Research on Security Framework of Mobile Application in Dispatch and Control Domain of Power Grid

XU Jiahui¹, YU Hongyuan², WANG Gang¹, WANG Zi³, BAI Jingjie¹, WU Jiang¹, YAN Xiaona¹ and JIA Zilei¹

¹Beijing Kedong Electric Power Control Company Limited, Haidian District, Beijing 100192, China
² Central China Power Grid Company Limited, Wuhan 430077, Hubei Province, China
³ State Grid Tianjin Electric Power Company, Hebei District, Tianjin 300010, China

Abstract. The rapid development of mobile Internet technology and the wide spread of smart terminals have brought opportunities for the transformation of power grid business model. Compared to the non-real-time information, the real-time and running data of dispatch and control domain is easy to be intercepted and cracked. To solve this problem, this paper presents a new approach to mobile application security framework for the power grid control field. It is to realize secondary encryption by using the method of MD5+AES mixed encryption algorithm and combining the time stamp in real-time data transmission process. At the same time it is to prevent cross-border operations and brute force by using Token authentication and Session technology. China EPRI safety test results show that the application of the framework significantly improves the integrity, safety and reliability of real-time data in power grid control.

1 INTRODUCTION

In recent years, with the promotion of mobile operating systems such as IOS, Android, and so on, the intelligent terminal has been popularized quickly. Mobile application is gradually integrated into people's daily life, and penetrated into the power grid which is closely related to people. The Power Grid Corp departments recognize the importance of mobile services to the innovation and development of all kinds of business, and build mobile applications, and continuously improve the company’s production and operation efficiency and quality service level.

Mobile application brings convenience to the smart grid, however, it also causes a series of security challenges[1]. Security index of Existing mobile applications cannot meet the interaction regulatory requirements of running data in dispatch and control domain of power grid.

The running data in dispatch and control domain of power grid is real-time and interactive. The encryption methods of traditional mobile applications are weak. At the same time, taking into account the core status of the dispatch and control in power grid, running data out of control will not only cause serious economic losses and may endanger social security.

In view of the above problems, a security framework for the mobile application in domain and control of power grid is proposed. The framework takes full consideration of the problem of security.

2 SECURITY FRAMEWORK OF MOBILE APPLICATION IN DISPATCH AND CONTROL DOMAIN OF POWER GRID

The security framework of mobile application described in this paper is based on the ENMIP, short for the external network mobile interactive platform. The ENMIP supports the development, management and operation of power grid. Considering the characteristics of running data in dispatch and control domain, the protection security of the ENMIP cannot meet its requirements. Therefore, the security framework proposed in this paper is to carry out two protection on the original safety guarantee, and ensures the confidentiality of data, and prevents software from being tampered.

The security framework of mobile application forms a rigorous security loops in the whole process. In the process of data flow, the mixed encryption technology is used to encrypt the real-time data. And the data is circulated in the form of data cipher-text, which ensures the safety of data interaction. The mobile application terminal uses Token authentication and Session mechanism to prevent cross border operation and violent cracking. These mechanisms can ensure the application rights and data effectiveness. The key technologies used in the real-time and running data transmission process and application are described in detail.
3 THE TRANSMISSION SECURITY OF RUNNING DATA

In the process of real-time and running data transmission, the hybrid encryption algorithm is used to ensure data security. The hybrid encryption algorithm is based on the optimized MD5 (Message-Digest Algorithm 5) and the optimized AES (Advanced Encryption Standard). The real-time and running data is encrypted two times by the hybrid encryption method. It circulates in the form of cipher-text in the whole process, which greatly reduces the risk of intercepting and breaking and ensures data security.

3.1 IMPROVED MD5 ENCRYPTION ALGORITHM

MD5[2] algorithm has an important application in data encryption, such as digital signature, identity authentication and so on. It is used to ensure the integrity and consistency of information in network transmission. In the MD5 algorithm, we need to pass the following 4 processes [3-4]:

1) data filling: The message is filled with data so that the length of the message is 448 to 512. According to this formula, the length of the data will be extended to N*512+448.

2) message supplementing: After the first step is completed, the result is filled with a 64 bit binary representation of the length of the information. The information byte length is N*512+448+64, that is (N+1)*512.

The optimization algorithm is similar to the original algorithm. It is the improvement of the third step and the fourth step of the original algorithm.

3) data preparation: 8 constants (A, B, C, D, E, F, G, H) are used to compute the information summary. A=0x01234567, B=0x89abcdef, C=0xabcdef, D=0xedcba01, E=0xabcdef01, F=0xedcba01, G=0xedbca01, H=0x67543210, G=0x67543210. The 8 constants which is A, B, C, D, E, F, G, H are assigned to 8 variables which is a, b, c, d, e, f, g, h. 4 functions—F(X,Y,Z)=(X & Y) | ((~X) & Z); G(X,Y,Z)=(X & Z) | (Y & (~Z)); H(X,Y,Z)=X ^ Y ^ Z; I(X,Y,Z)=X ^ (Y ^ ~Z).

4) 4 round operations: Choose 3 variables from a, b, c, d, e, f, g, h and do a nonlinear function. And then the results will be added to the ninth variable Mj (a subgroup of the text) and a constant Tj. And then the result will be shifted to the left with an indefinite constant s, added one of a, b, c, d, e, f, g, h. Finally replaced a, b, c, d, e, f, g, h of the results.

Let Mj denote the j subgroup and Tj represent the integer part of 232×abs(cos(x)). <<<< represents moving to the left s bit. The following function is used for the round operation:

FF(a, b, c, d, e, f, g, h, Mj, s, Tj) represents
a=b+=(c +d +e +I(f, g, h)+ Mj +Tj)<<<<)

Finally replaced a subgroup of the text) and a constant results will be added to the ninth variable Y) | ((~X) &Z); G(X,Y,Z)=(X & Z) | (Y & (~Z)); H) are used to compute the fourth step of the original algorithm.

3.2 OPTIMIZED AES ENCRYPTION ALGORITHM

AES (advanced encryption standard) is an iterative and symmetric cipher. The encryption process is on a two-dimensional byte array called state[5]. AES algorithm is composed of 4 different functions, namely SubBytes(SB), ShiftRows(SR), MixColumns(MC) and AddRoundKey(AK) [6]. A lot of shift operations are used in the process of round function encryption, which is time-consuming.

In order to improve the speed of the algorithm, taking AES-128 as an example, let put SR and MC merge. The state after the SB is matrix as:

$$S = \begin{bmatrix} S_0 & S_1 & S_2 & S_3 \\ S_4 & S_5 & S_6 & S_7 \\ S_8 & S_9 & S_{10} & S_{11} \\ S_{12} & S_{13} & S_{14} & S_{15} \end{bmatrix}$$

After SR, the state is:

$$S' = \begin{bmatrix} S_0' & S_1' & S_2' & S_3' \\ S_4' & S_5' & S_6' & S_7' \\ S_8' & S_9' & S_{10}' & S_{11}' \\ S_{12}' & S_{13}' & S_{14}' & S_{15}' \end{bmatrix}$$

so, $$S' = \begin{bmatrix} S_0' & S_1' & S_2' & S_3' \\ S_{12}' & S_{13}' & S_{14}' & S_{15}' \end{bmatrix} \begin{bmatrix} S_0 \ S_1 \ S_2 \ S_3 \ S_4 \ S_5 \ S_6 \ S_7 \ S_8 \ S_9 \ S_{10} \ S_{11} \end{bmatrix}$$
According to the characteristic of matrix multiplication, the above formula can be written as a form of vector transformation.

\[
\begin{bmatrix}
S_0' \\
S_1' \\
\vdots \\
S_{14}' \\
S_{15}'
\end{bmatrix} = 
\begin{bmatrix}
02 & \ldots & 01 \\
\vdots \\
00 & \ldots & 00
\end{bmatrix}
\begin{bmatrix}
S_0 \\
S_1 \\
\vdots \\
S_{14} \\
S_{15}
\end{bmatrix}
\]

The SR and the MC are combined. The AES encryption process is shown in Figure 2.

3.3 MIXED ENCRYPTION

Both MD5 encryption algorithm and AES encryption algorithm are quite mature algorithms. MD5 encryption algorithm is an irreversible encryption. The encryption speed of AES is fast. And the amount of calculation is small. According to the characteristics of these two algorithms, we study the hybrid encryption technology, and combine the advantages of the two. The flow chart of the hybrid encryption technology is as follows:

![Mixed encryption technology and decryption flow chart](image)

In the whole process, data is transmitted in the form of data cipher-text. The improved MD5 algorithm has inherited the stability and reduced the collision. The optimized AES encryption algorithm can reduce a calculation step and shorten the encryption time. The use of mixed encryption can guarantee the integrity, timeliness and security of the running and real-time data.

4 APPLICATION SECURITY

Identity authentication plays a very important role in the whole security system. The key technologies used in identity authentication are the Session mechanism and the Token authentication mechanism.

The Session mechanism uses a scheme to maintain a state on the server side. When the program needs to create a Session for a client request, the server first checks whether the client request has included Session ID. Session is the only identification information that maintains communication with the server side during the entire operation of the same user.

Token is the technology to verify the user’s identity and ensure the user’s safe login. Token has three parts: header, payload and signature. The schematic diagram of the generation of Token is shown in Figure 4.

![Schematic diagram of Token generation](image)

Based on the above two technologies, this paper uses combination of Session and Token to achieve identity authentication. In the mobile application, Session and Token authentication is to ensure that the same user opens an interface. The combination of two technologies not only prevent repeated information submission and prevent cross site request forgery, but also prevent application from being brute force and protect application security.

5 FRAMEWORK TEST

According to the mainstream smart mobile phone operating system, China EPRI respectively test the security framework of mobile application on the deployment of IOS system and Android system. The contents include security function test, penetration test, and test code. It is worth mentioning that the test has passed.

The test results show that this framework significantly improves the integrity, security and reliability of real-time and running data interaction in dispatch and control domain of power grid.
6 CONCLUSIONS

This paper presents a security framework of mobile application oriented dispatch and control domain. The framework uses a mixed encryption method to encrypt real-time and running data. In the whole process, data is transmitted in the form of data cipher-text to ensure the storage security and transmission security of the data. The framework uses Session Token to ensure the security of the application, and prevents the application from being transacted and violent. The test results given Chinese EPRI indicates that the framework is proved to significantly improve the integrity, reliability and safety of real-time and running data. It has a certain value of research and promotion.

REFERENCES

1. Xu Zhen. Mobile Application Security Technology for Smart Grid[J]. Automation of Electric Power Systems, 2012, 16(36): 82-86.
2. Wang Yanbo, Xue Tong. Applied cryptography [M]. Bei Jing: China Machine Press, 2013.
3. Jia Xiaoqiang, Improvement of MD5 encryption algorithm and its application in antivirus software [J]. Electronic Design Engineering, 2015, 23(23): 26-29.
4. Mao Yi, Chen Na. Research and Improvement of MD5 Algorithm [J]. Computer Engineering, 2012, 38(24): 112-114.
5. Wang Changlin, Wu Bin. A Scheme of Data and Encryption Algorithms Based on AES and Improved ECC[J]. Science Technology and Engineering, 2009, 18(9), 5379-5382.
6. Wang Ying, Improvement and implementation of AES encryption algorithm [J]. Computer Security and Maintenance. 2010, (17): 84-86.
7. Zhan Lindan. The Research and Application of Token-based unified authentication system[D]. Nan Jing: Zhongshan University, 2010.