World Scientific Research Journal Volume 8 Issue 11, 2022
ISSN: 2472-3703 DOI: 10.6911/WSRJ.202211_8(11).0039

Research and Design of Encryption Algorithm Security Protection Software in Automobile Industry

Chenxing Ouyang[1, a], Yue Qin[1] and Yinshu Wu[1]

[1]CATARC (Tianjin) Automotive Engineering Research Institute Co.,Ltd., Tianjin, China

[a]ouyangchenxing@catarc.ac.cn

Abstract

At present, the distribution of security algorithm file in the automobile industry is backward and inefficient. Based on the requirements of production and design of traditional automobile enterprises, this paper research on a combination of client/server software architecture and business to design an encryption algorithm security protection software to implement the encryption-decryption and remote transmission of security algorithm files in the automotive industry.

Keywords

Software architecture; Client/server; Security algorithm file; Automotive industry.

1. INTRODUCTION

The security algorithm files from the automotive electronics field are the core secrets of automobile enterprises. They have a high level of security requirements, leakage will cause a great safety accident. This paper uses the client/server software architecture and data encryption technology to design an encryption algorithm security protection software. This software can improve the efficiency of the engineer to invoke the secure access algorithm while meet the security requirements.

2. BACKGROUND RESEARCH AND REQUIREMENT ANALYSIS

2.1. Background Research

The DLL file is short for Dynamic Link Library, it contains a number of small piece of instructions or scripts that other programs can invoke to complete other tasks. Nowadays, automobile enterprises usually store their secure access algorithms into the dynamic link library file which called security algorithm file[1]. When engineers attempt to invoke a secure access algorithm, they directly use the security algorithm file as an input to the tasks, so that engineers do not have access to check the exact secure access algorithm code, in this way, automobile enterprises guarantee the security of the secure access algorithm.

2.2. Requirement Analysis

The way of traditional management for the security algorithm files is to save them in an offline data center. The distribution method of the security algorithm file is manual, engineer copy the target security algorithm file to an USB flash drive after they gets approved. They may use this security algorithm file on their work laptop or workstation. However, there is a risk of security algorithm file leakage on this process. If the security algorithm file leak to outside, people may apply the DLL file decompiling technology to extract the key secure access algorithm[2]. The process of replication consumes manpower and time which cannot meet the

ISSN: 2472-3703 DOI: 10.6911/WSRJ.202211_8(11).0039

actual business needs in time and cannot ensure the security of the security algorithm files stored on engineer's work devices. Therefore, the traditional process has great security risks and low efficiency.

For solving the above problems, this paper explores a software solution to digitize the distribution process in a safe way by using encryption and decryption technology and network communication security protocol. This software solution achieves the purpose of improving the efficiency of the engineers and keeping the files safely.

3. SOFTWARE OVERALL DESIGN

3.1. Software Architecture Design and Operating Environment

The encryption algorithm security protection software contains three major components: the server, the file management platform and the engineer invoking platform.

The server is the place to store all the security algorithm files. The file management platform is a browser/server based management platform to manage the distribution of the security algorithm files and all the client behaviors including decryption invoking and requesting. Finally, the engineer invoking platform is the key components to allow engineers to request and invoke the security algorithm files quickly and safely without operating the actual security algorithm files manually.

The file management platform runs on any server operating system, and should be able to be used on any major browser, including Firefox and Chrome. The B/S software architecture adapts well and is not restricted by the server operating system.

All the software data are stored in the enterprise security server. For satisfying the administrator and engineer 7x24 hours a year uninterrupted use requirements, the server needs to be online 24 hours and only allows abnormal shutdown no more than once a year. The server provides standard periodic data backup and archiving functions to cope with system downtime caused by uncontrollable factors. The file management platform communicates with the server through HTTPS protocol to ensure data security. The network communication bandwidth should be sufficient for 200 concurrent users in real time.

The engineer invoking platform uses the client/server structure, and is installed and run on the Windows operating system. The client must be compatible with the recent generations of Windows operating system. The secure storage mode of the engineer invoking platform may choose USB flash drive or local disk space based on different usage requirements.The running environments of both the file management platform and the engineer invoking platform requires to be connect to the network. The structure of the encryption algorithm security protection software system is shown in figure 1:

3.2. Software Users and Roles

According to the position responsibilities of engineers, the roles of users of this software system are divided into two categories: the administrator and the field engineers. The administrator has the function of permissions management and they can set the administrator permissions for other approved users, inquire user details or freeze the permissions.The administrator operates the file management platform, and their main responsibility is to manage the security algorithm files and the personnel permissions of each end.

The field engineers have normal permissions. They can only log into the engineer invoking platform and invoke security algorithm files for work requirements. One client-side only has one user and one account. The field engineers cannot log into other client-side and the file management platform.The user roles of the software is shown in figure 2:

ISSN: 2472-3703 DOI: 10.6911/WSRJ.202211_8(11).0039

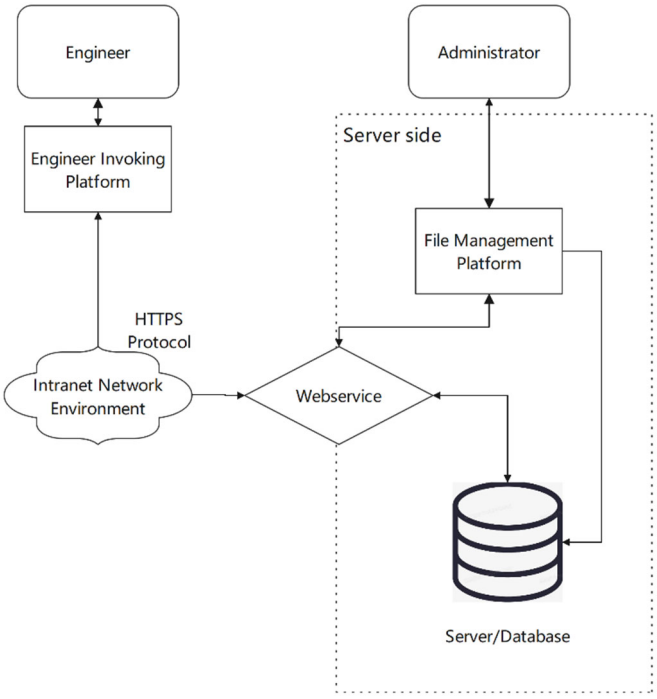

Figure 1. Software system structure diagram

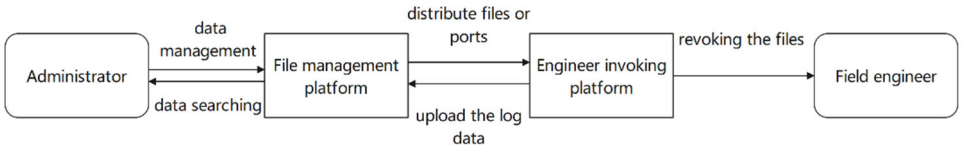

Figure 2. Software system structure diagram

4. SOFTWARE FUNCTION DESIGN

The functions of the file management platform mainly include: secure login, user management, security algorithm files management, log management.

Secure login: the personnel with the administrator permission can use their phone number for registration, secure login and password retrieval.

User management: this function displays and queries all information of the client users, and add a user, set the account and password for the new user. Modifying the information and reset the password for a user. Deleting a user and revoke an authorized user as well as the permission setting, adding a user type and configure corresponding permissions for the certain type.

Security algorithm files management: displaying the security algorithm file list and queries the security algorithm information. This function also can update the algorithm database and upload the new security algorithm file as well as delete expired security algorithm files.

Log management: displaying a list of users operation logs, including but not limited to the invoking user name, login time, and port name/number. The log searching: searching operation information by file name, user name and time.

The functions of the engineer invoking platform mainly include: secure login, personal information management, security algorithms and shortcuts.

Secure login: the engineer's user name and password are used to secure login to the platform. If they forget the password, they must contact the administrator to reset the password.

ISSN: 2472-3703 DOI: 10.6911/WSRJ.202211_8(11).0039

Personal information management: displaying personal information, and the password changing allows users to change passwords after security verification.

Security algorithm has two schemes:

1. Verifying the version of the local security algorithm library. If necessary, update the library after security verification, and then update the library for users to invoke. If no update is required, this function can be used after security verification.

2. Engineers enter the security algorithm file information to send the request. After security verification by the administrator, engineers can invoke the files.

Shortcut: this function saves and displays the records of the last five invoking made by a client user. They can click the shortcut to make a quick invoking.

5. SOFTWARE PROTECTION DESIGN

5.1. File Management Platform

A permission setting function is required for this platform and different permissions can access different functions. A client monitoring function is required to save client usage logs and check the operation records of users invoking DLL format files to ensure its security. The operations on the platform can be performed on the corresponding server side, external devices cannot connect to the server and modify any software data. All data that contained in the software cannot be invoked or copied by any external devices. Administrators who log in the platform will automatically log out without any operation within 5 minutes. The file management platform must encrypt the security algorithm files before distributing it to the client-side. At last, this platform should consider various virus attack and recovery options.

5.2. Data Transmission

The communication between database and the file management platform uses the HTTPS protocol to secure data. The software uses intranet network to complete the transmission between server-side and client-side, and the secure transmission specification follows the symmetric algorithm and AES standard data encryption algorithm to ensure the security, and the transmission process uses base64 encoding[3][4].

The public key cryptography mechanism and digital certificate technology are used to protect the confidentiality and integrity of information transmission, which is used to build a secure channel between client and server.

5.3. Engineer Invoking Platform

The engineers cannot access the encrypted security algorithm files directly. When the engineer invoking platform receives a security algorithm file, it should hide it and save it to a locally allocated secure storage space so that the engineers cannot modify the encrypted security algorithm files. The engineers also cannot copy these files to external devices. After the engineer invoking platform is uninstalled, everything in the local secure storage (including security algorithm files) should be erased. If an external USB flash drive is used for storage, all files in the storage space should be erased too.

6. THE IMPLEMENTATION SCHEME OF THE SOFTWARE PROTECTION

6.1. Security Algorithm Files Stored in The Cloud

The engineer invokes the security algorithm files through the cloud and does not directly save these files to their local operating system. After receiving the request to invoke the files, the administrator distributes the file port to the client-side. The engineer invoking platform does not need to directly manipulate the files, which ensures the security. In this way, the security

ISSN: 2472-3703 DOI: 10.6911/WSRJ.202211_8(11).0039

verification (secret key mechanism) between the client-side and the server-side is the core of the development. It also needs to ensure that the file management platform and the server are online 24 hours a day. The network conditions should match the number of potential users.

6.2. Security Verification Mechanism

The server communicates with the client-side using HTTPS protocol. The file management platform creates a secret key library and store it into the database. This secret key library generates a pair of public and private keys that matches a unique engineer account. When the engineer invoking platform sends a request to invoke the security algorithm files, the file management platform conducts security verification to the client.

In particular, after receiving the request, the file management platform sends a randomly generated string to the client-side. The client-side encrypts the string with the private key and sends it back to the file management platform, and it searches for the public key matching the engineer account in the library. If the two characters are consistent, the authentication process is complete. In the end, the file management platform send the security algorithm file port to the client-side for invoking[5]. The top level business flow diagram of this scheme is shown in figure 3:

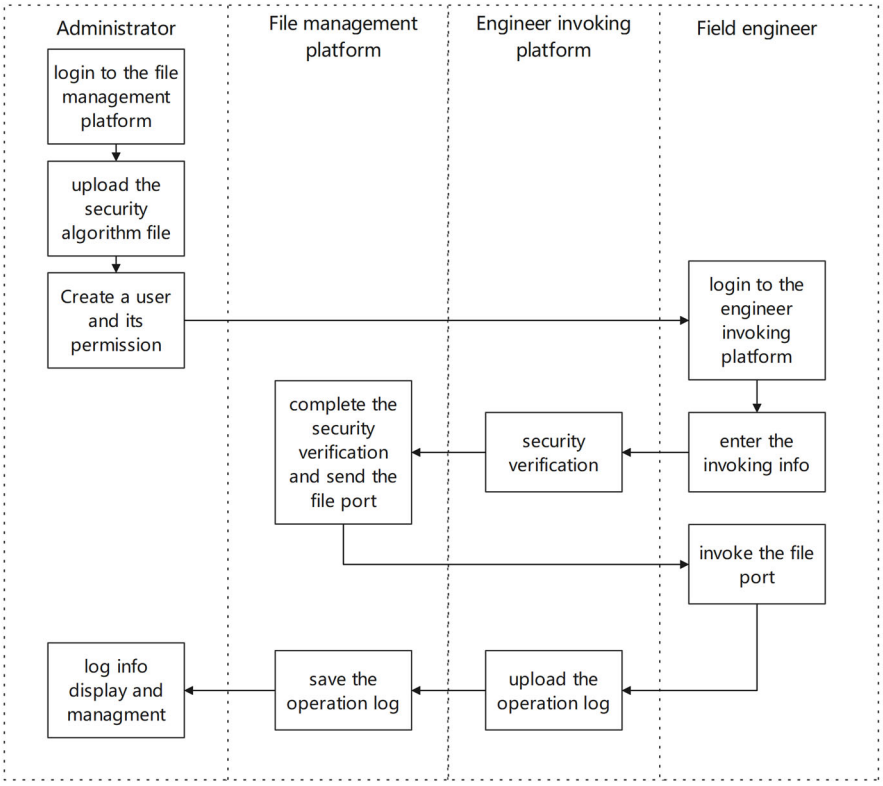

Figure 3. The top level business flow for cloud invoking scheme diagram

6.3. Security Algorithm Files Stored Locally

The file management platform encrypts the target files and sends them to the client-side through the intranet. The engineer invoking platform saves them locally. Engineers do not need to invoke the port through the real-time networking, but the file management platform initiates security verification irregularly to ensure safety.

The client-side can be securely stored locally in two ways. The first approach is to store the security algorithm files in the external USB flash drive of the engineer's laptop or workstation. Developing an unique external driver to unlock the specified USB flash drive which is only for

ISSN: 2472-3703 DOI: 10.6911/WSRJ.202211_8(11).0039

the client-side to invoke the files but these files cannot be independently accessed by the outside environment. The benefits for this approach is that it saves the local storage space, but the engineer's machine must have at least one USB interface.

The limitation of USB interface can lead to second approach. The engineer invoking platform allocate an exclusive local disk space(large capacity custom format file generation). Then setting up a file system under the custom space saves the security algorithm files and only for client-side to invoke. The visibility of the custom space from the outside is an large custom format file. The top level business flow diagram of this scheme is shown in figure 4:

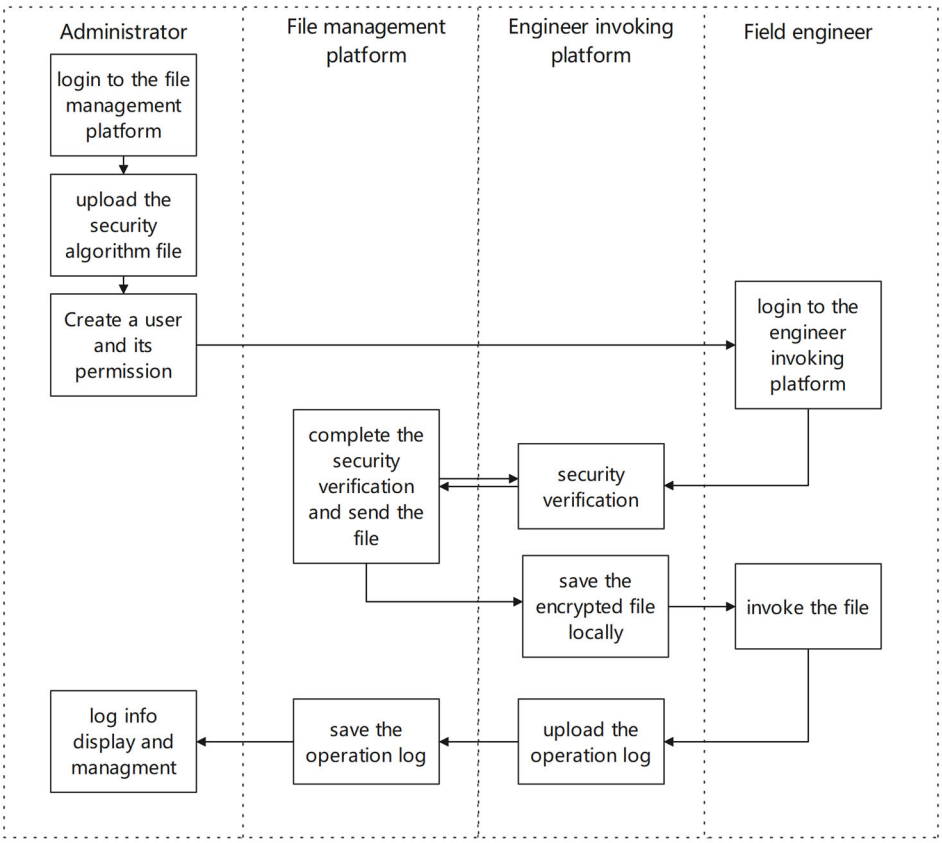

Figure 4. The top level business flow for local invoking scheme diagram

7. CONCLUSION

Combining with the engineer's hardware environment and work needs, this paper provides a variety of safety protection scheme for the automobile enterprises to develop customized security software. As specified in the preceding chapters, this unique software architecture either hide the security algorithm files into the shell file or store them in the server-side, which the administrator have access to manage the port distribution process. In conclusion, through the research of this paper, the automobile enterprises could use this software solution to improve their work efficiency and safety at the same time.

REFERENCES

[1] Li Mengyin,Ge Xinye. Application of Electronic Technology in Automobile Safety System[J]. Journal of Physics: Conference Series,2021,1948(1).

ISSN: 2472-3703 DOI: 10.6911/WSRJ.202211_8(11).0039

[2] Mohd Amir Siddiqui,M Akheela Khanum. Implementation of Security Algorithm for Data Security in Cloud Computing[J]. International Journal of Innovative Technology and Exploring Engineering (IJITEE),2019,8(5).

[3] Muthavhine Khumbelo Difference,Sumbwanyambe Mbuyu. Preventing Differential Cryptanalysis Attacks Using a KDM Function and the 32-Bit Output S-Boxes on AES Algorithm Found on the Internet of Things Devices[J]. Cryptography,2022,6(1).

[4] LiliWang,JianguoWu. Study on Computer Software Encryption Based on AES and RSA Combinational Algorithm[J]. Journal of Residuals Science & Technology,2016,13(6).

[5] Ping Luo,Mumtaz Majid. An Improved Cryptanalysis of Large RSA Decryption Exponent with constrained Secret key[J]. International Journal of Information and Computer Security,2021,14(1).