Key technologies of data security protection system for power grid

Yu Zhang$^1$ and Xichao Zhao$^2$

$^1$NARI Group Corporation, Nanjing, Jiangsu, 210003, China
$^2$NARI Group Corporation, Nanjing, Jiangsu, 210003, China
*Corresponding author’s e-mail: zhang_yu@sgepri.sgcc.com.cn

Abstract. The extensive application of a large number of intelligent terminals and advanced communication technologies in the smart grid has greatly increased the pathways in which various sensitive business data are destroyed and leaked out. Existing data security protection methods relying mainly on encryption and access control cannot meet the requirements of data security protection in all aspects of the smart grid. Firstly, this paper presents data security protection system management platform architecture for smart grid from the aspects of data classification, data label management, policy management and authority management. On this basis, the data protection system for smart grid introduces the functional modules and flowcharts of the data security protection system for terminals and networks in detail. In the future, the data security protection system can be applied in generation, transmission, substation, power distribution and electricity consumption of power system.

1. Introduction

With the development of smart grid, the massive application of various wireless communication technologies such as 4G undoubtedly increases the risk of business system data leakage in all aspects of smart grid. The security protection of business data is essential to the safe and stable operation of smart grid generation, transmission, transformation, distribution and power consumption. Meanwhile, with the construction of China State Grid Corporation’s data centre, kinds of business data are being stored more and more centrally, and reliable data storage and safety protection are essential. Through the security protection of the business data in the smart grid throughout the life cycle, the leakage of sensitive data in smart grid is solved, and the safe and stable operation of the strong smart grid is provided.

With the continuous development of power informatization, mobile smart terminals are widely used in business application systems such as transmission line inspections, electricity information collection and other business application systems, and data exchange with the power information intranet through logical isolation devices.

Meanwhile, the development of a strong smart grid has increased demand for interactive services, and more businesses will need to use wireless communication technology. This will present higher requirements for building a comprehensive information security protective system of smart grid. Therefore, how to ensure the security of the collection, transmission, storage and application of business data in each aspect of the smart grid has become the focus of the development of power information.
Meanwhile, power companies develop business applications based on unstructured data such as documents and pictures to support the actual demand for unstructured data in various business applications of the entire smart grid. Therefore, how to ensure the transmission and content security of unstructured data in power applications is very important to the construction of power informatization. Based on the actual demand of data security protection of power system, this paper presents the architecture and key technologies of data security protection system for smart grid in detail from the aspects of the management platform architecture of data security protection system for power grid, data security protection system for terminal and data security protection system for network. The remainder of this paper is organized as follows. Section 2 focuses on the functional modules of data security protection system for power grid. Section 3 proposes terminal-oriented data security protection. Section 4 presents the network oriented data security protection technology. Section 5 summarizes and looks forward to the future.

2. The architecture of data security protection system management platform for smart grid

Grid-oriented data security protection system management platform is responsible for the unified management of sensitive data labels, categories, policies, permissions, logs, etc. The management platform mainly includes data classification, sensitive data label management, policy management and authority management.

2.1. Data classification

According to the confidentiality level of the company's data, different sensitivity levels are made for the company's data. Different sensitive data levels are classified by keywords, so as to maintain a keyword dictionary with different sensitivity levels. The sensitivity level is divided according to the keyword and the data source (different departments of the company). The classification of the sensitive level is determined as level 1, level 2 and level 3…the smaller the number, the higher the level. The classification of sensitive data can refer to the company's secret classification regulations. The classification table structure of sensitive data is shown in Table 1.

| The field name      | Data type | Primary key |
|---------------------|-----------|-------------|
| keyword             | character | true        |
| data sources        | character | false       |
| sensitivity level   | character | false       |

2.2. Sensitive data tag management

Its tags are defined according to the defined level of sensitive data, and each sensitive data level corresponds to one or more tags. At the same time, the defined hash function is used to generate the hash value of these tags, and for each tag, the sensitive data leak prevention strategy is adopted by its sensitive data level. These strategies are pre-defined by the strategic management of the unified management platform. Finally, a tag table is generated with the hash values of the tags and a list of policy IDs for each hash value. For example, the hash value for the power token is “0x123”, ID is 1, and the corresponding policy ID is a. The structure of the tag table is shown in table 2:

| The field name          | Data type | Primary key |
|-------------------------|-----------|-------------|
| Tag ID                  | character | true        |
| The hash value of the tag| character | false       |
| Strategy ID             | character | false       |
2.3. Strategic management
First, the strategies are classified according to the anti-leakage link, which are divided into port control strategy (including USB port, infrared port, WiFi port and Bluetooth port, printer port, etc.), application control strategy (including P2P application, email, instant messaging application), sensitive data operation control strategy (including copy, paste, clipboard protection and screenshot operation), sensitive data transmission control strategy (including network transmission protocol, network transmission medium). Under each type of strategy, the parameter list of how to prevent leakage of the system call is specifically formulated, and finally, a strategy table containing the strategy ID, the strategy name, and the strategy parameter name is generated. The table structure of the strategy table is shown in Table 3:

| The field name  | Data type | Primary key |
|-----------------|-----------|-------------|
| Strategy ID     | character | true        |
| Strategy name   | character | false       |
| Strategy parameters | character | false     |

2.4. Authority management
Develop and use the permission management of the unified data security protection management platform. The permission management uses role-based management to specify the user set of the unified platform (including administrators and general users) and different permission sets of each type of user (S-private, P-Public). The permission set includes data classification, sensitive data marking, policy viewing and editing (add, delete, modify) permissions. The structure of the user permission table is shown in Table 4, and the structure of the permission table corresponding to the roles is shown in Table 5:

| The field name            | Data type | Primary key |
|---------------------------|-----------|-------------|
| User ID                   | character | true        |
| User name                 | character | false       |
| User set                  | character | false       |
| User department           | character | false       |
| User password (encrypted) | character | false       |

| The field name            | Data type | Primary key |
|---------------------------|-----------|-------------|
| Permission ID             | character | true        |
| User set                  | character | false       |
| Permission                | character | false       |

At the same time, combined with strategy issuance and update, it is specified to which terminals the data leakage prevention strategy can be delivered, and which end users can update the local data leakage prevention strategy.

3. Data security protection for terminal
Terminal data leakage prevention mainly includes five modules: making label, sensitive data discovery, blocking for sensitive data, transparent encryption and decryption for sensitive data, and sensitive data destruction. Its functional design is as follows:

- Making label: first, develop various data security protection strategies on the data security protection unified management platform. For example, the label name is "Label", and the data security protection strategy is "prevent copy", then all electronic documents marked with "Label" cannot be copied. The tag content is: the hash value of the tag + tag name (where
the tag name is our custom) is marked by the file creator. The entire data leak prevention strategy consists of two tables: Table 1 (tag table) includes hash values and policy identifiers a, b, c, d; Table 2 (policy table) includes policy identifiers a, b, c, d, policy names, and policy parameters.

- Sensitive data discovery: the client uses label matching to determine whether the data is sensitive data.
- Blocking for sensitive data: based on sensitive data discovery, users' operation behaviour on sensitive data is identified through the policy table, and blocking policies are implemented through the parameters in the policy table.
- Transparent encryption and decryption for sensitive data: to allow for requirement for some sensitive data to be transmitted over the network, consider marking these sensitive data with a label called "encryption and decryption", which is similar to other tags.
- Sensitive data destruction: Using the U.S. department of defence disk cleaning specification to adopt the method of character cover destroyed sensitive data on a storage medium, in which data must be overwritten three times: the first time is overwritten with an 8-bit character, the second time is overwritten with the complement of the character (characters with 0 and 1 reversed), and the third time is overwritten with a random character.

The flow of terminal data security protection is depicted in Figure 1. Data security protection for terminal is mainly implemented through technologies such as making label, kinds of strategy, blocking policies and transparent encryption and decryption to achieve protection.
4. Data security protection for network

Network data security protection mainly includes three aspects: sensitive data collection, analysis and recognition.

- Sensitive data collection: this module uses mirroring to access the network, and collects network traffic through Libpcap or Tcpdump.
- Sensitive data analysis: by network transmission analysis, the physical address, using pattern, destination address and data label are achieved.
Sensitive data recognition: by data label, sensitive data transmitted in the network can be easily identified, and the specific location of the sensitive data storage is returned. And setting the conditions for remote scanning (including IP address range). The process of network data security protection is shown in Figure 2.

![Figure 2. Flow chart of network data leakage prevention](image)

5. Conclusions
This paper discusses the domestic and foreign research status and cutting-edge technologies of data leakage prevention technology, and combines the technical characteristics of major data leakage prevention manufacturers in the industry at home and abroad to analyze and study the key technology of data leakage prevention in detail. After analyzing and comparing the technical characteristics of the two mainstream data leakage prevention architectures, a data security protection system based on making label and strategy technology, which is suitable for the company's specific information background, is proposed to solve the leakage prevention problem of sensitive data from the terminal and network levels. And with the construction of the company's unstructured data centre, combined with some technical advantages of the data security protection system based on making label and policy technology, the protection scheme of unstructured data is proposed. Finally, the data making label technology in smart grid is useful application.

Acknowledgments
We would like to thank the anonymous reviewers for their comments and constructive suggestions that have improved the paper.

References
[1] Srikantha P, Kundur D. (2017) A DER Attack-Mitigation Differential Game for Smart Grid Security Analysis. IEEE Transactions on Smart Grid, 7(3):1476-1485.
[2] He H, Yan J. (2016) Cyber-Physical Attacks and Defenses in the Smart Grid: A Survey. IET Cyber-Physical Systems: Theory & Applications, 1(1):13-27.
[3] Khanna K, Panigrahi B K, Joshi A. (2017) Bi-level modeling of false data injection attacks on security constrained optimal power flow. IET Generation Transmission & Distribution, 11(14):3586-3593.

[4] Hao J, Piechocki R J, Kaleshi D. (2017) Sparse Malicious False Data Injection Attacks and Defense Mechanisms in Smart Grids[J]. IEEE Transactions on Industrial Informatics, 11(5):1-12.

[5] Yang Q, Li D, Yu W. (2017) Towards Data Integrity Attacks against Optimal Power Flow in Smart Grid. IEEE Internet of Things Journal, 4(5):1726-1738.

[6] Liu X, Bao Z, Lu D. (2017) Modeling of Local False Data Injection Attacks With Reduced Network Information. IEEE Transactions on Smart Grid, 6(4):1686-1696.

[7] Zhaoyang D, Fengji L, Gaoqi L. (2018) Blockchain: a secure, decentralized, trusted cyberinfrastructure solution for future energy systems [J]. Journal of Modern Power Systems and Clean Energy, 6(5):958-967.

[8] Mostefaou A, Raynal M. (2016) Intrusion-Tolerant Broadcast and Agreement Abstractions in the Presence of Byzantine Processes. IEEE Transactions on Parallel & Distributed Systems, 27(4):1085-1098.

[9] Okamoto T. (2017) Design of a Lightweight Intrusion-Tolerant System for Highly Available Servers. Procedia Computer Science, 112: 2319-2327.

[10] Madan B B, Banik M, Wu B C. (2016) Intrusion Tolerant Multi-cloud Storage. IEEE International Conference on Smart Cloud. IEEE, 262-268.

[11] Zheng J, Okamura H, Dohi T. (2017) Performance Evaluation of VM-based Intrusion Tolerant Systems with Poisson Arrivals. Fourth International Symposium on Computing and NETWORKING. IEEE, 181-187.

[12] Zhang Y, Wang L, Xiang Y. (2016) Power System Reliability Analysis with Intrusion Tolerance in SCADA Systems. IEEE Transactions on Smart Grid, 7(2):669-683.