ISSN: 2664-9640

Analysis of password application requirements in the intelligent network connected automobile industry

Xuebin Shao [a], Weinan Ju [b] , Ruiqing Zhai [c] , Shimeng Wang [d, *] ,Liping Liu [e]

and Qiujun Zhao [f]

CATARC Software Testing (Tianjin) Co., Ltd Tianjin, China

[a] shaoxuebin@catarc.ac.cn, [b] juweinan@catarc.ac.cn, [c] zhairuiqing@catarc.ac.an,

[d]*wangshimeng@catarc.ac.cn, [e]liuliping2019@catarc.ac.cn, [f]zhaoqiujun@catarc.ac.cn

Abstract

Based on the supply and demand docking status of password applications in the new energy and intelligent networked automobile industry, a supply and demand docking platform for the password application industry chain in the automobile industry has been built, which covers upstream and downstream enterprises in the industry chain such as automobile enterprises, password enterprises, parts manufacturers, and technical service providers, and can provide service guarantee for the development of password applications in the new energy and intelligent networked automobile industry. This paper makes a detailed analysis of the password application requirements of the intelligent connected vehicle, clarifies the development direction of the future password direction, and provides suggestions for the high-quality development of the industry.

Keywords

Intelligent Connected Vehicle; password; V2V;TSP.

1. Introduction

In recent years, with the rapid development of China's new energy and intelligent connected vehicle industry and the increasing number of automobile information security incidents, automobile information security issues have begun to attract extensive attention in the industry. As the basic service support and core technology guarantee of information security technology, the implementation and application of password technology in the automobile industry will push the automobile information security to a new height, from the underlying architecture to the upper application, and ensure the information security of new energy sources and intelligent networked automobile industry in an all-round and full life cycle from inside to outside the vehicle.

Compared with the security problems in traditional cyberspace, automobile information security problems have the characteristics of wider attack scope, stronger concealment and greater harmfulness. They not only threaten the safety of personal property, but also have a significant impact on social public order and even national security. In 2015, two white hat hackers remotely cracked an unmodified JEEP vehicle, thereby realizing remote control of the vehicle, causing Chrysler to recall 1.4 million problematic vehicles, with direct economic losses reaching hundreds of millions of dollars. Since then, automotive information security has attracted extensive attention in the industry.

The State attaches great importance to the security role of passwords and encourages the application of commercial password technology. On January 1, 2020, the Password Law of the People's Republic of China was officially implemented to regulate password application and management and ensure network and information security, which has risen to the legislative level. Articles 21 and 25 of the Password Law clearly state that the State encourages the research and development of commercial password technology, and encourages employers to voluntarily accept commercial password detection and certification, so as to enhance their market competitiveness.

In July 2018, the General Office of the Central Committee of the Communist Party of China and the General Office of the State Council issued the Work Plan for Cryptographic Application and Innovative Development in Financial and Important Fields (2018-2022), which proposed that cryptographic applications should be promoted in 30 important fields, including infrastructure, digital economy, and information for the benefit of the people, all of which are closely related to intelligent connected vehicles.

The purpose of this paper is to solve the problems such as insufficient connection between supply and demand information in the domestic password industry chain of China's new energy and intelligent network connected automobile industry, the absence of an efficient collaboration system for password products and service providers, automobile enterprises, and evaluation institutions, and insufficient application transformation and industrial support capabilities. Based on solving the problems and development needs of password application in the current automobile industry, a basic service platform for password application oriented to new energy and intelligent connected vehicles is built, and the password application needs in the intelligent connected automobile industry are emphatically analyzed, which provides a good foundation for the construction of the subsequent platform.

2. Application Demand Analysis of Intelligent Connected Vehicles

2.1. Car cloud communication password application requirements

The security requirements of Car Cloud Communication mainly include the following five aspects:

(1) Mutual authentication:

1) The cloud TSP authenticates the terminal equipment, identifies illegal terminal equipment, and ensures that only legal terminal equipment can connect to the TSP;

2) The terminal device authenticates the cloud TSP, identifies illegal center connections, and ensures that only legitimate TSPs can connect the terminal device.

(2) Data confidentiality:

1) The data transmission process (terminal to TSP, TSP to terminal) is ciphertext transmission;

2) The key agreement mechanism ensures that each call uses a different key, and prevents the key from being cracked due to long-term use of a group of keys;

3) Ensure that one machine has one secret, and each terminal device uses a different secret key to prevent all terminal devices from being cracked because one terminal device is cracked.

(3) Data integrity:

The digital digest technology with high security is used to ensure the integrity of data and prevent the message from being tampered with.

(4) Data legitimacy:

Key instructions use digital signatures to ensure the validity (non repudiation) of data.

(5) Key protection:

1) The generation, distribution and protection of the platform key are provided by the cipher machine to ensure that the platform developers cannot access the key;

2) The generation and protection of vehicle terminal key is provided by vehicle specification level encryption chip, ensuring that terminal developers cannot access the key.

2.2. Application requirements of in vehicle communication password

On the premise that the electronic and electrical architecture and bus topology of the original vehicle are not affected, based on the business scenarios and security threats of in vehicle communication and diagnosis, the password based security technical requirements to be implemented are as follows:

1) OBD equipment access certification requirements, realize the general scheme of OBD interface access certification based on the in vehicle gateway, effectively identify external illegal equipment and prevent the access and transmission of data in the vehicle. The technical realization is universal.

2) ECU security communication requirements, encrypted message transmission between ECUs, can identify, shield and process illegal devices or messages, and can effectively prevent replay attacks.

3) For ECU security rewriting requirements, the gateway and ECU equipment can identify the source of the updated software package and verify the integrity of the received updated files.

4) For ECU safety startup requirements, the gateway and ECU equipment can identify the source of the application program to be run and verify the integrity of the application program.

The gateway and ECU equipment can ensure the safe storage and integrity verification of key, business sensitive configuration and communication data to prevent illegal reading and tampering.

2.3. Vehicle/vehicle road communication password application requirements

V2V and V2I communications have many common security requirements, which involve hardware design, system permission management, operating environment security, resource security management, etc. In terms of password based security requirements, they are very similar to Car Cloud communications. The main security requirements are as follows:

The safety requirements of vehicle/vehicle road communication mainly include the following five aspects:

(1) Certification:

Vehicle road communication and vehicle vehicle communication generally use broadcast communication to send basic security information, so the receiver of the message (vehicle end or roadside unit) needs to verify the identity information of the sender (vehicle end or roadside unit) to ensure that only the information sent by the legal vehicle end or roadside unit can be received, while the sender does not need to ensure the legitimacy of the receiver's identity.

(2) Data confidentiality:

1) The data transmission process (terminal to terminal, terminal to roadside unit) is ciphertext transmission;

2) The key agreement mechanism ensures that each call uses a different key, and prevents the key from being cracked due to long-term use of a group of keys;

3) One computer and one secret shall be guaranteed. Each terminal device or roadside unit shall use different keys to prevent all terminal devices from being cracked because one terminal device or roadside unit is cracked.

(3) Data integrity:

The digital digest technology with high security is used to ensure the integrity of data and prevent the message from being tampered with.

(4) Data legitimacy:

Key instructions use digital signatures to ensure the validity (non repudiation) of data.

(5) Key protection:

The generation and protection of key of vehicle terminal or roadside unit are provided by vehicle specification level encryption chip to ensure that terminal developers cannot access the key.

3. Requirements for password application of Internet connected vehicles

3.1. Password application requirements

The basic requirements for password application of the network connected vehicle system are as follows: key equipment, communication network, sensitive data and other links shall be protected with password algorithm, mainly involving the following aspects:

(1) Car factory service platform

The vehicle factory service platform shall establish a security partition isolated from the external network. The physical isolation equipment such as access control of the security partition, the network isolation equipment such as gateway/gateway, the vehicle remote management server, the user management server, etc. shall conduct equipment authentication and establish a trusted security environment through password application. The equipment operators shall conduct authentication authorization and access control through password application. The data server in the service platform shall encrypt and protect key data through password application to ensure data security.

(2) Vehicle end equipment

Access equipment, on-board gateway, ECU and other key equipment at vehicle end shall adopt security protection measures based on password application.

(3) Mobile terminal

The application software in the mobile terminal that realizes remote vehicle monitoring and control functions shall establish a security mechanism through password application. Operators shall perform authentication and access control through password application.

(4) Open Network

Each network communication channel of the open network shall be protected by the password application to establish a safe channel.

Therefore, it is necessary to study the reference architecture of the network security of the intelligent connected vehicle system. Based on the results of risk analysis and in combination with the basic requirements of the Information System Password Application, the Password Module Security Technical Requirements and other standards, define the password technical requirements for the intelligent connected vehicle system, and develop the password technology and products that meet the needs of the intelligent connected vehicle field; The security system based on password application shall be established according to the basic requirements for password application of information system, and the password application strategy and password module suitable for the vehicle end shall be adopted, so that the service platform can reach the third level goal of Basic Requirements for Password Application of Information System.

In terms of password application, ICV should mainly carry out password application and security design from service platform, vehicle terminals (including T-BOX, IVI and bus gateway), mobile terminals and mobile networks. It mainly designs security functions from key security, identity authentication, data transmission/storage security, access control security and other aspects of secret products (such as terminals, cryptographic devices, service platform hosts, etc.) to solve terminal security, access security, transmission security and service security during business interaction between terminals and service platforms, and comprehensively improve the information security defense capability of the intelligent connected vehicle system.

In the process of system cloud, management and end password application, password security management is essential. The intelligent connected vehicle shall establish password security management, which realizes the full life cycle management of keys in the system, including key generation, storage, distribution, import, export, use, backup, recovery, archiving, destruction and other links for management and policy formulation. At the same time, during the life cycle of the key, the validity and compliance of the key should also be monitored in real time. Once invalid or illegal keys are found, they should be stopped and the system administrator should be prompted.

On the basis of the existing service platform, ICV shall establish a key management infrastructure, supervise the key management infrastructure, and manage the password resources and password applications of the ICV system. The new key management infrastructure includes symmetric key management subsystem, asymmetric key management subsystem, etc.

The ICV shall establish a digital certificate authentication system to provide a public key infrastructure solution for the ICV system. It mainly realizes the whole life cycle management of digital certificates, which is an important means to maintain the legitimate rights and interests of interested parties in the network and improve the network and information security guarantee capability. The digital certificate authentication system provides terminal user registration, audit, key generation, distribution, certificate issuance, certificate preparation and release and other basic functions for the intelligent connected vehicle system, and provides online certificate application and download, online certificate status query services for the application system, so as to provide certificate issuance functions for front-end vehicles, mobile terminals, third-party applications, background service equipment, etc. of the intelligent connected vehicle system, meeting the certificate authentication requirements, At the same time, through online certification, online certificate status query and other functions, the application system can more easily use the digital certificate authentication system to achieve security applications.

The ICV shall design the vehicle end device password module, which can provide the subsystem of password resource support for the security mechanism of the device. The password module of on-board access equipment is mainly composed of hardware security unit, software security unit and password service interface software. The hardware security unit supports cryptographic operation unit, random number generation, counter, memory and other components, while the software security unit supports cryptographic algorithm, random number generation and secure storage of keys, certificates, etc. Based on them, the cryptographic module provides cryptographic services to its upper security mechanisms and functions, mainly including encryption, decryption, integrity verification, key management and certificate management.

3.2. Password application requirements of automobile remote monitoring cloud platform

At this stage, the new energy vehicles sold on the market are mainly electric vehicles and oil electric hybrid vehicles, all of which use the battery+motor power system. However, the development and use time of new energy vehicles are relatively short, and related technologies and industries are still in an immature stage, resulting in endless incidents of spontaneous combustion and explosion of new energy vehicles. Based on the consideration of the reliability, safety, stability and durability of the new energy vehicle battery, it is necessary for the vehicle manufacturer to establish a new energy vehicle remote monitoring cloud platform to transmit the battery data information to the remote monitoring in real time. In this way, it is convenient for vehicle manufacturers and parts manufacturers to obtain the operation information of the vehicle and related parts, and define the focus of subsequent research and development of new energy products and remote OTA maintenance; Provide safe and reliable new energy vehicles for automobile users.The password monitoring process is shown in Figure 1:

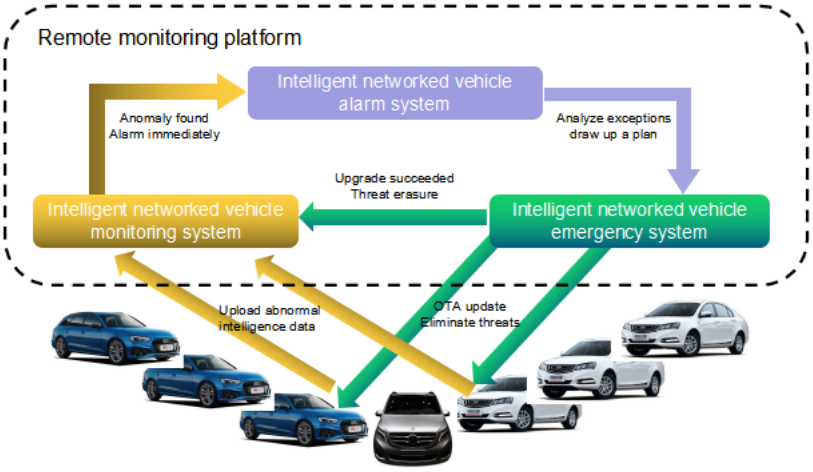
Remote monitoring platform
Intelligent networked vehicle alarm system
Anomaly found
Alarm immediately
Analyze exceptions
draw up a plan
Upgrade succeeded
Threat erasure
Intelligent networked vehicle monitoring system
Intelligent networked vehicle emergency system
Upload abnormal intelligence data
OTA update
Eliminate threats

Fig. 1 Password monitoring process

As shown in the above figure, we can use the current technically mature Internet of Vehicles system and big data mining, analysis and other related technologies to conduct real-time collection, real-time monitoring, data mining and analysis of vehicle holographic operation data, consumer driving habits and vehicle parts data for new energy vehicles on sale and in use, and timely report, handle and trace to the source when new energy vehicles are facing abnormalities, Reduce the possibility of subsequent similar accidents of new energy vehicles, which is also in line with the development trend of networking in the "new four modernizations of automobiles".

3.3. Application requirements of automobile smart grid password

The new energy vehicle (V2G) can be used as an auxiliary system in the smart grid to compensate the discontinuity and randomness generated by other new energy power generation systems (such as wind energy, tidal soft energy, solar energy, etc.), smooth the fluctuations of the grid, and ensure the stability of the grid voltage and frequency. As shown in the figure below, when new energy vehicles are connected to the power grid, the interaction and exchange of information flow and power flow between the two sides are completed under the unified dispatching and control of the power grid, and the energy stored by a large number of new energy vehicles is used as the buffer of the power grid and new energy. If the grid load is high, the new energy vehicle will feed back the surplus computer to the grid; If the grid load is low, the battery pack of new energy vehicles can be used to store excess electric energy. The benefits can include:

(1) Energy storage unit

As a mobile energy storage unit, new energy vehicles can serve as a buffer for other new energy power generation and provide auxiliary services for the grid when they participate in the grid dispatching.

(2) Discharge service

By providing discharge service to the power grid, users of new energy vehicles can get a certain reward according to the electricity charges to offset part of the cost of purchasing new energy vehicles and charging, so as to promote low-carbon development.

(3) Reduce costs

To ensure the safe and economic operation of the power grid can also reduce the operating cost of the power grid.

3.4. Automobile V2X password application requirements\

At this stage, the high-speed development of the Internet of Things covers more and more areas, and gradually includes the automobile and road infrastructure into the Internet of Vehicles system. As shown in the above figure, V2V (vehicle to vehicle), V2I (vehicle to infrastructure), V2P (vehicle to pedestrian) and other application methods are gradually taking shape, which will also solve the problems described above for new energy vehicles. After the V2I system can be accessed through the charging pile, the emergence of applications such as empty charging pile, booking charging, charging payment, etc. will bring more convenience to new energy owners, and remind the owners of the charging status through V2P, so as to provide the owners with real-time status of the car. At the same time, the rapid and real-time information exchange between these new energy vehicles and the outside world will also bring a large number of information security problems. It is necessary to establish a complete information security system to ensure the complicated identity authentication and data security.Figure 2 shows the requirements of intelligent connected vehicle V2X.

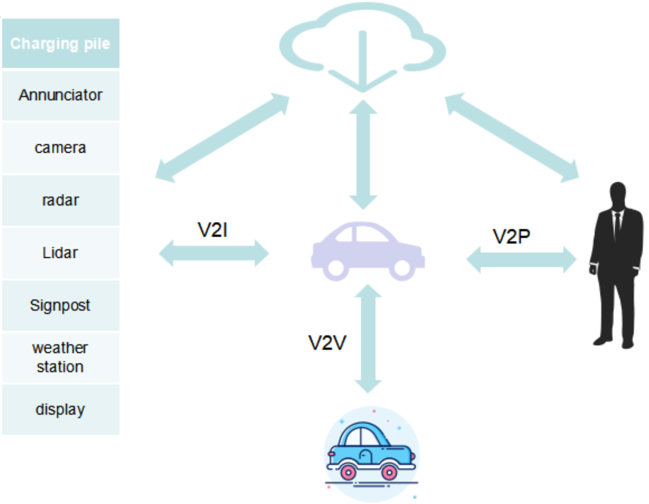

Fig.2 V2X demand of intelligent connected vehicle

At this stage, the gradually mature password technology can protect the confidentiality and integrity of information, meet the security requirements of V2X, and also provide security authentication for the identity and information source between information interchangers. It is the core technology and basic support to ensure the security of the Internet of Vehicles, and the most effective, reliable, and economic means to solve the security problems faced by new energy vehicles at this stage.

In order to ensure the security authentication and secure communication between devices in the V2X scenario, asymmetric encryption algorithms are used, and a reasonable PKI mechanism is established. HTTPS communication is built based on TLS/SSL protocol. While authenticating the authenticity of the identities of both parties, user data is encrypted to ensure that information is not eavesdropped, counterfeited, tampered, etc. during transmission, so as to provide privacy protection for communication between modules, Finally, the security of V2V/V2I/V2P direct connection communication is implemented by digital signature and other technical means. The digital identity authentication technology is applied to the Internet of Vehicles communication to achieve mutual authentication of various roles such as on-board equipment, roadside equipment and application service providers, ensure the authenticity of communication message sources, effectively prevent replay, man in the middle attack and identity counterfeiting. It provides key basic security guarantee for Internet of Vehicles applications such as safety early warning and efficiency improvement based on Internet of Vehicles communication technology.

4. Conclusion

The purpose of this paper is to solve the problems of insufficient connection between supply and demand information of domestic password industry chain in China's new energy and intelligent connected automobile industry, the efficient collaboration system of password products and service providers, automobile enterprises and evaluation institutions has not been established, and the application transformation ability and industrial support ability are insufficient. Through a detailed analysis of the demand for password applications, detailed discussions were carried out in multiple directions, from car, car cloud, car road to the password application and platform construction of ICV, laying the groundwork for the development of the password industry.

References

[1] Blockchain-Based Decentralized Trust Management in Vehicular Networks. [J] . Zhe Yang,Kan Yang 0001,Lei Lei 0004,Kan Zheng,Victor C. M. Leung. IEEE Internet of Things Journal . 2019 (2).

[2] A Blockchain-Based Privacy-Preserving Payment Mechanism for Vehicle-to-Grid Networks [J] . Gao Feng,Zhu Liehuang,Shen Meng,Sharif Kashif,Wan Zhiguo,Ren Kui. IEEE Network . 2018 (6).

[3] LNSC: A Security Model for Electric Vehicle and Charging Pile Management Based on Blockchain Ecosystem [J] . Huang Xiaohong,Xu Cheng,Wang Pengfei,Liu Hongzhe. IEEE Access . 2018.

[4] An Anti-Quantum Transaction Authentication Approach in Blockchain [J] . Yin Wei,Wen Qiaoyan,Li Wenmin,Zhang Hua,Jin Zhengping. IEEE Access . 2018.

[5] Blockchain-based secure firmware update for embedded devices in an Internet of Things environment [J] . Boohyung Lee,Jong-Hyouk Lee. The Journal of Supercomputing . 2017 (3).

[6] An Efficient Revocable Group Signature Scheme in Vehicular Ad Hoc Networks. [J] . Zhen Zhao,Jie Chen,Yueyu Zhang,Lanjun Dang. KSII Transactions on Internet and Information Systems（TIIS）:KSII Transactions on Internet and Information Systems（TIIS） . 2015 (10).

[7] A Framework for Secure and Efficient Data Acquisition in Vehicular Ad Hoc Networks. [J] . Khaleel W. Mershad,Hassan Artail. IEEE Trans. Vehicular Technology . 2013 (2).