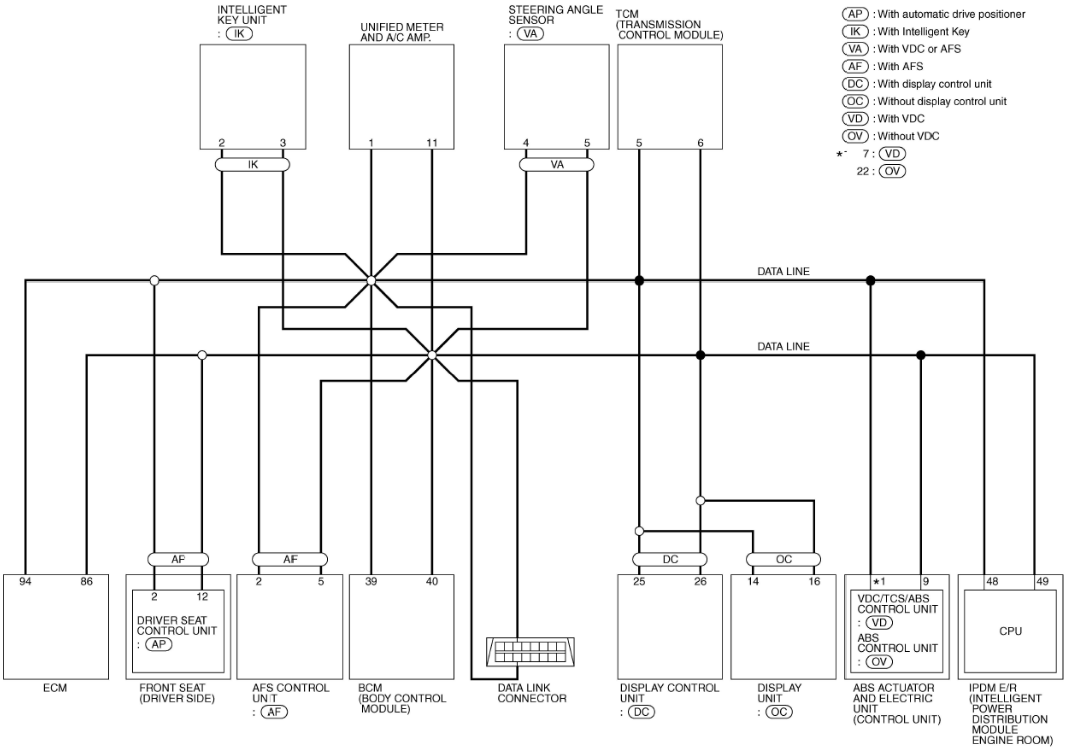
INTELLIGENT KEY UNIT : IK
UNIFIED METER AND A/C AMP.
STEERING ANGLE SENSOR : VA
TCM (TRANSMISSION CONTROL MODULE)
AP : With automatic drive positioner
IK : With Intelligent Key
VA : With VDC or AFS
AF : With AFS
DC : With display control unit
OC : Without display control unit
VD : With VDC
OV : Without VDC
★ 7 : VD
22 : OV
2 3
1 11
4 5
5 6
IK
VA
DATA LINE
DATA LINE
AF
AF
DC
OC
94 86
2 12
2 5
39 40
25 26
14 16
★1 9
48 49
ECM
DRIVER SEAT CONTROL UNIT : AP
FRONT SEAT (DRIVER SIDE)
AFS CONTROL UNIT : AF
BCM (BODY CONTROL MODULE)
DATA LINK CONNECTOR
DISPLAY CONTROL UNIT : DC
DISPLAY UNIT : OC
VDC/TCS/ABS CONTROL UNIT : VD
ABS CONTROL UNIT : OV
ABS ACTUATOR AND ELECTRIC UNIT (CONTROL UNIT)
CPU
IPDM E/R (INTELLIGENT POWER DISTRIBUTION MODULE ENGINE ROOM)

Figure 6: CAN-bus of the Nissan Teana J31

The connection scheme for the additional device to the CAN-bus is illustrated in Figure 7. Using the formula R_{total} 1 = R_1/N_1, we find out that the number of devices on the bus N_1 ≈ 11.7 ≈ 12. Consequently, there is an extra device connected to the bus.

Moreover, the transceiver has an internal CAN capacity of 10 picofarads (pF). As the total capacitance increases when a supplementary device is connected, this method enables the detection of an unauthorised device.

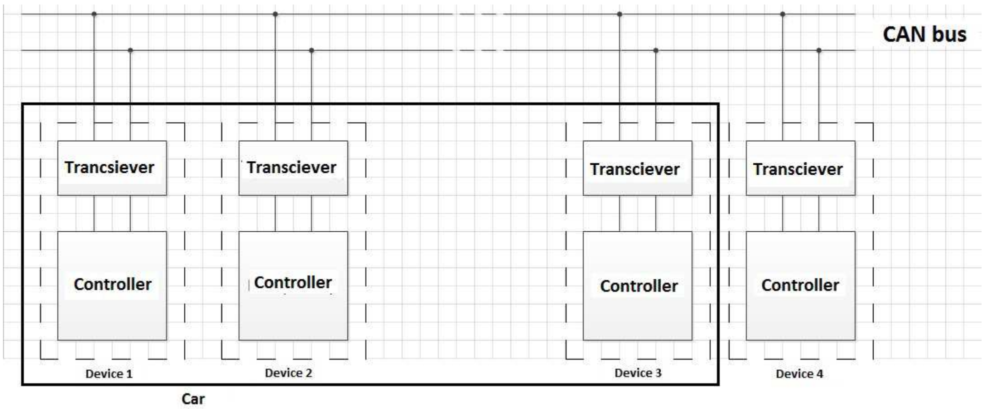

Figure 7: An Extra Device Connected to a CAN-Bus

3.2 Blocking Commands, which Introduce One or More Blocks in the Service Mode

If we make a radical change in the mode of the bus, we can block commands, which introduce one or more blocks in the bus service mode. Switching the mode of the bus from dominant to recessive prevents the sequence from completing the task (Figure 8).

As indicated in the diagram, by increasing the logic level on the bus you can get a completely different command. The new command does not allow you to add blocks in the service mode, and thus protects the car.

Here is a detailed explanation of the method. At first the system is checked for malicious sequences which consist of at least three commands. When two commands of such a type are detected, the second of them is deactivated. The next step is to check the blocks for the mode. If the blocks are in service mode, the mode is changed. The system then sets off an alarm reporting the attack.

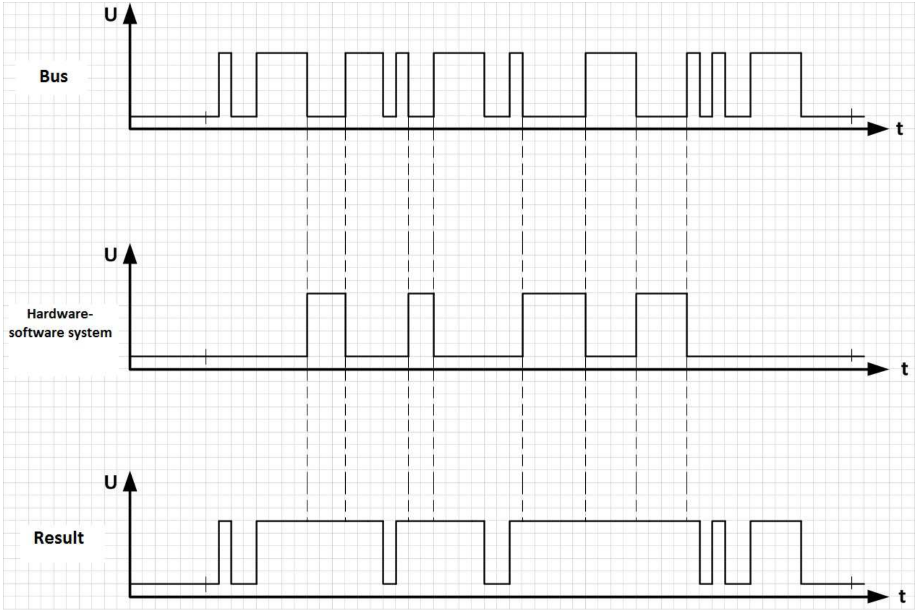

Figure 8: Protection from Malicious Logic

Resistive-capacitive features of the bus are checked and compared with their reference state for the vehicle. The system sends an attack alarm if any mismatches are detected.

Figure 9 illustrates an example of modification of the third input command into service mode of the ABS/ESP block of a Ford Mondeo MK4. The entire instruction for inputting a module into the service mode is:

02 00 08 35 FF 00 48 04 1A FC 43;
04 00 08 FF FA 0A 86 BC 31 FF F0;
02 F0 08 0F F1 62 CE FB 40 F0 FF.

The resulting (modified) sequence module

02 00 08 35 FF 00 48 04 1A FC 43;
04 00 08 FF FA 0A 86 BC 31 FF F0;
02 F0 08 FF FF 62 CE FB 7F FF FF

does not enter into the service mode. The sequence results in turning off the ESP, which is not critical and can be resolved by pressing a button on the driver's console.

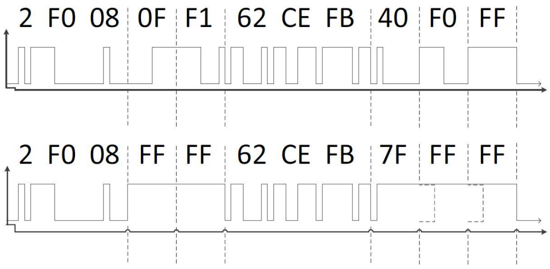
2 F0 08 0F F1 62 CE FB 40 F0 FF
2 F0 08 FF FF 62 CE FB 7F FF FF

Figure 9: Example of Modification of the Third Input Command Into Service Mode.

A detailed description of the proposed defence mechanism is as follows: first, a harmful sequence is detected, which consists of at least three commands. A typical harmful sequence has at least three commands. If two such commands are detected, the third one is deactivated. Note that the third command is blocked, because the first command is used in a normal service mode, but after two suspicious commands in a row the system knows that the third one needs to be blocked as malicious. As soon as the command identifier is detected on the bus, the system begins blocking the command. Then, module states are checked. If there are modules working in a service mode, they are exited from this mode. After that, the system prepares a report about the attack.

Resistive and capacitive bus characteristics are checked and compared with a standard state of the particular car. If any characteristics are off, the system reports the attack. The bus protection module reports the attack by (for example) making beeping sounds. Additionally, it can have an LED indicator displaying a green light under normal operations. If intrusion is detected, the bus protection module displays blinking red light and beeps. When the attack is blocked, the yellow light is displayed on the LED and the blinking red light indicating a presence of a bug. The bus protection module can store the details of the intrusion and provide them to a user if the user connects to a computer.

Then, a check is conducted to detect any external radio waves. If any, the first step is to analyse the source in order to exclude the irrelevant waves (mobile, Wi-Fi). If the waves of the malicious source are identified and confirmed, the system sends an alarm signal indicating that an attack has been detected. The algorithm of this defence mechanism is shown in Figure 10.

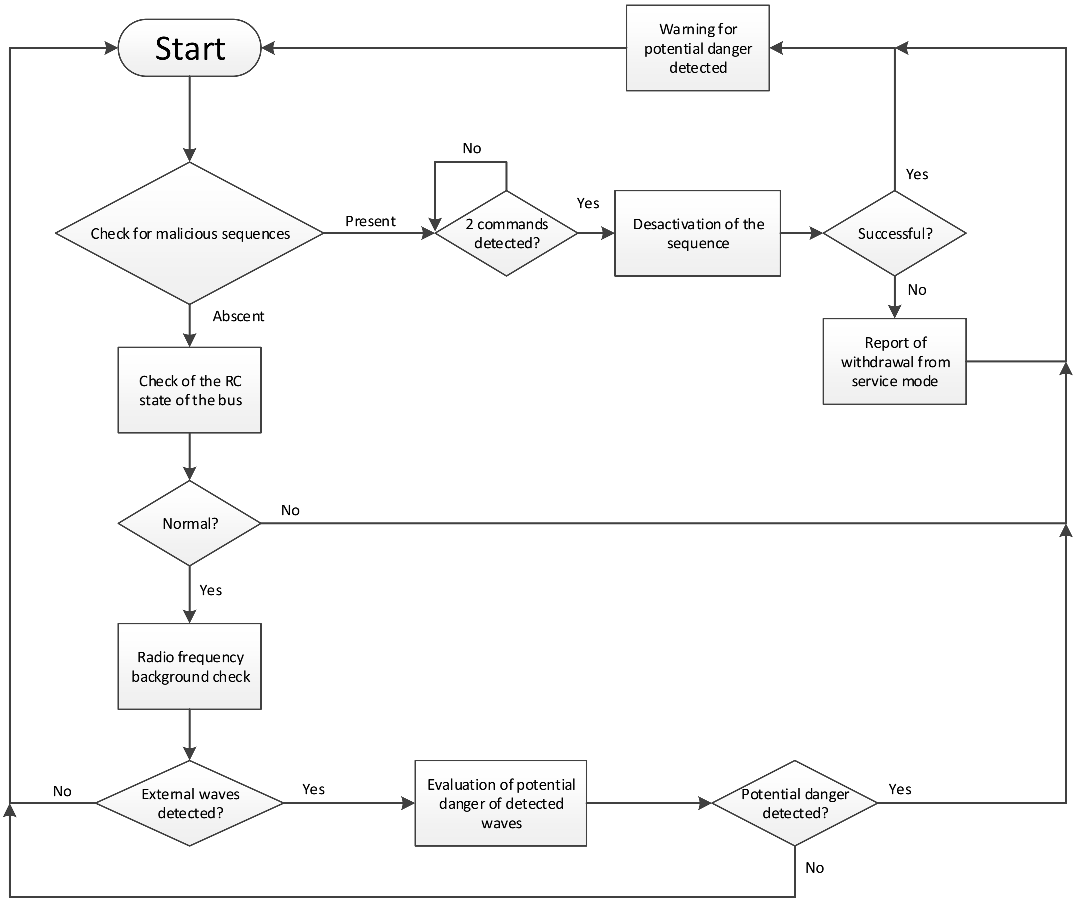
Start
Warning for potential danger detected
Check for malicious sequences
Present
No
2 commands detected?
Yes
Desactivation of the sequence
Successful?
Yes
No
Report of withdrawal from service mode
Abscent
Check of the RC state of the bus
Normal?
No
Yes
Radio frequency background check
External waves detected?
No
Yes
Evaluation of potential danger of detected waves
Potential danger detected?
Yes
No

Figure 10: Algorithm of the Defence Mechanism

4. CONCLUSION

The article describes the system and a potential vulnerability of a CAN-bus in a vehicle. Then, the paper provides an analysis of possible attacks that can be realised with the help of a bug in on-board electronics. The article gives an analysis of possible effects of the bug, as well as suggesting possible means of protection. There is also a detailed layout of protection algorithms.

While developing the hardware-software complex several tests were performed. An experiment, based on changes in the frequency of the standing wave, was conducted in order to detect malicious logic in hardware (Figure 11).

A frequency generator and an oscilloscope were set in the CAN-bus at a distance of 1.5 meters from each other. Then we measured the frequency of the standing wave on the bus with the bug and without it. You can see the results in Table 1.

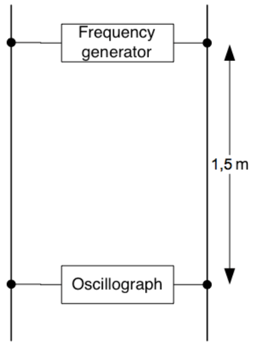

Figure 11: Measurement of a standing wave on a CAN-bus

Table 1: Measurement Results of a Standing Wave on a Can-Bus.

Without a bug	18.9 MHz	15.7 MHz	7.2 MHz
With a bug	18.9 MHz	16.1 MHz	7.2 MHz

As can be seen in Table 1, the measurement of the standing wave on CAN-bus does not provide any statistically significant results: out of three pairs of frequencies obtained only one has any difference in value.

The work is underway to improve the accuracy of the described hardware-software complex and diversify its functionality.

REFRENCES:

[1] Lei Jun; Luo Min; Chen Zhi Chu. Design and development of smart car DC motor speed control system. *31st Chinese Control Conference* (CCC), 2012, pp. 4916-4919.

[2] Ying You; Jian Hu; Gangyan Li. Primary models of passenger car information integrated control system. *IEEE International Conference on Automation and Logistics* (ICAL), 2010, pp. 618-623.

[3] Liu, X.Q., Yan, T.Y. Electronic control unit design of electronically controlled air suspension (ECAS) for vehicle based on Freescale microcontroller. *2013 International Symposium on Vehicle, Mechanical, and Electrical Engineering*, ISVMEE 2013; Taiwan; China. Volume 494-495, 2014, Pages 242-245.

[4] Xu, Y., Zhang, Z., Huang, Z.Y. Vehicle embedded speech recognition and control system research and implementation. *International Symposium on Vehicle, Mechanical, and Electrical Engineering, ISVMEE 2013*; Taiwan; China. Volume 494-495, 2014, Pages 104-107.

[5] Jian Hu; Gangyan Li; Duanfeng Chu; Jun Xu. Research on passenger car windscreen wiper controller and control method based on CAN. *International Conference on Mechatronics and Automation*, 2009. ICMA 2009, pp. 4901-4906.

[6] Dai Qiang Wang, Shi-you Gao, Yu Qing Chen, Yi Wang, Qiao Liu. Intelligent Control system based on CAN-bus for car doors and windows. *3rd International Conference on Anti-counterfeiting, Security, and Identification in Communication*, 2009. ASID 2009, pp. 242-245.

[7] Wang Yong-ding, Nie Li-na. Design of Smart Car Speed Control System Based on Fuzzy Control. *International Conference on Artificial Intelligence and Computational Intelligence* (AICI), 2010 (Volume: 2), pp. 516-519.

[8] Darabi, Z.; Ferdowsi, M. An Event-Based Simulation Framework to Examine the Response of Power Grid to the Charging Demand of Plug-In Hybrid Electric Vehicles. *IEEE Transactions on Industrial Informatics*, (Volume: 10, Issue: 1), Feb. 2014. Pages: 313 – 322.

[9] Jian Hu, Gangyan Li. CAN-based passenger car starter information integrated control method and its implementation. *IEEE International Symposium on Industrial Electronics*, 2009. ISIE 2009, pp. 1203-1208.

[10] Studnia, I.; Nicomette, V.; Alata, E.; Deswarte, Y.; Kaaniche, M.; Laarouchi, Y. Survey on security threats and protection mechanisms in embedded automotive networks. *43rd Annual IEEE/IFIP Conference on Dependable Systems and Networks Workshop* (DSN-W), 2013, pp. 1-12.

[11] Vijay, E.V., Rao, C.V.R., Kumar, E.V., Swamy, G.N. Electronic control unit for an adaptive cruise control system & engine management system in a vehicle using electronic fuel injection. *International Conference on Emerging Trends in Robotics and Communication Technologies* (INTERACT), 2010. pp. 143-146.

[12] Miucic, R., Mahmud, S.M. Wireless Reprogramming of Vehicle Electronic Control Units. *5th IEEE Consumer Communications and Networking Conference*, 2008. CCNC 2008, pp. 754-755.

[13] Klausner, M., Dietrich, A., Hathout, J. P., Springer, A., Seubert, B., Stumpp, P. Vehicle data management system with remote access to electronic control unit-internal states. *International Conference on Advanced Driver Assistance Systems*, 2001. ADAS. (IEE Conf. Publ. No. 483), pp. 68-72.

[14] Wang Tianxu, Gong Mingde. Design electronic control unit of blend brake system for heavy vehicle. *International Conference on Electronic and Mechanical Engineering and Information Technology* (EMEIT), 2011 (Volume: 4), pp. 1791-1794.

[15] Novak, J., Kocourek, P. Automated Testing of Electronic Control Units Compatibility in Vehicle CAN Networks. *Proceedings of the IEEE International Symposium on Industrial Electronics*, 2005. ISIE 2005. (Volume: 4), pp. 1423-1428.

[16] *SAE J1939 Standards*. SAE International, 2012-06-01. URL: http://standards.sae.org/j1939_201206/.

[17] *Data exchange via CAN I bus*. The basics. Self-tuition program 238. LLC "Volkswagen Group Rus," as of 10/01. URL:

http://www.autodela.ru/assets/files/books/VW/238_Shina_dannih_%20CAN%20I.pdf.

[18] Kammerer, R., Fromel, B., Wasicek, A. Enhancing security in CAN systems using a star coupling router. *7th IEEE International Symposium on Industrial Embedded Systems* (SIES), 2012, pp. 237-246.

[19] Groza, B.; Murvay, S. Efficient Protocols for Secure Broadcast in Controller Area Networks. *IEEE Transactions on Industrial Informatics*, (Volume: 9, Issue: 4), Nov. 2013. Pages: 2034 – 2042.

[20] Chung-Wei Lin, Sangiovanni-Vincentelli, A. Cyber-Security for the Controller Area Network (CAN) Communication Protocol. *International Conference on Cyber Security* (CyberSecurity), 2012. Pages: 1 – 7.

[21] Chung-Wei Lin; Qi Zhu; Phung, C.; Sangiovanni-Vincentelli, A. Security-aware mapping for CAN-based real-time distributed automotive systems. *IEEE/ACM International Conference on Computer-Aided Design* (ICCAD), 2013. Pages: 115 – 121.

[22] Dennis K. Nilsson, Phu H. Phung, and Ulf E. Larson. Vehicle ECU Classification Based on Safety-Security Characteristics. *In Proceedings of Road Transport Information and Control – RTIC 2008 and ITS United Kingdom Members' Conference*, IET, May 20-22, 2008, Manchester, UK.

[23] P. Kleberger, T. Olovsson, E. Jonsson. Security aspects of the in-vehicle network in the connected car. *IEEE Intelligent Vehicles Symposium* (IV), 2011, pp. 528-533.

[24] Tobias Hoppe, Stefan Kiltz, Jana Dittmann. 'Security Threats to Automotive CAN Networks – Practical Examples and Selected Short-Term Countermeasures. Computer Safety, Reliability, and Security Lecture Notes', *Computer Science*, Volume 5219, 2008, pp. 235-248.

[25] Dennis K. Nilsson and Ulf E. Larson. Simulated Attacks on CAN Buses: Vehicle virus. *Proceedings of the Fifth IASTED Asian Conference on Communication Systems and Networks* (ASIACSN), 2008.

[26] D. K. Nilsson and U. E. Larson. Combining Physical and Digital Evidence in Vehicle Environments. Proceedings of the Third International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE). *IEEE Computer Society*, 2008, pp. 10-14.

[27] D. K. Nilsson, U. E. Larson, F. Picasso, and E. Jonsson. A First Simulation of Attacks in the Automotive Network Communications Protocol FlexRay. *Proceedings of the First International Workshop on Computational Intelligence in Security for Information Systems* (CISIS). Springer, 2008, pp. 84-91.

[28] Daimler AG, Albert Held, Michael Müter. In-vehicle Intrusion Detection System. SeVeCom, 17 October 2007. URL: http://www.sevecom.org/Presentations/2007-10_Berlin/Sevecom_2007-10-17_J%20IntrusionDetection.pdf.

[29] Muter, M.; Groll, A.; Freiling, F.C. A structured approach to anomaly detection for in-vehicle networks. *Sixth International Conference on Information Assurance and Security* (IAS), 2010. Pages: 92 – 98.

[30] Chelishev Sergey. *CAN Scanner*. 2013. URL: http://canscanner.com/download/Kratkoe_opisanie_CANScanner.pdf.

[31] *What is Automatic?* Automatic Labs, Inc. September, 2014. URL: https://www.automatic.com/?utm_source=dashboard%20CTA&utm_medium=button&utm_campaign=dashboard%20demo%20CTA%20.

[32] *CAN-bus of a Nissan Teana J31*, Specification. URL: https://docs.google.com/file/d/0B07nPSMlhMHwcG9XdnNWbEtrTDQ/edit?usp=sharing&pli=1.