Advances in Social Science, Education and Humanities Research, volume 586
Proceedings of the 2021 International Conference on Public Relations and Social Sciences (ICPRSS 2021)

Analysis on Cyber Security Development of Intelligent and Connected Vehicles in China

Hao Zhao[1,*] Zhibin Du[1] Xianglei Zhu[1]Chao Ma[1]

[1] *China Automotive Technology and Research Center Co., Ltd*
[*]*Corresponding author. Email: zhaohao@catarc.info*

ABSTRACT
At present, intelligent networked vehicles have become the key focus and strategic commanding point of the new round of development and reform of emerging industries in the world, and are in the critical stage of rapid technological evolution and accelerated industrial layout. It is extremely urgent to strengthen the network security of intelligent vehicles and promote the safe development of intelligent networked vehicles. The network security problem of intelligent networked vehicles may bring risks in the aspects of environment perception, network transmission, decision execution and driving control. As the software of automotive electronic platform has entered the stage of billions of lines of code, the inevitable security loopholes will cause a lot of risks. In addition, all kinds of data collected by vehicles and the privacy of users involved also need to be fully guaranteed. Therefore, ensuring the safety of automotive network will be one of the key elements of the transformation and upgrading of China's automotive industry towards a new era, and it is also an important measure to maintain cyberspace security, social security and even national security.

Keywords: *Intelligent Networked Vehicles; Cyber Security; Electrification.*

1. INTRODUCTION

With the continuous improvement of automotive intelligence, networking and electrification, the problem of intelligent networked automotive network security has become increasingly serious. Information tampering, virus intrusion and other means have been successfully used by hackers in automotive attacks, especially the frequent recalls of automotive network security in recent years have aroused great concern of the industry. The network security crisis of intelligent networked cars can not only cause personal privacy and economic losses of enterprises, but also cause serious consequences of car crash and death, and even become a national public security problem.[1] Although the security vulnerabilities of intelligent networked vehicles have not been widely used at present, some consumers say that network security and privacy protection will be the main considerations when they buy vehicles in the future. The network security of intelligent networked vehicles does not only refer to the network security of vehicles themselves, but an overall ecological security including communication, cloud platform and external emerging ecosystem. It is necessary to conduct regular safety inspection on the whole ecology in order to discover potential risks.

Although the research on intelligent networked car network security technology started late, it also achieved certain results: Tencent Cohen Lab focused on the research of cutting-edge security attack and defense technology of smart cars, and carried out in-depth research on the automatic driving network security of Tesla, BMW and other models; 360 has launched a number of car safety protection and testing products such as 360 car guards and CANPICK. The 360 car networking safety operation platform based on safe big data has also been put into operation; China Automotive Data has established the first network security vulnerability database in the automotive industry in China. At present, it has collected more than 2,000 vulnerability data and docked with the network security vulnerability information sharing platform of the Ministry of Industry and Information Technology; Shudao Data launched the vehicle "Active Safety Intelligent Prevention and Control System" to serve "two passengers and one danger" vehicles and drivers; Tianrongxin has launched a series of security detection and anti-intrusion products for vehicle networking, providing security protection for each module of vehicle networking. [2]

At present, the construction of intelligent networked automotive network security management system in

China is still in the initial stage. Enterprises generally pay more attention to the security status of traditional network security fields, such as APP, cloud platform, computer room and network equipment, and have mature testing and development experience, with sufficient staffing, and regularly carry out penetration testing and vulnerability scanning to ensure security. In view of the weak level of safety protection of automotive network, some problems have been exposed in safety detection and protection of vehicle parts and automotive data, etc., the awareness of safety management and safety protection needs to be improved, and the safety technology needs to be improved urgently. However, enterprises begin to attach importance to the development of product network safety, expand and extend the field of safety control, and promote the healthy development of enterprises.[3]

2. COMPARISON OF INTELLIGENT CONNECTED AUTOMOTIVE CYBER SECURITY DEVELOPMENT

2.1. USA

The release of relevant policy documents in the United States provides a guiding framework of rules and regulations for traditional automotive manufacturers and other relevant institutions that produce, design, supply, test, sell, operate or apply autonomous vehicles.[4] In 2016, the U.S. Department of Transportation issued the "Policy Guide for Self-driving Vehicles in the United States", which proposed that manufacturers and other institutions should take the initiative to provide safety evaluation reports on how to follow the guide, including using identification, protection, detection, response and recovery functions to make risk management decisions, solve risks and threats, respond to network security incidents quickly, and share relevant industry information.

2.2. Europe

On May 17, 2018, the European Union adopted the EU Future Travel Strategy (Directive 283), which emphasizes increasing investment in network security, data protection and data access of autonomous vehicles. In February 2019, the European Union issued an action guide for Directive 283, which put forward specific requirements for the safety of automotive type certification. In terms of network security, the guide requires the adoption of network security design for vehicles to protect vehicles from hackers; Automotive manufacturers are required to take necessary measures such as software upgrade to ensure the network security of automatic vehicles during use.[5]

2.3. Japan

The National Police Agency of Japan released the revised draft of the Road Traffic Law, and listed the possible hacker attack risks of self-driving vehicles due to the need to obtain maps and traffic information on the Internet, as well as other cyber attacks against self-driving vehicles.[6]

In August, 2013, Japan Information Processing and Promotion Agency (IPA) released the Guide to Vehicle Network Security, and put forward the model of vehicle network security "IPA Car", aiming at the network security of "networked" vehicles, and formulated safety policies and measures at various stages of the automotive life cycle. In Japan's Cyber Security Strategy, the requirements of building an information sharing platform, classifying the severity of events, managing risks, maintaining and promoting safety rules, and enhancing emergency response capabilities are put forward. JAMA also established J-Auto ISCA, a Japanese automotive information sharing organization.

3. DEVELOPMENT TREND OF AUTOMOTIVE CYBER SECURITY TECHNOLOGY

3.1. Vehicle enterprises pay full attention to safety construction and speed up the safety layout of automotive network

Due to the long industrial chain of car networking, with "one cloud at both ends" as the main body, including smart cars, mobile intelligent terminals, car networking service platforms and other objects, it is very important for the whole vehicle enterprise between upstream and downstream to ensure the network security of smart cars. Automotive manufacturers represented by Geely, BYD and BAIC have started the deployment of intelligent networked automotive network security, and started to build security capabilities such as network security institutions, personnel and emergency management systems, and made certain progress.[7]

3.2. Actively promote the formulation of safety standards to promote the safe development of automotive networks

At present, various organizations at home and abroad are actively studying and standardizing the safety of automotive network, and have set up a special safety working group to develop the safety standard of automotive network, which provides the necessary theoretical basis for the development of the safety of automotive network. ISO/TC22 technical Committee on road vehicles defines the scope, object and content framework of international standard ISO/SAE21434 (road vehicles-network safety engineering); 3GPP is

working on LTE-V2X security research and standard formulation. Domestic relevant departments, societies and standards committees have also vigorously promoted the research on the standard system of vehicle networking after the introduction of the national standards for network security. Xin 'an Standards Committee, Intelligent Transportation Standards Committee, Automotive Standards Committee and China Automotive Engineering Society have formulated and issued guidelines and technical requirements related to network security, providing a strong grasp for all vehicle companies and suppliers.[8]

3.3. The momentum of automotive network security is developing strongly, and the security technology needs to be improved.

At present, the intelligent networked automotive industry is developing rapidly, and network security has received widespread attention from relevant administrative departments and the industry. The research and formulation of relevant security policies and standards are being actively promoted. With the gradual landing of relevant work achievements, the overall development of network security will gradually take shape. [9]However, at this stage, vehicle safety technology is still in transition, and it will take time for some network safety technologies to be developed, applied and popularized, and it will take a certain period for upgrading production lines and deploying and applying safety products. In addition, the elimination cycle of existing cars is long, so there is no mature solution to strengthen the network security capability of existing cars.

3.4. Analysis of the status quo of the security protection system

The construction of network security protection system is the internal requirements of enterprises based on the modernization of information development, but also an important guarantee to improve information security management ability and promote the healthy development of enterprises. For the vehicle, the common protection means are as follows:

1. The data structure, arbitration technology, flexible communication mode and other features of CAN bus CAN meet the real-time and lightweight requirements of automobiles, but also exposed some security risks. To solve these problems, the key protection technologies include: protecting the CAN bus message data source by means of device authentication and adding OBD firewall; CAN bus data is protected by using AES packet encryption technology and secure CAN transceiver chip. Important domains are protected by physical isolation of gateways. Intrusion detection system; Secure diagnostic access services.

2. T-box security protection is mainly carried out from three layers: system layer, software layer and communication layer. The protection of the system layer revolves around the promotion of authority, sensitive information leakage, weak password, address space layout randomization, data execution protection and firewall configuration. Software layer protection needs to fully consider stack overflow, heap overflow, integer overflow, format string, hard-coded sensitive data, anti-debugging mechanism and shell protection technology; For communication layer protection, consider the SSH service.

3. IVI security protection is mainly carried out from four layers: hardware layer, system layer, software layer and communication layer. The hardware layer mainly focuses on debugging interface, security chip and USB security. The system layer covers protection against system vulnerabilities, hidden back doors, and port exposure; The software layer mainly includes system application security, third-party application security and sensitive data security; In the communication layer, plaintext transmission and network isolation are the main protection contents.

4. As an integral part of intelligent connected vehicle control and information display, the safety of APP is particularly important. Due to the diversity of apps from different manufacturers, there are various security problems. Common security vulnerabilities in apps are sorted out. Protection means include: installation package protection; Component protection; Information leakage protection; Default Settings for vulnerability protection.

5. As the core component of intelligent networked vehicle information processing interaction, common protection means include: WEB application protection; Middleware security protection; System security protection; Network security protection, etc.

6. As for the safety protection of radio, the intelligent connected car mainly involves Wi-Fi, Bluetooth, intelligent wireless car keys, GPS positioning and tire pressure monitoring system, etc. The main protection technology is: strengthen the car Bluetooth pairing check, PIN code to mix case random; Real-time bluetooth security driver update, tracking domestic and foreign vulnerability disclosure; Handle the exception of the external receiving data module in the bottom interface of bluetooth driver; Secure Ble communication encryption for APP or car keys, and improve APP reinforcement; Pay attention to the dynamics of the protocol stack, update and repair the driver protocol in time.

4. EXISTING PROBLEMS IN THE INDUSTRY

Cyber security incidents occur frequently. According to the 2020 Automotive Network Security Report

released by Upstream Security, by 2020, 330 million vehicles have been connected, and the increase in the number of connected vehicles has increased the potential destructive power after being attacked by the network. Large-scale attacks against connected vehicles may destroy the whole city and even lead to catastrophic loss of life. Since 2016, the number of annual security incidents has increased by 605%, and has more than doubled in 2019 alone. In 2019, 57% of the incidents were carried out by cybercriminals, aiming at destroying business, stealing property and demanding ransom.[10]

Security technology gap still exists. Due to the policy and financial obstacles in the technical research and application of vehicle networking enterprises,[11] it is difficult to build a complete system-level security solution, and the security technology gap still exists, so the vehicle networking security system covering the application scenarios has not yet been formed.

Lack of a unified safety monitoring platform. At present, the detection methods and evaluation standards of intelligent networked automotive network security have not yet achieved professional unification, the number of samples in vulnerability database is low, and threat intelligence cannot be exchanged, which makes it impossible for vehicle manufacturers, parts suppliers and automotive networking service providers to effectively verify the safety and reliability of their products, tools and services.[12] However, a vehicle networking monitoring platform with high credibility and rich data resources has not been established in China, and the detection results and monitoring data cannot be effectively recognized and shared, resulting in unequal information and waste of technology and data resources in the docking between supply and demand.

The system of policies and regulations needs to be improved. The Network Security Law has been officially implemented since June 1, 2017, which clearly requires network operators, including car networking operators, to fulfill their network security protection obligations, improve the level of network security protection, and promote the healthy development of the industry. The newly released Strategy for Innovation and Development of Smart Vehicles clearly proposes to ensure the healthy and orderly development of the intelligent networked automotive network security industry. However, there are still a large number of laws and regulations that have not yet been issued. We should introduce and absorb foreign advanced management experience, improve policies and regulations that adapt to the development of China's car networking security industry, and speed up the construction of a network security management system including the whole vehicle and key system components.

5. CONCLUSION

In the future, the development of China's automotive network security can start from perfecting laws and regulations, gradually strengthen the research on legal issues related to intelligent networked automotive network security, and increase the protection of data privacy and property rights. Explore the establishment and improvement of network security management system and vehicle identity authentication management system, and put forward more targeted capability requirements for intelligent networked vehicles in terms of network security on the basis of meeting the relevant requirements of traditional vehicles. Guide automotive enterprises to establish a complete network security, software upgrade and other management processes, ensure that intelligent networked automotive production enterprises effectively implement the management process requirements, and prevent the safety risks brought by intelligent and networked vehicles. A national supervision platform should be established, and a three-level platform of enterprise, local and national intelligent networked automotive network safety supervision should be set up to ensure the safety of the whole industry chain and life cycle of intelligent networked vehicles and improve the operation level of intelligent networked vehicles.[13]

ACKNOWLEDGMENTS

This work was financially supported by China Automotive Technology Research Center Co., Ltd., Guideline Project-20223405 fund.

REFERENCES

[1] Qin Deze and Meng Junquan. Analysis and Comparison of Cyber security Risk Assessment Methods [J]. Cyber security Technology and Application, 2011(04).

[2] Zhang Jianxiao, Discussion on Cyber security Risk Assessment and Key Technologies [J], Science and Technology Entrepreneurship Monthly, 2015(03).

[3] Yan Feng. Research on Cyber security Risk Assessment Technology Based on Attack Graph [D]. Jilin University, 2014,12 (04): 119-124.

[4] SAE J3061, Cybersecurity Guidebook for Cyber-Physical Vehicle Systems[S].

[5] GB/T 20984-2007, cyber security technology cyber security risk assessment specification [S].

[6] GB/T 31509-2015, implementation guide of cyber security technology cyber security risk assessment [S].

[7] NHTSA. (2018). Automated Vehicles for Safety. [Online]. Available: https://www.nhtsa.gov/technology-innovation/automated-vehicles safety.

[8] K. Eykholt et al., “Robust physical-world attacks on deep learning visual classification,” in Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit., Jun. 2018, pp. 1625–1634.

[9] C. Yan, W. Xu, and J. Liu, “Can you trust autonomous vehicles: Contactless attacks against sensors of self-driving vehicle,” in Defcon, vol. 24, no. 8, p. 109, 2016.

[10] J. Petit, S. Bas, M. Feiri, and F. Kargl, “Remote attacks on automated vehicles sensors: Experiments on camera and lidar,” in Black Hat Eur., vol. 11, p. 2015, Nov. 2015.

[11] P. Kapoor, A. Vora, and K.-D. Kang, “Detecting and mitigating spoofing attack against an automotive radar,” in Proc. IEEE 88th Veh. Technol. Conf. (VTC-Fall), Aug. 2018, pp. 1–6.

[12] Y. Tu, Z. Lin, I. Lee, and X. Hei, “Injected and delivered: Fabricating implicit control over actuation systems by spoofing inertial sensors,” in Proc. 27th USENIX Secur. Symp., 2018, pp. 1545–1562.

[13] M. Amoozadeh et al., “Security vulnerabilities of connected vehicle streams and their impact on cooperative driving,” IEEE Commun. Mag., vol. 53, no. 6, pp. 126–132, Jun. 2015.