 https://doi.org/10.3311/PPtr.13785

Periodica Polytechnica Transportation Engineering, 49(1), pp. 80–88, 2021

Novel Approaches to Evaluate the Ability of Vehicles for Secured Transportation

Bence Kocsis[1], Gábor Vida[1*], Zsolt Szalay[1], György Ágoston[2]

[1] Department of Automotive Technologies, Faculty of Transportation Engineering and Vehicle Engineering, Budapest University of Technology and Economics, H-1521 Budapest, P. O. B. 91, Hungary
[2] Department of Software Development and Application, Institute of Informatics, University of Dunaújváros, H-2401 Dunaújváros, P. O. B. 152, Hungary
[*] Corresponding author, e-mail: gabor.vida@gjt.bme.hu

Received: 24 January 2019, Accepted: 18 March 2019, Published online: 24 October 2019

Abstract

The assurance of process safety plays an important role in the field of information technology. Securing the information has become one of the biggest challenges in the present day. Whenever we think about the protected systems the first thing that comes to our mind can be malicious interventions which are increasing immensely day by day. Nowadays we live the world of huge automotive developments with the appearance of the demand for autonomous vehicles. On the other hand, technological developments also provide a lot of advantages for the society. The benefits of autonomous cars include reduced mobility costs, increased safety, increased mobility, significant reduction of traffic collisions. However, it cannot be forgotten that the extension of cyberspace affects the transportation increasingly. Accordingly, cars are produced with high level of connectivity and automation. Therefore, the risks arriving from the cyberspace can now endanger the safe and secured transportation. These tendencies shall motivate manufacturers and developers to permanently improve the ability of vehicles to protect themselves and their passengers.

Keywords

penetration test, protection ability, wireless channels

1 Introduction

Nowadays, the world can be characterized by a significant development process in the field of automotive industry in which the demand for autonomous transportation systems plays a crucial role (Tettamanti et al., 2016). The benefits of autonomous cars include reduced mobility costs, increased safety, increased mobility, significant reduction of traffic collisions (Zöldy, 2018). It is strongly expected, that autonomous transportation will provide more efficient mobility patterns, especially considering road transportation of goods and passengers.

Autonomous cars combine a lot of technology solutions in order to perform the autonomous driving (Checkoway et al., 2011). This includes the precise detection of the vehicle's position on the map (Szíjj et al., 2015), and also the precise detection of the objects which surround the car. To be able to perform this, cars use wide variety of sensors (radar sensors, LIDAR sensors, ultrasonic sensors, computer vision). These sensors provide a huge amount of data, and it is not a trivial task to process these data. In order to fulfil the functional requirements, we need to have better and better ECUs in the car.

It is only one side of the problem to perform the calculations in suitable time. It is also an important task to comply with the safety requirements, since now the ECUs will control the car, and a failure would risk the life of the passengers. Since the number of connected devices increases permanently, the task of connecting vehicles in the big system is even more difficult than before .... With other words, it is already obvious for people that everything is connected and synchronized, so they also want their cars to be connected. Of course this results in a huge amount of advantages, for example the possibility of communicating with the road side objects and other cars to gather data about other vehicle's positions and movement, traffic and road conditions (v2x communication), it is easier to apply software updates, and there can be applications which may give information to the car owner even if he is outside the car. However, on the other hand, the car's connection channels with the outside

Cite this article as: Kocsis, B., Vida, G., Szalay, Zs., Ágoston, Gy. (2021) "Novel Approaches to Evaluate the Ability of Vehicles for Secured Transportation", Periodica Polytechnica Transportation Engineering, 49(1), pp. 80–88. https://doi.org/10.3311/PPtr.13785

world can also cause vulnerabilities for malicious interventions Therefore nowadays it is one of the most important topics to protect vehicles from cyberattacks.

In the IT world there are already a lot of established process which can support the identification and exploitation of system vulnerabilities. In case of cars, considering the embedded characteristic of the systems, the methodologies may be slightly different.

The scope of this paper is to investigate the main concepts applied to break the vehicular security system, and to identify the applicable techniques in detecting and preventing attacks by developing a novel ranking system focusing on the security level of the analyzed framework.

2 Literature review

Modern cars are controlled by complex distributed computer systems comprising millions of lines of code executed on a lot of different microcontrollers, which are connected to several networks inside the vehicle. This structure offers a huge amount of advantages on the field of safety and cost efficiency, however it also creates some vulnerabilities which can be exploited by attackers. In the next section the most relevant attack methods a classified (Checkoway et al., 2011).

2.1 Indirect physical access attacks

In modern vehicles there are several physical interfaces which access the vehicle's internal networks either directly or indirectly. The most significant (and well known) automotive interface is the OBD-II port, which usually gives direct access to the vehicle's internal CAN bus (Controller Area Network) and provides access to several automotive systems. In most cases the OBD-II port is used by service personnel during car maintenance to read out the error code, which helps the diagnostics, and it is also possible to program the ECUs through the OBD-II port, for example in case of a software update (Szíjj et al., 2015). Historically during these analysis processes dedicated "scan" tools were used, but nowadays the approach is rather PC centric. This means that the mechanic uses a laptop computer as a "PassThru" device, which is connected to the car's ODB-II port via USB or WiFi. After the connection is initiated, the software on the laptop computer enables either to read out information from the ECUs of the car, or to program them. Summing up, an operation system based computer (mostly windows based) controls the data which is sent to the vehicle. Such laptops are typically internet connected, so it is possible to hack these laptops with "traditional" methods from the IT world. It is easy to imagine, if a laptop in a garage is infected, and it is used with several vehicles, it can apply malicious software to several cars. It makes the situation worse, that nowadays, in the world of internet, also incompetent persons try to connect to the OBD-II port at home, which can be easily managed without having an idea how dangerous the situation is. Furthermore, electric vehicles may also communicate with external chargers via the charging cable. If an attacker is able to compromise the external charging infrastructure, it can affect any vehicles which are using that charging network.

The other important groups of physical interfaces belong to the entertainment systems. All cars are shipped today with a CD player which is able to handle several audio formats. Similarly, the manufacturers also provide other type of external media ports (typically USB port or phone docking port), which allow the car owner to connect a mobile phone, and control the car's media system with it. It is a risk that an attacker can somehow deliver malicious programs by encoding it to a CD or a song file (for example using social engineering), or can hack the car owner's phone and install a software on it which attacks the car's media system. Of course a CD player can have limited effect on the driver (it is a good question how limited it, if the music starts with full volume after silence on a congested motorway section), but these media systems are not standalone devices. They are usually connected to an internal network, so a compromised CD player can offer an opportunity to attack automotive components.

2.2 Short-range wireless access attacks

The main difference of short-range wireless access compared to the indirect physical access is that the access criteria against the attacker are less strict. It is assumed, that an attack surface (Miller and Valasek, 2014; SAE, 2016) is left unprotected on the car, which is operating over short ranges. These include Bluetooth, Remote Keyless Entry, RFIDs, Tire Pressure Monitoring Systems, WiFi, and Dedicated Short-Range Communications (DSRC). It is also assumed, that the attacker has a short range wireless transmitter within the car's operation range (between 5 m and 300 m, depending on channel).

Compared to indirect physical access, here the operational requirements are weakened related to the attacker and the attack path is considered to be operated over short range. These include Bluetooth, Remote Keyless Entry, RFIDs, Tire Pressure Monitoring Systems, WiFi, and Dedicated Short-Range Communications (DSRC). In case

of this attack type it is assumed that the perpetrator is able to place a wireless transmitter close to the car's receiver (between 5 and 300 meters depending on the applied communication channel (Checkoway et al., 2011)).

Bluetooth has become a standard communication channel in case of supporting hands-free phone-conversation in automobiles and is a standard technology in most of the vehicles. The lowest level of the Bluetooth protocol is typically implemented on a hardware level, but the higher level protocols (management, services) are already implemented on a software level. Normally Class 2 Bluetooth devices are used for automotive applications, which enable a range of 10 meters, but there are demonstrations which show that this range can be extended with amplifiers and antennas (Checkoway et al., 2011). To attack the Bluetooth interface, a paired Bluetooth device is required. It might cause some problems for the attacker to establish a Bluetooth connection, but these devices are designed to handle multiple paired devices. When the attacker has a paired connection, with analyzing and reverse engineering it is possible to find the weaknesses of the software (for example unsafe usage of memory allocation or copy functions).

2.3 Long range wireless attacks

Last but not least, vehicles also provide the possibility to establish long distance (greater than 1 km) digital connection. These channels can be classified in two groups: broadcast channels and addressable channels.

In case of broadcast channels, the messages are not specifically sent to a given vehicle. Additionally, long-range broadcast mediums can also be used as control channels (for example in case of a malicious intervention), because in their cases the it is even more difficult to identify the perpetrator, through these channels multiple receivers can be commanded at once, and they do not make it necessary for attackers to know the precise parameters of the car. The modern automobile can include many broadcast receivers for long-range signals: Global Positioning System (GPS) (Kis and Lantos, 2013), Satellite Radio, Digital Radio, Radio Data System (RDS) and Traffic Message Channel (TMC) where signals are transmitted as digital subcarriers on existing FM-bands (Farkas and Telek, 2018).

In case of addressable channels, the most important part is the continuous availability of the attack surface owing to the telematics systems which provide continuous connectivity via cellular voice and data networks. These systems offer several useful features for the car owner, for example supporting safety (crash reporting), diagnostics (early alert of mechanical issues), anti-theft (remote track and disable), and convenience (hands-free data access such as driving directions or weather) (Checkoway et al., 2011), but also offer advantages for attackers: they can be accessed over arbitrary distance (due to the wide coverage of cellular data infrastructure) in an environment reasonably supporting the anonymity of the malicious intervention. These channels typically have relatively high bandwidth, are two-way channels (supporting interactive control and data exfiltration), and are individually addressable (Checkoway et al., 2011).

2.4 Automotive communication systems

We have seen that there are several opportunities to gain access to the vehicle's internal communication channels. Now let's investigate, how we can exploit that access. In the following session CAN and on Automotive Ethernet is discussed.

2.4.1 CAN attacks

Once the attacker gained access to the CAN bus, there are multiple possibilities to continue with. In order to understand these possibilities, it is required to have a little understanding of CAN communication. CAN is a broadcasted protocol with maximum 8 bytes of data. At the beginning of each message there is an 11-bit long identifier. Typically, ECUs will broadcast messages and other ECUs that are interested (decided by CAN ID) will listen for those messages and ignore the rest. However, the CAN ID does not only identify a message, but also define its priority (CAN arbitration). Based on these basic rules, we can easily imagine different attack scenarios.

2.4.2 Spoofed messages

In this kind of attack, the attacker tries to send a spoofed message simulating that it is valid message, generated by a real, existing ECU. The attacker uses a fake node ID which is not assigned in the CAN message. Attacker has a high chance to inject 8 bytes long spoofed messages without the risk of detecting the intrusion. If the attacker changes a single bit in the message, then the probability of being detected increases to 0.39 % (Checkoway et al., 2011).

2.4.3 Replay attacks

In a replay attack, an attacker sniffs the CAN message and captures the data from the sniffed dump. After doing this, the attacker replays the message after some amount of time. The attacker can also send duplicated messages in the CAN network. As CAN does not support authentication of

the message, receiver ECU cannot identify the data in the message and performs the function which is in the CAN packet. For instance, an attacker changes the data in the CAN packet if he wants to attack the brakes of a vehicle. He would send the false packet once on the network which will launch the attack on the vehicle. But if he keeps on sending the packet continuously, the brakes would stop functioning (Checkoway et al., 2011).

2.4.4 Message injection

We can distinguish three types of message injection. First type, if an attacker wants to target a single function of a vehicle (e.g., access to doors), then he would send a message with single CAN ID to the CAN bus. Sending repeated messages will operate the vehicle according to the injected message. Second, if an attacker wants to attack a system as a whole rather than a single part of the vehicle, he would use multiple random CAN IDs. For example, if an attacker wants to stop a vehicle, he would attack on the brakes of the vehicle then kill the engine. This would force the user of the vehicle to stop the vehicle. Third, the attacker may circulate a huge amount of CAN messages which can disrupt the normal functioning and communication of CAN bus. As the capacity of CAN bus is 1 Mbps, attacker can create huge traffic on the bus. CAN bus would not be able to handle such a huge traffic and would fail to function in an appropriate manner. Quantitatively, each CAN message consists of 128 bits and three inter-frame spaces which are of 1 bit between messages. Hence, the attacker can launch a Denial-of-Service (DoS) attack by generating 8000 messages per second (Pan et al., 2017).

2.4.5 Automotive Ethernet attacks

With the demand for higher bandwidth Automotive Ethernet is getting more and more popular nowadays. It offers a huge amount of advantages in the field of infotainment system and autonomous functions, but it also means a dangerous attack channel. On the one hand, since the Automotive Ethernet is based on the regular Ethernet protocol, there are tons of possible attack methods, which can be applied. On the other hand, there are automotive protocols, which are relatively fresh, therefore they can contain vulnerabilities which are not yet known. Previous researches have already investigated the protocols of Automotive Ethernet (Talic, 2017) form security point of view. According to the results, it is possible to inject messages which enable the attacker to classify himself as a proper participant of the communication, disturb data exchange and the flow of the communication.

3 Detection of penetration

The main goal is to detect messages on the network which are sent by the attacker. In order to achieve this, we need an intrusion detection system. After the attack begun, the intrusion detection system either can raise a warning in the direction of the driver, if necessary, or can just simply filter the corrupted messages.

3.1 Intrusion detection on CAN bus

Pan et al. (2017) suggest different approaches for intrusion detection on the CAN bus. One of them is an algorithmic approach. This method can grant protection against the denial of service type of attacks. A monitoring system is set up on the network, which identifies the repetition in the messages, and increases the belonging counters. If the counters reach a pre-defined threshold, an alarm is triggered, which indicates the intrusion process.

Another detection method is the DMS (data management system (Miller and Valasek, 2014)). In this case the CAN messages are sent through an observer to identify malicious events on the network. There are three main different approaches to apply DMS: centralized, distributed, hybrid. In the centralized solution, all traffic pass through the central DMS. It improves the maintainability, but has the disadvantage that if the central point gets compromised, all data on the network will be threatened. In the distributed solution, multiple ECUs handle the data monitoring, which gives a solution to the disadvantage of centralized model, however it increases the traffic on the network which may result in bottleneck or crucial capacity allocation problems. The third approach is a hybrid solution, which mixes the centralized and distributed approach, keeping their advantages.

The last detection possibility is a security based solution (Pan et al., 2017). The heart of this method is an algorithm, which uses encryption and authentication of the nodes during the system start-up period. An ECU is assigned as master ECU, which consists of a key and a serial number. When the vehicle is started, specific processes come off between the master ECU and all the other ECUs on the network. The master ECU generates two randomly generated numbers, and gives them to all other ECUs. The other ECUs perform some functions using these two numbers, and send back the results to the master ECU. If the value is matched with the stored expected value, then the ECU is valid. This would detect any malicious node on the network.

As a summary, it can be stated that if the intrusion is aimed to be defined based on the communication, a method

similar to the firewall concept is necessary. This firewall should be placed between the external access interface and the network itself. On the one hand the task of this firewall is to filter out messages coming from the cyber space, which would eliminate many malicious attacks at relatively low cost; on the other hand the firewall should act as filter. Before the packet is sent to the network, it should go through the firewall. There the packet can be compared to the packets stored in the database, can be compared to previously sent packets, statistics and other measurements can be made, which can be useful to decide whether the system is under attack or not. Besides the firewall, encryption methods can also be used to make the attack harder.

Although, it has been introduced that the detection approaches can be centralized, distributed and hybrid, there is only one layer, the firewall between the network and the attacker. If this is broken, the attacker has full access to the network. To address this disadvantage, a good solution is the HSS (Hybrid Security System (Rizvi et al., 2017)), which consists of multiple protection layers. HSS consists of three layers, a layer similar to firewall, and the HSP (hybrid security program) layer, which communicates with the HSS resource layer. When a packet passes through the firewall, it decides if the packet is trusted or untrusted. If it is trusted, the firewall allows the packet to pass through. If it is untrusted, the firewall blocks the packet. In addition, a flag is generated in the firewall independent HSS system. There is two type of flags: yellow flag and black flag. If a packet tries to pass through, after predefined amount of occasions a yellow flag is generated. After the flag handler receives enough yellow flags, a black flag is generated, which generates a filtering rule update and sends it to all ECUs firewall.

4 Classification of security levels

The SAE refers to two security classification methods, which provide engineering process suggestions aligned to ISO 26262 (Martin et al., 2017; Salay et al., 2018) standard: HEAVENS (HEAling Vulnerabilities to ENhance Software security and safety) and EVITA (E-Safety Vehicle Intrusion Protected Applications) (Cheah et al., 2018). Now I will describe the EVITA method and define additional improvement suggestion in regard to its methodology.

The classification method consists of three steps. The first step is the threat modelling. This is the most critical step, because this will be the base of the following processes. This is a manual process based on expert knowledge. The best way to model the threats is an attack tree. Attack trees are diagrams, which represent the actions that are required to achieve the goal. The attacks tree has events, and between events there are logical connection (and, or, etc.). The outcome of the attack trees serves as a starting point for the next step, the penetration testing. However, this outcome could be used also as a starting point of other safety methods (Ghadi et al., 2019; Gopalakrishnan et al., 2018), like FMEA (Failure Mode and Effect Analysis) (Hajiagha et al., 2016). In order to achieve this, the attack potential number has to be introduced to every step in the attack tree, which can be important from security point of view. This number should be generated based on three properties: the difficulty to achieve the attack, the probability, that someone is able to implement the attack, and the reliability of the detection method which could identify the attack. Table 1 shows the generation process of the introduced parameter.

As we can see, the attack difficulties have an incremental scale beginning from the basic complexity to nearly impossibly difficult attacks. These values can be interpreted based on the amount of the effort being required to execute and implement the given attack. Therefore, the easier to execute an attack the higher its potential is. The situation is the same with the probability, the higher the probability the higher its potential is. Now if the sum the two values is calculated, the result is between 2 and 8. In this framework the detection method cab be represented as a multiplier. In this case the more advanced the detection method is, the lower the multiplier is. As a result, no an attack potential value can be generated between 2 and 10. With this approach, it is possible to describe, compare and consider

Table 1 Attack potential calculation

Attack difficulty	
Basic	4
Advanced	3
Hard	2
Nearly impossible	1
Attack probability	
Likely	4
Possible	3
Unlikely	2
Very unlikely	1
Detection methods	
No detection	1.25
Central detection	1.2
Distributed detection	1.1
Hybrid detection	1

different attack types during the design period of in-vehicle automotive communication networks.

The next step is the penetration testing. The penetration testing is a specific analysis method focusing on the security characteristic of the vehicle. The goal is to collect the vulnerabilities and try to exploit them. Regarding penetration testing, methods can be classified into two groups. Let's call the first group to automated penetration tests. The tests of this group check a huge number of parameters, which can strongly affect vulnerabilities (for example brute force scanning of ports). The other group should contain the expert analyses, which are based on the results of the tests in the first group on the one hand, and on the other hand they are based on technical experiences and creative ideas. The outcome of the penetration test is a report, which can be used as a starting point for the classification.

The last part of the investigation is the classification procedure, which is based on Table 2 in case of EVITA.

Besides that, the attack potential calculated based on Table 1 gives a starting point for EVITA classification. Furthermore it also can be used to extend the FMEA procedure, which is developed to explore failure possibilities and their effects. Its goal is to identify and localize failure possibilities and support their prevention. During the FMEA process, a number, between 1 and 10, should be matched to each property group of each failure. These groups are the possibility of occurrence (O), the severity of the failure from the user point of view (S), and the ability for detection (D). As a result, three indicator numbers between 1 and 10 are defined, therefore if they are multiplied by each other, the risk priority number (RPM) can be generated, with a value between 1 and 1000. Based on SAE recommended practice (SAE, 2016), if the RPM is below 125, no action is required, if the RPM is between 125 and 420, further analysis is required, and if the RPM is over 420, intervention is required. Since attack potential number has been defined with a value between 2 and 10, it provides a great opportunity to integrate it into the FMEA. If our previous indicator numbers are multiplied by the attack potential (A), the following result can be achieved: RPM = O * S * D * A, which means a number between 2 and 10000. Based on the previous classification, introduce new thresholds can be introduced: if the RPM is under 1000, no further action is required, if the RPM is between 1000 and 3360, further analysis is required, and if the RPM is over 3360, intervention is required.

5 Examples

In this paragraph some examples are given, how an attack tree can be created discussed in the previous section, and the calculation method related to the attack potential is introduced.

On Fig. 1 there is the textual attack tree of this given scenario: there is an ECU in a car, which communicates over the air with TCP/IP based protocols. The communication is not encrypted, but the ECU is not connected to safety critical systems, and the attacker has full access to the network. The goal of the attack has to be defined, and now the goal is data mining. The SAND keyword stands for sequential logical and, which means we execute the given steps after each other. The AND and OR keywords stand for logical and and logical or. As we can see, the attack process begins with reconnaissance. This means that the attacker tries to get as much information about the system as he can. This includes processing the properties of the messages present on the network, trying to figure out parameters and properties with different kind of

Table 2 EVITA classification

Class	Safety	Privacy	Financial	Operational
0	No injuries.	No unauthorized access to data.	No financial loss.	No impact on operational performance
1	Light / moderate injuries.	Anonymous data only.	Low-level financial loss	Operational impact not discernible to driver.
2	Severe and life-threatening injuries (survival probable) or light/moderate injuries for multiple vehicles.	Identification of vehicle or driver.	Moderate financial loss, or low losses for multiple vehicles.	Driver aware of performance degradation, or indiscernible operational impacts for multiple vehicles.
3	Life threatening (survival uncertain) or fatal injuries, or severe injuries for multiple vehicles.	Driver or vehicle tracking, or identification of driver or vehicle for multiple vehicles.	Heavy financial loss, or moderate losses for multiple vehicles.	Significant impact on operational performance, or noticeable operational impact for multiple vehicles.
4	Life threatening or fatal injuries for multiple vehicles.	Driver or vehicle tracking for multiple vehicles.	Heavy financial losses for multiple vehicles.	Significant operational impact for multiple vehicles.

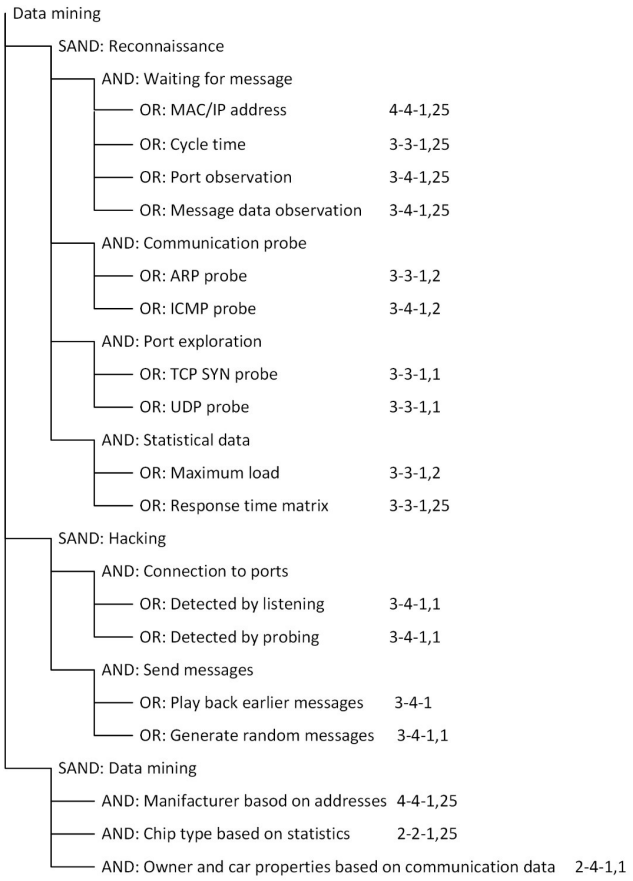

Fig. 1 Data mining attack tree

probes, and gathering statistical data. Besides the description of the steps there are the indicator numbers based on Table 1. As it can be seen, waiting for messages and gather the MAC and IP addresses has a high attack potential, because it is a basic and attack with a relatively high probability, without any detection mechanism. The TCP SYN probe (Vetrella et al., 2019) has already lower values, because it is a more difficult attack with some detection methods built in, but it still gives a relatively high attack potential (6,6); which already can be a heavy multiplier in the further analysis (previous section). After the hacker gathered enough information, the hacking process can be started. This includes connection to ports, and sending messages (in multiple communication layers). As a last step, the answer messages on the network have to be evaluated, and then datamining process can be performed.

Fig. 2 shows the attack tree of a message injection attack represented in a diagrammatic form (Wang et al., 2018). According to the assumed scenario the hacker is able to infect a third party hardware which is connected to the car's OBD II port, therefore he has a chance to create malfunction on the CAN network. Following the attack tree, after the connection the hacker is able to detect and record messages, and also generate messages. After the detection phase, the hacker can play back the earlier messages, but can also generate own CAN messages. However, this figure does not contain the attack potential indicator numbers, it can be concluded, that the message generation phase has a high attack potential, because it is a basic attack type with relatively high probability value, with a detection multiplier of 1-1,2, since there supposed to be some built in detection mechanism.

Fig. 3 shows the last example, which is a Denial of Service attack against a Bluetooth interface. After starting the Bluetooth discovery process, the attacker has multiple possibilities to gather enough information for pairing. One the connection is established, the DOS attack (Zhang et al., 2018) can be started either by playing back previously recorded messages, or by injecting randomly generated messages. However, the attack potentials will

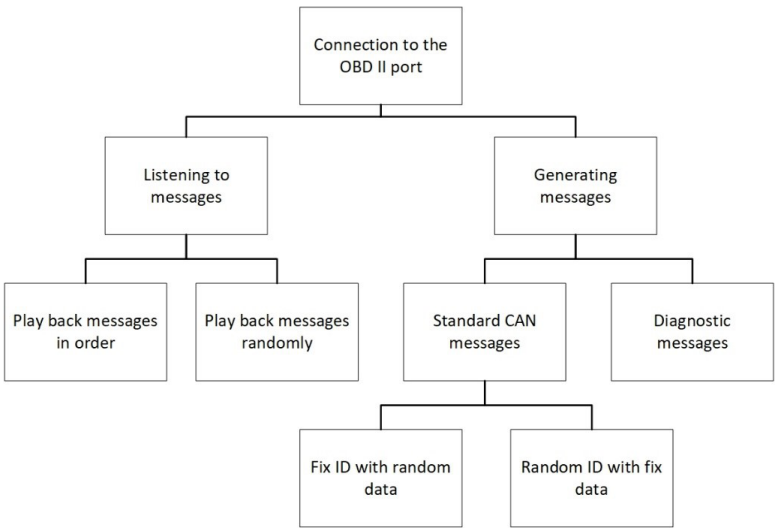

Fig. 2 Message injection attack tree

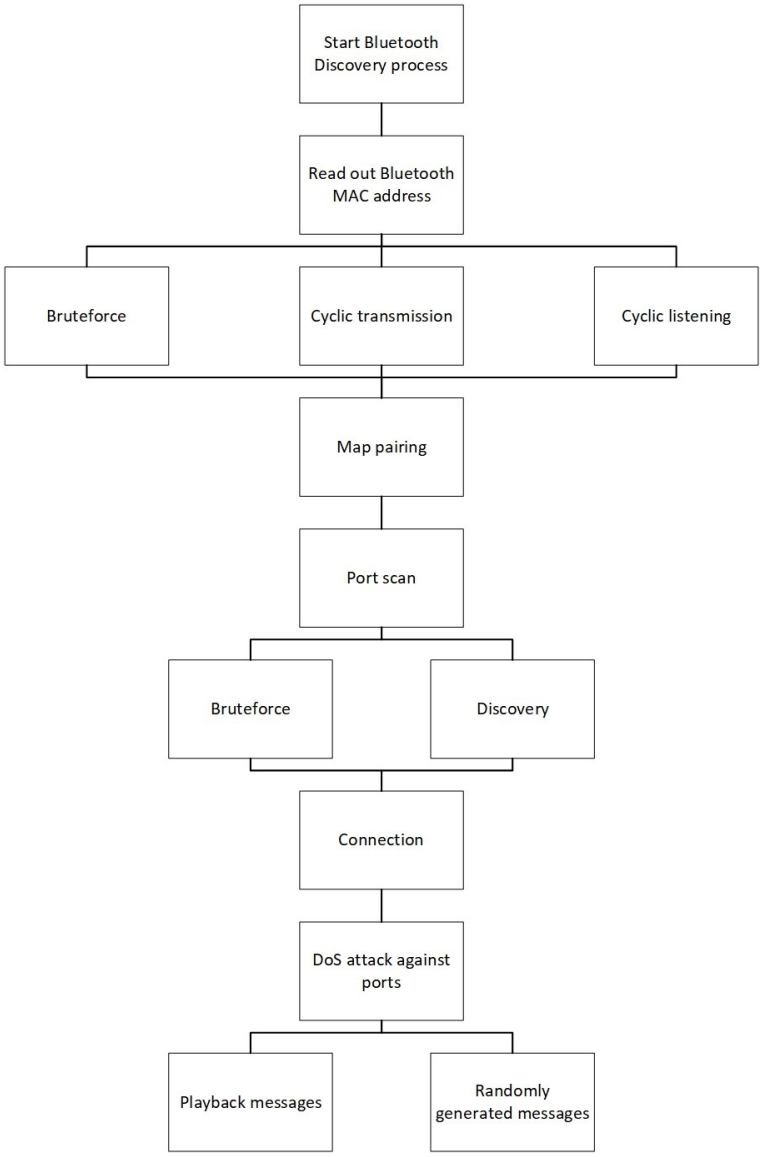

Fig. 3 DOS attack tree

be a bit lower in this case because of the increased difficulty, the multiplier is still relevant. If we think a bit about the extended FMEA RPM number introduced in the previous section, we can imagine a relatively high RPM number, since the severity can be high, if the Bluetooth interface has control over the speakers and can produce for example sudden, loud noises.

6 Summary

Summing up the results, the document has presented the applicable attack methodologies targeting to break the security systems of a road vehicle. The paper has also discussed the detection possibilities, and has introduced a novel ranking system based on the security mechanism of the given intervention. As a new result, an attack potential number has been introduced, which is based on the attack probability, attack difficulty and detection methods. With the introduced novel attack potential indicator a new extension of FMEA approach has been prepared.

Although, the security related evaluation techniques (Abdo et al., 2018) requires a lot of abstraction and sometimes it seems to be difficult to work out and apply objective evaluation methodologies, it has been introduced that a parameter based, quantifiable approach can provide objective basis for security related decision processes. Nonetheless it still requires a lot of imagination and experience to identify the possible attack channels, and quantify probabilities and characteristics. Even if such an analysis is prepared, the industry has to be ready to continuously improve the security aspects, to keep abreast of the advanced methods and technology of malicious interventions.

Acknowledgement

The research reported in this paper was supported by the Higher Education Excellence Program of the Ministry of Human Capacities in the frame of Artificial Intelligence research area of Budapest University of Technology and Economics (BME FIKP-MI/FM).

References

Abdo, H., Kaouk, M., Flaus, J.-M., Masse, F. (2018) "A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie–combining new version of attack tree with bowtie analysis", Computers & Security, 72, pp. 175–195. https://doi.org/10.1016/j.cose.2017.09.004

Cheah, M., Shaikh, S. A., Bryans, J., Wooderson, P. (2018) "Building an automotive security assurance case using systematic security evaluations", Computers & Security, 77, pp. 360–379. https://doi.org/10.1016/j.cose.2018.04.008

Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czeskis, A., Roesner, F., Kohno, T. (2011) "Comprehensive Experimental Analyses of Automotive Attack Surfaces", In: 20th USENIX Conference on Security, San Francisco, USA, pp. 77–92.

Farkas, C., Telek, M. (2018) "Capacity Planning of Electric Car Charging Station Based on Discrete Time Observations and MAP (2) /G/c Queue", Periodica Polytechnica Electrical Engineering and Computer Science, 62(3), pp. 82–89. https://doi.org/10.3311/PPee.11841

Ghadi, M., Török, Á., Tánczos, K. (2019) "Integration of Probability and Clustering Based Approaches in the Field of Black Spot Identification", Periodica Polytechnica Civil Engineering, 63(1), pp. 46–52. https://doi.org/10.3311/PPci.11753

Gopalakrishnan, K., Gholami, H., Vidyadharan, A., Choudhary, A., Agrawal, A. (2018) "Crack Damage Detection in Unmanned Aerial Vehicle Images of Civil Infrastructure Using Pre-trained Deep Learning Model", International Journal for Traffic and Transport Engineering, 8(1), pp. 1–14. https://doi.org/10.7708/ijtte.2018.8(1).01

Hajiagha, S. H. R., Hashemi, S. S., Mohammadi, Y., Zavadskas, E. K. (2016) "Fuzzy Belief Structure Based VIKOR Method: An Application for Ranking Delay Causes of Tehran Metro System by FMEA Criteria", Transport, 31(1), pp. 108–118. https://doi.org/10.3846/16484142.2016.1133454

Kis, L., Lantos, B. (2013) "High precision GPS positioning with multiple receivers using carrier phase technique and sensor fusion", Periodica Polytechnica Electrical Engineering and Computer Science, 57(3), pp. 83–97. https://doi.org/10.3311/PPee.2102

Martin, H., Tschabuschnig, K., Bridal, O., Watzenig, D. (2017) "Functional Safety of Automated Driving Systems: Does ISO 26262 Meet the Challenges?", In: Watzenig, D., Horn, M. (eds.) Automated Driving: Safer and More Efficient Future Driving, Springer, Cham, Switzerland, pp. 387–416. https://doi.org/10.1007/978-3-319-31895-0_16

Miller, C., Valasek, C. (2014) "A Survey of Remote Automotive Attack Surfaces", [online] Available at: http://illmatics.com/remote%20attack%20surfaces.pdf [Accessed: 21 May 2018]

Pan, L., Zheng, X., Chen, H. X., Luan, T., Bootwala, H., Batten, L. (2017) "Cyber security attacks to modern vehicular systems", Journal of Information Security and Applications, 36, pp. 90–100. https://doi.org/10.1016/j.jisa.2017.08.005

Rizvi, S., Willet, J., Perino, D., Marasco, S., Condo, C. (2017) "A Threat to Vehicular Cyber Security and the Urgency for Correction", Procedia Computer Science, 114, pp. 100–105. https://doi.org/10.1016/j.procs.2017.09.021

SAE Vehicle Cybersecurity Systems Engineering Committee (2016) "SAE J3061_201601 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems", SAE (Society of Automotive Engineers) International, USA. https://doi.org/10.4271/J3061_201601

Salay, R., Queiroz, R., Czarnecki, K. (2018) "An Analysis of ISO 26262: Machine Learning and Safety in Automotive Software", SAE Technical Paper, 2018-01-1075. https://doi.org/10.4271/2018-01-1075

Szíjj, A., Buttyán, L., Szalay, Zs. "Hacking cars in the style of Stuxnet", [pdf] Laboratory of Cryptography and System Security, Budapest, Hungary, Available at: http://www.hit.bme.hu/~buttyan/publications/carhacking-Hacktivity-2015.pdf [Accessed: 20 November 2018]

Talic, A. (2017) "Security Analysis of Ethernet in Cars", MSc Thesis, KTH Royal Institute of Technology, [online] Available at: https://people.kth.se/~maguire/DEGREE-PROJECT-REPORTS/171006-Ammar_Talic_with_cover.pdf [Accessed: 12 June 2018]

Tettamanti, T., Varga, I., Szalay, Z. (2016) "Impacts of Autonomous Cars from a Traffic Engineering Perspective", Periodica Polytechnica Transportation Engineering, 44(4), pp. 244–250. https://doi.org/10.3311/PPtr.9464

Vetrella, A. R., Causa, F., Renga, A., Fasano, G., Accardo, D., Grassi, M. (2019) "Multi-UAV Carrier Phase Differential GPS and Vision-based Sensing for High Accuracy Attitude Estimation", Journal of Intelligent & Robotic Systems, 93(1-2), pp. 245–260. https://doi.org/10.1007/s10846-018-0821-9

Wang, Q., Lu, Z., Qu, G. (2018) "An Entropy Analysis based Intrusion Detection System for Controller Area Network in Vehicles", [manuscript] Computer Science, Cryptography and Security (cs.CR), arXiv:1808.04046, Cornell University, Ithaca, NY, USA.

Zhang, H., Qi, Y., Wu, J., Fu, L., He, L. (2018) "DoS Attack Energy Management Against Remote State Estimation", IEEE Transactions on Control of Network Systems, 5(1), pp. 383–394. https://doi.org/10.1109/TCNS.2016.2614099

Zöldy, M. (2018) "Legal Barriers of Utilization of Autonomous Vehicles as Part of Green Mobility", In: Burnete, N., Varga, B. O. (eds.) Proceedings of the 4th International Congress of Automotive and Transport Engineering (AMMA 2018), Springer, Cham, Switzerland, pp. 243–248. https://doi.org/10.1007/978-3-319-94409-8_29