E3S Web of Conferences **268**, 01010 (2021) https://doi.org/10.1051/e3sconf/202126801010
VESEP2020

Study on cybersecurity attack-defense visualization method based on intelligent connected vehicle

Yafei Wang, *Shengqiang* Han*, *Nan* Zhang and *Peng* Hu
Automotive Technology Information Research Institute, China Automotive Technology and Research Center Co., Ltd, Tianjin, China

Keywords: intelligent connected vehicle, cybersecurity, attack-defense, visualization.

Abstract. Attack test and defense verification are important ways to effectively evaluate the cybersecurity performance of Intelligent Connected Vehicle (ICV). This paper investigates the problem of attack-defense visualization in ICV cybersecurity. For the purpose of promoting cybersecurity research capabilities, a novel Cybersecurity Attack-Defense Visualization method based on Intelligent Connected Vehicle (CADV-ICV) is proposed. In this scheme, an Attack-Defense Game model (ADG) is designed so that the logical relationship between the attack and defense can be studied through a system architecture. Then, the CADV-ICV method is implemented through three layers that are hardware layer, software layer and visualization layer. Finally, through an Intelligent Connected Vehicle, two TV monitors, a computer and a server, a real experimental environment is built to test the CADV-ICV method. The experimental results show that CADV-ICV can realize the visual display of attack-defense process, attack messages, defense state, real-time message monitoring, and attack-defense principle for 10 car's components.

1 Introduction and motivation

Intelligent Connected Vehicle (ICV) is refers to the organic combination of Internet of Vehicles and smart cars. It is equipped with advanced in-vehicle sensors, controllers, actuators, etc., and integrates modern communication and network technology to make the car realize the intelligent information sharing with people, cars, roads, and back-offices, to ensure the car's safety, comfortable experience, energy-saving, efficient driving. as well as ultimately to replace people to operate the next-generation cars [1]. With the improvement of the intelligence of automobiles, the cybersecurity of automobiles is getting more and more attention. However, the rapid changes to enhance the intelligent and connected functions of cars are having a serious effect on their security, and the cybersecurity incidents of cars are constantly emerging. In 2015, preeminent Hackers Charlie Miller and Chris Valasek

* Corresponding author: hanshengqiang@catarc.ac.cn

dominated headlines with their landmark hack of a Jeep Cherokee [2]. In 2016, team of hackers take remote control of Tesla Model S from 12 miles away [9]. In 2017, Keen Lab discovered new security vulnerabilities on Tesla motors and realized full attack chain to implement arbitrary CAN Bus and ECUs remote controls on Tesla motors with latest firmware [3]. In 2018, researchers hacked BMW cars and discovered 14 vulnerabilities [4]. As the cybersecurity incidents of automobile are mostly signal attacks which are mostly invisible for human's eye and even inaudible [5-7], people are so unfamiliar with automotive cybersecurity attacks that the effective protection measures cannot be taken to solve that. With the adoption of the Cybersecurity Law of the People's Republic of China [8], people began to pay attention to the knowledge of cyber-attack and cyber-defense that are important technologies to effectively evaluate the cybersecurity performance of Intelligent Connected Vehicle (ICV). The research work and experiments on cybersecurity attack testing and defense verification are gradually increasing. Whereas there is relatively little research on the visualization method of cybersecurity attack and defense. Specifically, visualization is a theory, method and technique that uses computer graphics and image processing techniques to convert data into graphics or images for display on the screen and then interactive processing [9]. If visualization technology can be applied to the research and development of automotive cybersecurity attack-defense, it will not only enhance people's better understanding of problems, facilitate dialogue, exploration and communication, but also simplify the complexity of research questions and enhance the review.

In order to realize the visualization of automotive cybersecurity attack and defense technology research, this paper is motivated. The main contributions of this paper include the following: (i) The Attack-Defense Game model (ADG). (ii) Cybersecurity Attack-Defense Visualization Method Based on Intelligent Connected Vehicle (CADV-ICV). The remainder of this paper is organized as follows. Section 2 presents the design of Attack-Defense Game model. Section 3 provides the implementation procedure of cybersecurity attack-defense visualization method. Section 4 depicts the experimental result that includes the experimental environment construction and the verification results. A conclusion is given in Section 5.

2. Attack-defense game model

Taking ICV as the research object, the Attack-Defense Game model (ADG) between Intelligent Connected Vehicle (ICV) and hacker is designed in this section. Specifically, the ADG model takes hacker's malicious attack command as input, and the effect of ICV as output, such as attack-defense states, can message and real-time message monitoring. It includes attack flow and defense flow. The attack flow mainly consists of attack instructions sent by hackers, such as attack messages of door, window and throttle, and the defense flow is mainly composed of the security defense effect of the vehicle's network protection mechanism, such as car security access authentication, signature verification mechanism. The working principle of ADG model is shown as follow. Firstly, defense flow intercepts the instructions in each attack flow and matches the corresponding defense measures. Then, if the interception is successful, the model outputs the information of defense success and attack failure. Otherwise, the attack success and defense failure will be output. Subsequently, the visualization module will show the state of the corresponding information during a vehicle's attack-defense. Finally, the attack visualization and protection visualization modules work together to demonstrate a visual representation of their logical relationship.

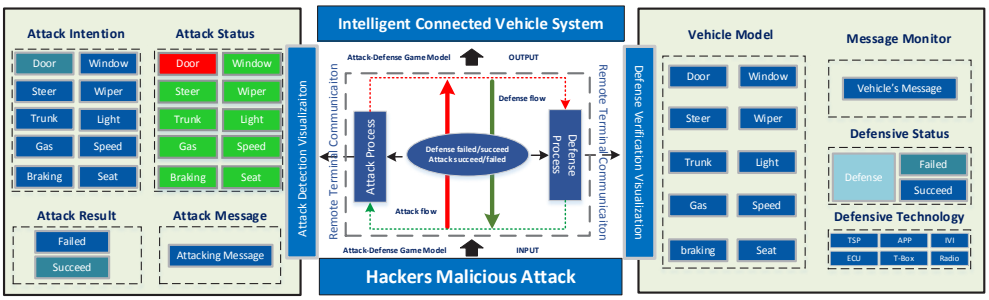


Fig. 1. The Attack-Defense Game model.

In the CADV-ICV method, the attack and defense visualization is realized in the form of a display platform interface, and the visualization method mainly utilize HTML5, jQuery and CSS3 technologies for development, and it implemented real-time communication through the socket based on the terminal communication technology. According to the change of real-time data, dynamic effects display is performed by using canvas technology and CSS animation. The visual page layout is mainly implemented by a combination of percentage and flex layout. The attack-defense visual interface is mainly composed of two pages: attack detection visualization and defense monitoring visualization. The ADG model is used to visually present the ICV's three network states, which are no attack, defense failure (attack success) and defense success (attack failure) .

The Attack Detection Visualization (ADV) design is based on the Button Group, Prompt Box, Status Group, List Group, and Popup. It can implement attack intent visualization, attack status visualization, attack result visualization, and attack message visualization, which are presented as follow.

a). Attack Intent Visualization (AIV), which is built to visualize the malicious hacking process of ten components, such as door, window, steering wheel, wiper, trunk, lights, throttle, speed, brake and seat. In particular, when each attack intention occurs, the window text prompt and the voice broadcast corresponding attack intention are displayed, and the button group corresponding item is pressed after 3 seconds. For example, when the door is attacked, the window text prompt and voice broadcast that the door is attacked, and the door button is pressed after 3 seconds.

b). Attack Status Visualization (ASV), which corresponds to the attack intent visualization, which visualizes the current state of the door, window, steering wheel, wiper, trunk, lights, throttle, speed, brake and seat. By the way, the normal state is green and the attackend state is red in our proposed method. For example, when the car door is attacked, the door in the attack intent visualization is in the pressed state, and the door item in the attack state visualization is rendered as the attacked red.

c). Attack Result Visualization (ARV), which presents the output of the ADG model in the form of local state popup and background motion. It is made up of two states of defense failure (attack success) and defense success (attack failure).

d). Attack Message Visualization (AMV), which is based on the List Group development, the message signal of the car being attacked is visualized in a scrolling manner.

The Defense Monitoring Visualization (DMV) development is based on the Status Group, Message List and Status Panel, which enables automotive model visualization, message monitoring visualization, defense status visualization and defense technology visualization, which are depicted as follows.

a). Automotive Model Visualization (AMV), which fully presents the security status of important parts of the car in the form of a schematic diagram of the vehicle model. When one of the car's components (windows, steering wheel, wipers, trunk, lights, throttle, speed, brake and seats) is attacked, the corresponding part will become red.

b). Message Monitoring Visualization (MMV), which is based on the Message List development. In MMV, the current message status of the car's network is displayed in real time, and the message display updates the form data according to the socket push based on the remote terminal communication technology.

c). Defense Status Visualization (DSV), which is based on the State Panel development. It can dynamically visualizes the working status of the vehicle protection system, including three states, which are system protecting, defense succeed and defense failed.

d). Defense Technology Visualization (DTV), which is based on the State Group development, It statically visualizes the security protection measures that the ICV system has taken.

3 Method and implementation

Relying on the ADG model, a novel Cybersecurity Attack-Defense Visualization method based on Intelligent Connected Vehicle (CADV-ICV) is proposed in this section. It realizes the visual presentation of the state of the car units around the ten important functional units (windows, steering wheel, wipers, trunk, lights, throttle, speed, brake and seats), as well as the visual presentation of the relationship between external attack and internal defense for ICV's system. The CADV-ICV method is implemented through three layers (Fig.2) that are hardware layer, software layer and visualization layer, which are presented as follows.

a). Hardware implementation

The hardware layer implementation mainly completes the deployment of the hacker devices, the Intelligent Connected Vehicle, the remote communication terminal, the cloud server, and the front-end display device. Specifically, the hacker device deployment includes a technician and an attack device computer. Intelligent Connected Vehicle is the main attack object of hacker. The remote terminal communication is deployed on the Intelligent Connected Vehicle to realize the monitoring of the vehicle's state. The cellular remote communication technology uploads the vehicle's status data to the cloud server. The cloud server is responsible for the collection and processing of the vehicle status data. The visualization screen is used as the display of invisible information, such as attack signal, vehicle's message, vehicle components states.

b). Software layer implementation

The software layer implements five major functions: attack message sending, CAN message collection, collected message transmission, message data analysis, and status information display. The attack message is sent by the hacker device. The CAN message collection is based on the Intelligent Connected Vehicle, which realizes the collection of the CAN message data of the car's system. The collected message transmission uploads the collected message data to the cloud server by means of the remote communication terminal. The message data analysis is performed on the cloud server and the information content of the packet data is parsed. The status information display is output to the front-end display to complete.

c). Visualization layer implementation

The visualization layer is implemented on the basis of the support of the hardware layer and the software layer. Through the HTML5 Web socket, TCP, JQuery, CSS3 and canvas technologies, it realize the visualization of the attack state and the visualization of the defense state, and the ICV's attack and defense game of the intelligent network is visually displayed.

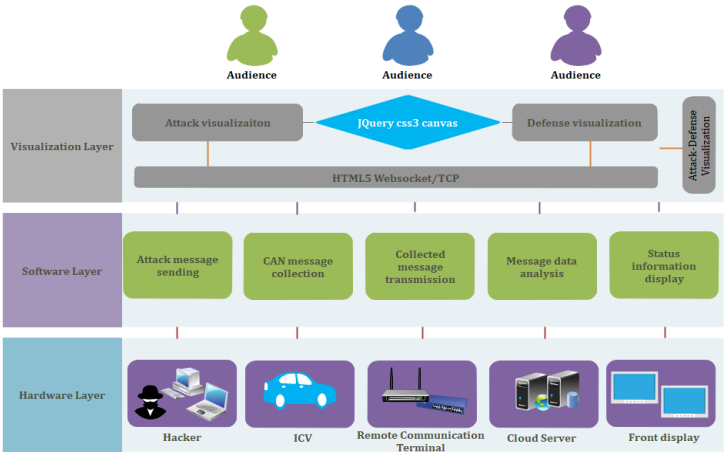


Fig. 2. The attack-defense game model.

4 Experiment result

4.1 Experimental enviroment

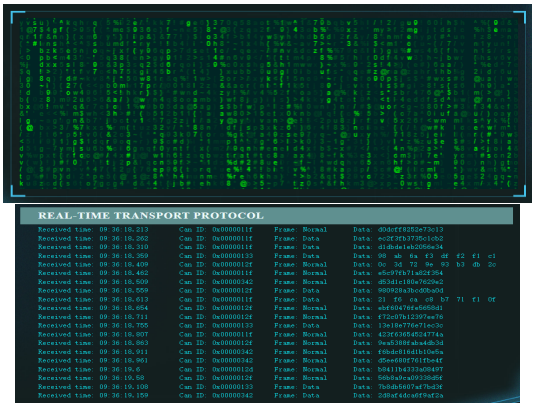
In our experiment, an Intelligent Connected Vehicle, two TV monitors, a computer and a server are selected to build an experimental environment to test the proposed method of CADV-ICV. Based on the ADG model, we designed the system interface as shown in Fig.3. Fig.3 (a) is an attack visualization experiment interface to visualize the information related to car's attacks. Fig.3 (b) is a protective visualization experiment interface to visualize the car's protection information.

(a). Attack visualization (b). Defense Visualization

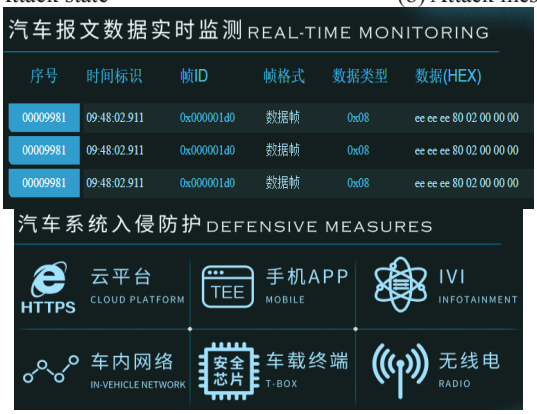
Fig. 3. Experiment environment interface.

4.2 Results

Based on the visual experimental environment that has been built, attack-defense visualization experiment was carried out on the top ten functional units (windows, steering wheel, wipers, trunk, lights, throttle, speed, brake and seats) of the car to test the validation of the CADV-ICV method. In the application, we exploited the car CAN bus protocol vulnerability to simulate the hacking behavior to attack the car. As well as the situation when the car defense system intercepted the car in the face of external attacks. The results show that CADV-ICV can realize the visualization of cybersecurity attack-defense for ICV, and the visualization contents covered the attack states, attack messages, real-time message monitoring, and defensive measures, which are shown in Fig.4. Besides, the experiment gave the result of the attack-defense principle's verification for 10 units of car in Tab.1. It is noticeable that attack and defense are two opposite faces.



(a) Attack state (b) Attack messages



(c) Real-time message monitoring (d) Defensive measures

Fig. 4. CADV-ICV method application.

Table 1. Verification results of CADV-ICV method.

Units	Attack		Defense		Verified result
Windows	Succeed	Failed	Failed	Succeed	Passed
Steering wheel	Succeed	Failed	Failed	Succeed	Passed
wiper	Succeed	Failed	Failed	Succeed	Passed
Trunk	Succeed	Failed	Failed	Succeed	Passed

Lights	Succeed	Failed	Failed	Succeed	Passed
Throttle	Succeed	Failed	Failed	Succeed	Passed
Speed	Succeed	Failed	Failed	Succeed	Passed
Brake	Succeed	Failed	Failed	Succeed	Passed
Seat	Succeed	Failed	Failed	Succeed	Passed

(a) Prompt and warning (a) Visualization of status

Fig. 5. Attack visualization.

Take the experiment when the car steering wheel receives an attack for instance, when it is attacked, the experimental result is shown in Fig 5. Fig 5 (a) is a pop-up prompt and voice warning broadcast of the steering wheel being attacked. Fig 5 (b) shows the visualization and status of the attacked message on the steering wheel. and the red part indicates where the car was attacked. Corresponding to the situation in Fig 5, Fig 6 gives the visual representation of the current defense state and attacked parts of the automotive system. Besides, the car's successful defense status is shown in Fig 7, which is the same as the running states when the car does not receive any external attacks. Once it receives an external attack, the interface will change to Fig 6. Furthermore, Fig 8 shows the visualization results when the two functional elements of the car are attacked at the same time, and the red parts indicate where the car were attacked.

Fig. 6. Hacked situation.

Fig.7. Defense succeed result.

Fig.8. Multiple units were hacked.

5 Conclusion

This paper investigated a novel approach of CADV-ICV to address the problem of invisible information flow in ICV's cybersecurity. The method not only can help to improve the security performance of automotive information, but also can popularize automotive cybersecurity knowledge to the audience. Specifically, the ADG model has been designed based on Intelligent Connected Vehicle, which presents the logical relationship between the ICV's attack and defense as well as information flow. Then, the CADV-ICV method has been implemented through three layers that are hardware layer, software layer and visualization layer. Finally, an ICV real experimental environment has been built to conduct the test. The results demonstrate the effectiveness of the proposed method.

This work described in this article has been supported by Automotive Data Center of China Automotive Technology and Research Center Co., Ltd. It provides the laboratory, the experiment car, testing hardware device and support required to carry out this method successfully.

Reference

1. Y. Li, Y. Cao, H. Qiu, L. Gao, Z. Du and S. Chen, Big wave of the intelligent connected vehicles, in China Communications, 13 (2), 27-41, 2016.
2. Tesla Model S hacked from 12 miles away. https://www.welivesecurity.com/2016/09/21/tesla-model-s-hack/. Accessed 17 Jan 2019

3. New Car Hacking Research: 2017, Remote Attack Tesla Motors Again. https://keenlab.tencent.com/en/2017/07/27/New-Car-Hacking-Research-2017-RemoteAttack-Tesla-Motors-Again/. Accessed 16 Jan 2019
4. Researchers hack BMW cars, discover 14 vulnerabilities. https://www.helpnetsecurity.com/2018/05/23/hack-bmw-cars/. Accessed 17 Jan 2019
5. Parkinson, S.: Cyber threats facing autonomous and connected vehicles: future challenges. IEEE Trans. Intell. Transp. Syst. 18(11), 2898–2915 (2017)
6. Sadek, A.: Special issue on cyber transportation systems and connected vehicle research. J. Intell. Transp. Syst. 20(1), 1–3 (2016)
7. Luo, Q.: Wireless telematics systems in emerging intelligent and connected vehicles: threats and solutions. IEEE Wirel. Commun. 25(6), 113–119 (2018)
8. (Authorized to publish) People's Republic of China Cyber Security Law http://www.xinhuanet.com/politics/2016-11/07/c_1119867015.htm
9. Wei Zong, Yang-Wai Chow, Willy Susilo. Interactive three-dimensional visualization of network intrusion detection data for machine learning[J]. Future Generation Computer Systems, 2020,102.