Data Security Isolation and Exchange for Smart Grid

Data Security Isolation and Exchange for Smart Grid

Yu Chen[1,*], Yan Chen[1], Minjie Zhu[1] and Naiwang Guo[2]

[1]Department of Science & Technology and ICT, State Grid Shanghai Municipal Electric Power Company, Shanghai, China

[2]Electric Power Research Institute, State Grid Shanghai Municipal Electric Power Company, Shanghai, China

*Corresponding author e-mail: chenyu@sh.sgcc.com.cn

Abstract. With the arrival of the big data era, data security is getting more and more important especially in many critical fields such as smart grid. At the same time of requiring strict data isolation, it also needs to exchange a lot of data between different security zones. How to implement the smooth data isolation and exchange becomes the focus of numerous data security researchers. Aiming at the data security requirement of smart grid, this paper designs a data security isolation and exchange scheme to ensure the data security in smart grid. The proposed scheme includes three modules: internal network host processing unit, data isolation and exchange unit and external network host processing unit, and provides four functions: user identity authentication, data access control, protocol stack parsing and SQL statement filtering. The implement details of four functions are elaborated. The data security isolation and exchange scheme provide a very useful means to enhance the data security of smart grid.

1. Introduction

With the arrival of the big data era, data has gained wide application and created tremendous value in many fields. But at the same time, the security of data has also brought a great impact on these fields. Data security is an important issue related to the military, political, economic and energy of a country, which has attracted more and more attention. Taking smart grid as an example, smart grid is an important infrastructure for a country. Data security is one of the important guarantees for smart grid to supply power reliably and smoothly. It is directly related to the social stability of a country, the development of industry and the improvement of people's life. Once smart grid happens with some data security problems, it will endanger the safe and stable operation of smart grid, and the loss and the impact will be incalculable.

The main contributions are as follows: Firstly, this paper discusses some key technologies of data security isolation, including security gate, depth detection, identity authentication and access control. Secondly, this paper designs a detailed data security isolation mechanism, which provides an effective technical scheme for data security protection in smart grid.

The rest of this paper is organized as follows. This paper begins with the related works in Section 2 and design a data security isolation and exchange scheme for smart grid in Section 3. Finally, the conclusion is drawn with discussion in Section 4.

2. The Related Works

External or human factors lead to frequent leakage of confidential data, which brings great losses to data owners. To solve this problem, data security isolation and exchange technology has become a

research hotspot of many researchers[1,2]. In the 1990s, the United States and Israel took the lead in putting forward network isolation technology for the protection of their private networks. After four generations of technology development, the network isolation technology has reached the fifth generation, that is the technology of secure isolation gateway. Based on the data isolation of client and server, the integrity and security of forwarded data are checked by protocol conversion, virus detection and killing technology, so as to ensure the security and reliability of forwarded data and provide effective security protection of confidential information[3,4]. Based on the in-depth researching of security isolation gate technology, a large number of researchers have proposed to use security isolation gate technology to solve some practical problems. Xu et. al. put a secure desktop technology forward by combining virtualization and security isolation gateway, which is mainly used for securely exchange and sharing of data between internal networks and external networks[5]. Sun et. al. applied this secure desktop technology in 3G-based mobile office to guarantee the security of real-time information transmission and exchange[6]. Zhang combined firewall technology with security isolation gateway to build a security network for program development[7]. Hu used this security network to download various confidential data[8]. In addition, Wen et al. used a virtual isolation gates to achieve the isolation of multi-tenant data centers and protect the security of tenants' commodity information[9]. Shin et al. proposed to achieve secure information sharing by combining security protocols and isolation gates[10].

3. A Data Secure Isolation and Exchange Scheme for Smart Grid

Regarding the data security of smart grid, a data isolation and exchange scheme that consists of internal network host processing unit, data isolation and exchange unit and external network host processing unit is designed as shown in figure 1. Both internal network host processing unit and external network host processing unit adopt special mechanisms of identity authentication and access control to form a trusted architecture. Data isolation and exchange unit establishes a data channel according to the business requirements and security strategies, and parses the transmission protocol and filters the SQL statement in the data channel. It only allows the business data that satisfies the security strategies to be exchanged and does not allow any other data to be transmitted.

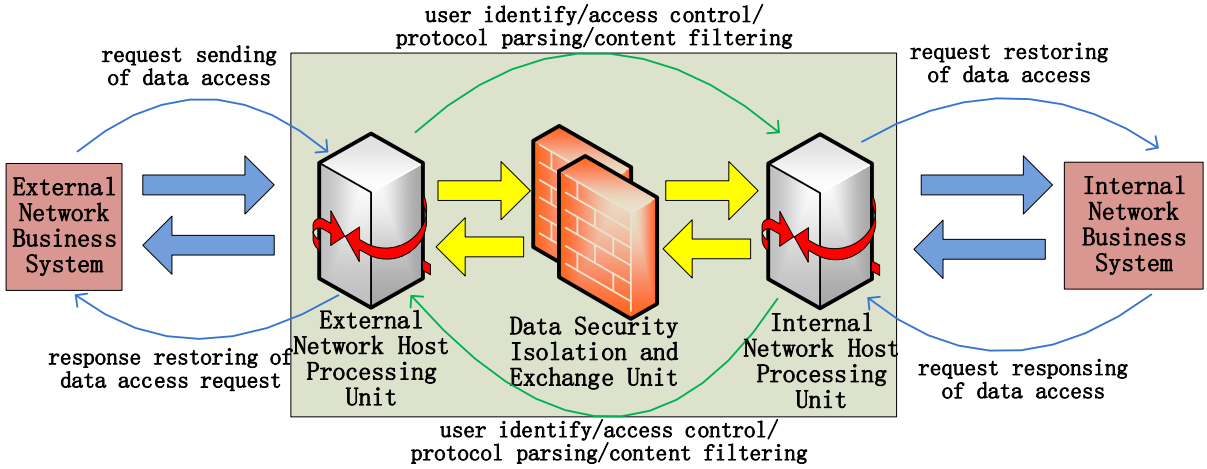

Figure 1. A data security isolation and exchange scheme of smart grid.

3.1User Identity Authentication

In order to enhance the safety of username and password against network attacks, the username and password will be encrypted in the process of user identity authentication. The procedure of user identity authentication is shown as figure 2.

Step 1: User sends a login request to the business server with single sign-on mode and inputs his/her username and password. The username and password will be sent to the authentication server.

Step 2: After receiving the username and password, the authentication server will use SHA256 algorithm and random number strategy to encrypt and store the username and password in a database, which ensures that the encrypted username and password will be not repeated and reversed. This way avoids the phenomenon of plaintext transmission and violent cracking. In addition, the information of username and password can only be modified by administrators and user.

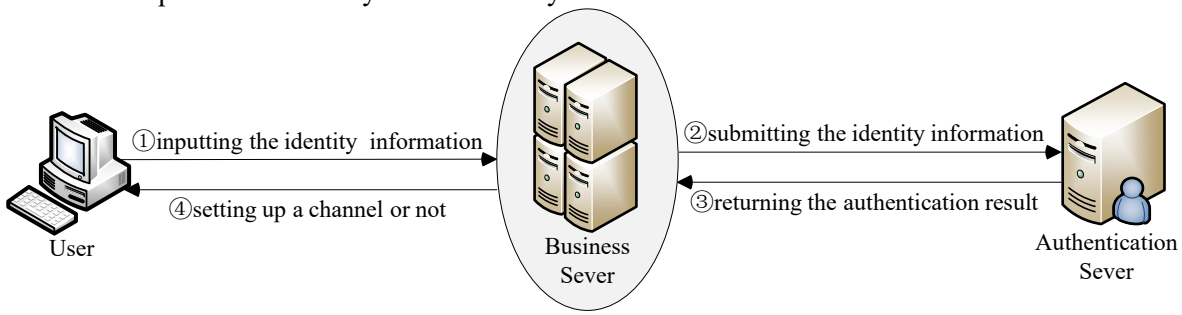

Figure 2. The procedure of user identity authentication.

Step 3: The authentication server will verify the correctness of username and password. If the username and password are correct, the authentication server will return an acknowledgement reply and the login succeeds. If the login fails, the user will be prompted for wrong username and password and asked to re-enter the username and password. If the successive login failure number exceeds a given value, the user will be locked and prompted to ask for administrator to unlock or wait for a specific time to automatically unlock by the authentication server. Further, the successive login failure number of the user's IP address will be judged. If the successive login failure number of the user's IP address exceeds a given value, the user's IP address will be locked and needed to unlock by administrator. All user login information (including username and IP address) will be recorded in a log file to build a black-and-white list of users.

Step 4: The process of user identity authentication is finished and a channel will be set up or not according to the authentication result.

3.2Data Access Control

The data security isolation and exchange scheme provide strict access control rules. These access control rules register all information of client and server about IP, port and MAC address, and make the corresponding association on this information. Only those access requests that satisfy the associated access control rules can pass through the data security isolation and exchange unit. The procedure of access control through role matching is shown in figure 3.

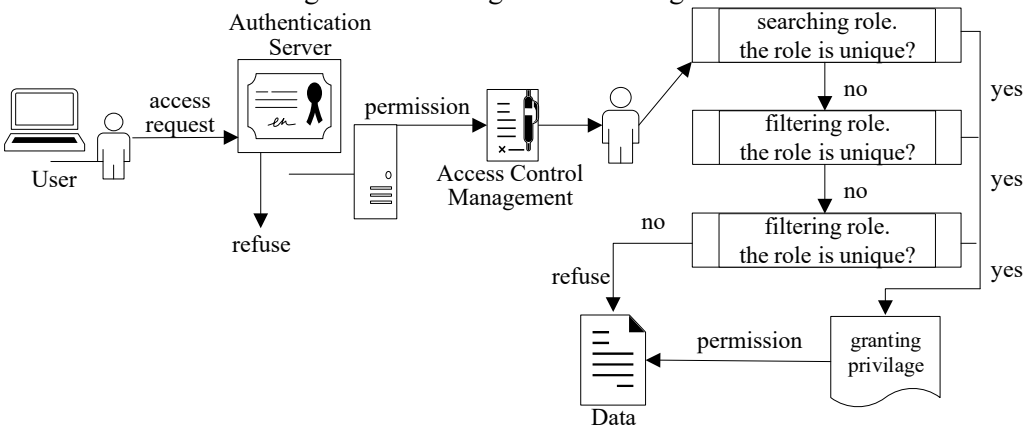

Figure 3. The access control process of RBAC model.

Step 1: User access request. User sends an access request to the authentication server. The authentication server checks the identity information sent by the user. If the identity information matches, the access request is allowed. Otherwise, the access request is refused.

Step 2: User role matching. According to the different tasks, users get different privileges. RMT-RBAC access control mechanism matches the corresponding roles for users. Firstly, the minimum set of roles with corresponding privileges is selected according to the role searching algorithm. If the minimum set of roles is unique, then goes to step 3. Otherwise, it is filtered according to the security requirements and security strategies of the specific business. If the filtered set of roles is unique, then goes to step 3. Otherwise, it will be filtered further based on the inheritance relationship number of the filtered set of roles, and goes to step 3.

Step 3: Access privileges granting. The filtered roles are matched to the corresponding users, and the users get the corresponding privileges of their roles.

Step 4: Data access. The user accesses the corresponding data according to their obtained privileges.

3.3Protocol Stack Parsing

After receiving a message, the data security isolation and exchange unit needs to analyse the protocol of the message, e.g. TCP/IP and TNS. It is critical to construct an efficient protocol parsing module.

3.3.1TCP/IP Protocol Parsing TCP/IP protocol parsing can be implemented by using a third-party protocol analysing mechanism such as *LibNIDS*. *LibNIDS* is a professional programming interface library and provides a basic framework for network intrusion detection, so that developers can do further development to quickly build a network intrusion detection system.

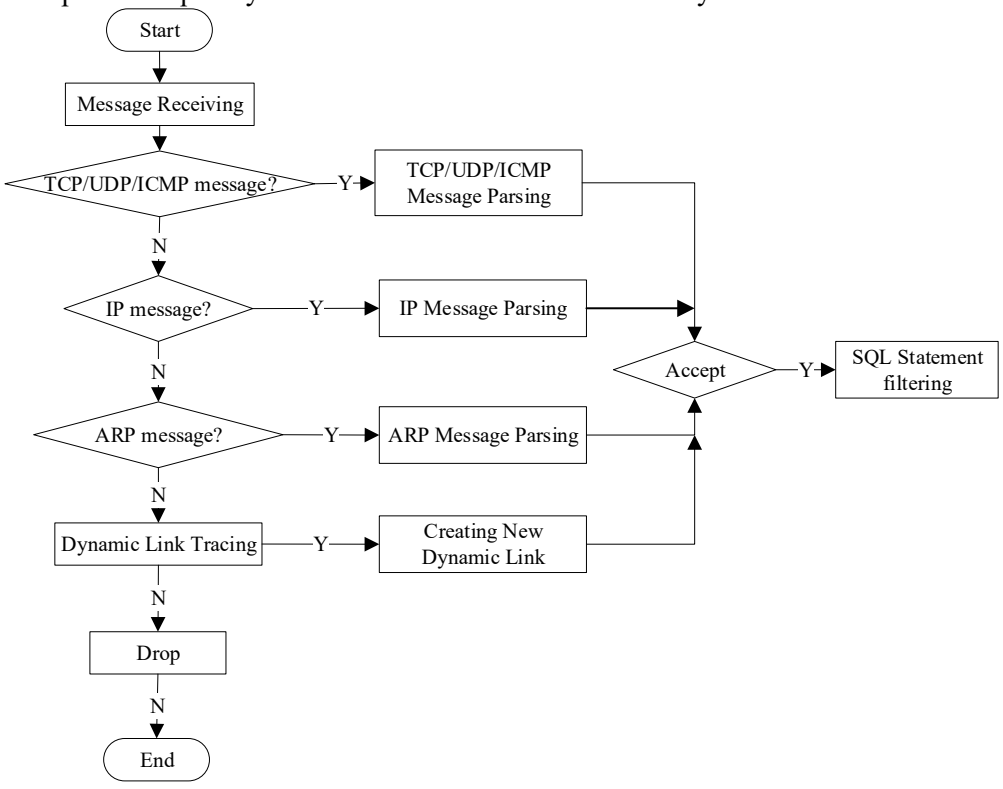

Figure 4. The procedure of TCP/IP, ARP protocol parsing.

LibNIDS implements the underlying functions of network intrusion detection that enable developers to only focus on the development of high-level functions. *LibNIDS* is implemented based on *Libpcap* and *Libnet* by imitating the TCP/IP protocol part in Linux 2.0.x kernel and has the same advantages as *Libpcap* and *Libnet* such as strong portability, high efficiency, high reliability and simple use. The main functions of *LibNIDS* include packet capture, IP fragmentation reorganization, TCP data stream reorganization, port scan attack testing and heterogeneous packet testing. *LibNIDS* uses the function of *Libpcap* to capture data packets. It can set filtering rules and specify the capture of interested data packets. IP fragment reassembly is an important part of *LibNIDS*, which is

implemented by imitating IP reassembly in Linux kernel. *LibNIDS* provides TCP data stream reorganization function, which *Libpcap* does not have. By using TCP data stream reorganization, various application layer protocols based on TCP protocol can be analyzed. In addition, *LibNIDS* also provides the function of detecting TCP port scanning attacks and abnormal data packets, which is the basic function of Intrusion Detection System. The procedure of TCP/IP protocol parsing is shown as figure 4.

- Receiving TCP setup, shutdown, data and other messages of TCP reorganization module.
- Receive new TCP messages, generate analysis threads according to TCP-stream structure, and submit parameters to analysis threads, including TCP-stream pointer, protocol processing callback function. Receive shutdown message and notify protocol analysis thread to quit. Receive data messages, analyze application data, and submit the current IP packet information and application data in TCP-stream structure to the analysis thread if it contains completion message information, otherwise discard it.
- Return processing results to flow parsing module.

3.3.2TNS Protocol Parsing TNS is a communication protocol between server and client in an Oracle system. TNS uses the protocol of TCP/IP, TCP/IP with SSL, name pipes and IPC to transmit data. TCP/IP transmits data in plaintext. TNS protocol parsing can be implemented according to its 8-bit message header structure and content.

Table 1. the structure of parsing rules.

The Header of Parsing Rules							
behaviour	protocol	source IP	source port	direction	mask bit number	destination IP	destination port
The Option of Parsing Rules (The Option Content of Parsing Rules)							

The data security isolation and exchange scheme provide many protocol parsing rules, and the structure of parsing rules is shown in table 1. This structure includes two logic part: the header of parsing rule and the option of parsing rule, and each appropriate parsing rules can be read according to this structure. The header of parsing rules includes the behaviour, protocol, source and destination IP, source and destination port, direction and mask bit number, the option of parsing rules includes the network alert information and the messages content under filtering. The connection, disconnection and redirection of communication link can be identified and the state of data channel by checking the first bit of message header structure and content can be analysed. After finishing these operations, the data access statement can be restored completely by restoring the complete data content of TNS protocol.

3.4SQL Statement Filtering

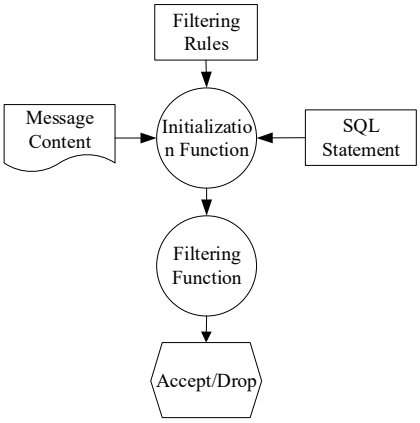

Figure 5. The procedure of SQL statement filtering.

The data security isolation and exchange scheme provide also many SQL filtering rules. The input parameters of SQL statement filtering are the pointers of message content and SQL statement, and the output of SQL statement filtering is Accept or Drop.

Firstly, all business data, default filtering rules and system log should be formed into a configuration file and downloaded to the data security isolation and exchange unit for the core program to control the IP, MAC address and port information of the communication process.

Secondly, the initializing function reads the filtering rules configured by a remote management software, analyzes the message contents and updates dynamically the filtering rules library. The message content will be filtered all special tag characters out to prevent various attacks on data message. If users access the business data with a mobile terminal, it should be registered into the data isolation and exchange unit beforehand to facilitate administrators to monitor and restrict its access to the business data.

Finally, the SQL statements are analyzed by the SQL filtering module. The SQL statement is formatted and filtered by calling the appropriate rules with some specified search algorithms, and the filtered result is used to judge whether the data message will be still transmitted. The filtering function analyzes the SQL statements submitted by the TNS protocol parsing module, matches the filtering rules according to the security policies and returns the filtering result.

4. Conclusion and Future Work

Data security isolation and exchange technology is an important security guarantee between internal networks and external networks. It includes not only traditional data fragmentation and reorganization, protocol transformation, cryptography, keyword filtering, authentication and audit, but also data identification, log audit and other fields. Based on the research of data security isolation and exchange technology, this paper designed a data security isolation and exchange scheme, which can effectively solve the problem of data security isolation and exchange between internal network and external network, and realized a broader and deeper active defence of data security in the interactive environment of smart grid.

References

[1] Ji J, Dun J, Shi N, et al. (2014) Design and implementation of border protection system based on secure isolation. Network Security Technology & Application, 8(1): 16-18.
[2] Yu T, Lin B S, Chang Y. (2017) Eight-way radial power splitter including ring-shape isolation network. Electronics Letters, 24(1): 1587-1589.
[3] Li M, Fei Y G. (2004) Research on Physical Isolation Technology. Computer Engineering, 30(4): 104-106.
[4] Yao R, Wu J, Zhou C L. (2010) Data synchronization method based on physical isolation in mobile applications. Computer Engineering and Science, 1(1): 10-12.
[5] Xu S B, Wang Q R. (2017) Design and Implementation of Multilevel Security Virtual Desktop System [J]. Computer and Network, 3(1): 65-71.
[6] Sun Q H, Liu D Q. (2013) Application and discussion of network isolation technology in 3G mobile office. Computer Science, 40(6A): 381-383.
[7] Zhang S B. (2003) Secret-related network security isolation solution[J]. Information security and communication secrecy, 2(1): 48-51.
[8] Hu Z G. (2014) Network Security Solution for Downloading Gate-based Data. Science and Technology and Enterprises, 22: 57-57.
[9] Wen Z C, Wang Y S, Bai Y H. (2015) Research on application of virtualization technology in electric power industry. Information Technology and Informatization, 9: 222-223.
[10] Shin D H, Koo J, Yang L, et al. (2013) Low-complexity secure protocols to defend cyber-physical systems against network isolation attacks. In: First IEEE Conference on Communication and Network Security. Washington DC. pp. 91-99.