

# *Problems and Countermeasures of Power Information Security*

**Mengqi Yu**

*Xiangyang No.5 Middle School, Xiangyang 441000, China  
352217510@qq.com*

**Keywords:** power information, information security, identification, firewall, backup and recovery.

**Abstract:** With the improvement of the level of science and technology, power companies must rely on computer and Internet technology in the development process, but there are still many hidden dangers in power information security, which directly affects the development of power companies. Based on this, this paper discusses the two aspects of power information, which are security issues and strategies. Firstly, it analyzes the information security problems from the production control system, administrative management system and marketing management system, and then solves the problem by improving the identification technology, the firewall technology, the backup and recovery technology.

## **1. Introduction**

Driven by global informationization, national economy informationization and enterprise informationization have become a development trend. The scale of computer information networks is constantly expanding. The information technology and information industry have infiltrated all walks of life in an unprecedented way. They are gradually changing people's production and lifestyle, and promoting the continuous reform of corporate mechanisms and systems. While the scope of the computer information network is expanding, the security of the information network has become increasingly important. Once it is damaged, its impact or loss is enormous. Therefore, the issue of information security has become a topic of great concern to experts and scholars at home and abroad and users. The power industry is the pillar industry of the national economy, serving the national economy and people's lives. The way in which power companies transmit data is usually network transmission. There are many drawbacks in of data transmission and sharing, and the process is often subject to malicious attacks. Once there is a problem with information security, the loss and impact will be incalculable. Therefore, power companies need to analyze the problems existing in power information security in a timely manner and take effective measures to ensure the safety risks of power information removal. To ensure the safety of power information to provide security for the development of enterprises. The characteristics of the power industry determine that the information security of the power system not only has the characteristics of information security of the general computer information network, but also has the characteristics of information security of the real-time operation control system of the power. Therefore, with in-depth study of the characteristics of power

system information security, taking measures to ensure the security of power system information is the main problem we face in the process of achieving "digital power system".

## **2. Problems in Power Information Security**

Power information security management is one of the tasks of power companies in implementing management reforms. It has the same important position as technology management and personnel management. Any work content in power companies involves information security issues, and confidentiality work is done to ensure that corporate information does not leak. The information security problems in power companies mainly appear in three aspects:

### **2.1 Information security issues related to production control**

The smooth transmission of information between various departments in the enterprise is one of the conditions for ensuring the orderly operation of the enterprise, and the production of the enterprise is the most important part. In the process of generating electric energy and subsequent transportation, distribution and dispatching, power grid dispatching automation, substation automation, power plant monitoring and other systems are very vulnerable to malicious attacks by criminals. With the increase of power information content, the production control system is changing from the traditional static management to the dynamic management. However, the situation of impersonation, tampering and even stealing often occurs in this process, which seriously affects the information security of the production control system.

### **2.2 Information security issues related to administration**

In the administrative work of power companies, the protection of information security needs to be improved. In the process of transmitting information or sharing information, there is a problem that the transmission equipment carries viruses or artificially leaks information. Enterprises neglect human factors in the work of information security management. For example, staff operations are not standardized, and no anti-virus measures are taken in time to make the power system fail. Therefore, enterprises should conduct information security protection of administrative systems according to the operation of the power system.

### **2.3 Information security issues related to marketing**

Paying attention to information security in the marketing system can further protect the interests of enterprises, suppliers and users. Since the work communication between the power company and other units is mostly carried out on the network, the security protection of information transmission and sharing should be emphasized. Many lawbreakers will damage the security of the marketing system through system procedures or networks, thus jeopardizing the interests of power companies.

## **3. Countermeasures to Solve Information Security Problems**

### **3.1 Improvement of identity technology**

Password-based identification technology requires the visitor to present a password to the system providing the service, and the identification system will compare the password with the original password in the system to confirm the identity of the visitor. The security of the password system in the grid system is related to the encryption algorithm, selection and distribution, and character length

of the password. In special cases, the usage time limit must be set. The system verifies the password and the legality of the visitor to prevent illegal login to the internal website of the power company.

Identification technology based on digital certificate relies on third parties for identification. After the certification authority identifies the user, the certificate is issued to the user, and the user holding the certificate can access the server by the certificate. When the user accesses the internal server of the power enterprise, a certificate needs to be provided, and the server uses the public key of the certification authority to unlock the signature of the certification authority to obtain a hash code. The server also obtains a hash code by processing a part of the information of the certificate, and after verifying the two hash codes, the authenticity of the certificate can be determined. The above process is shown in the figure below:

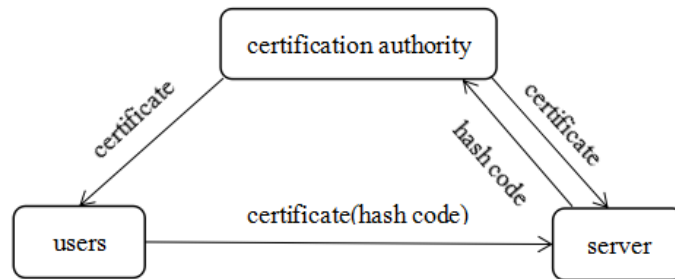


Fig.1 The process of identification technology based on digital certificate

### 3.2 Improvement of firewall technology

The power enterprise setting firewall is a protection technology to protect power information security. It is a control technology that controls access between networks. It can filter communication between two power networks and filter out unauthorized network communication. The architecture of the firewall is mainly divided into a dual-homed host architecture, a shielded host architecture, and a shielded sub-network architecture. The grid system can filter out the safe information allowed by the network protection through the above three protection systems. The firewall establishes a communication monitoring system between the networks to isolate the network, thereby blocking the intrusion of the external network into the grid system. The firewall set by the power enterprise has two functions of packet filtering and proxy service.

The packet filtering router establishes an information filtering table by using the packet header information, and the data packet can only pass when the requirements of the filtering table are met. This way, the illegal user can be prevented from invading the grid system of power enterprise. The packet filtering router can analyze the data such as the IP address, port number, and IP representation of the data packet through the control table. Set the internal host to Host C and the host that meets the access requirements to Host A. The packet filtering rules are as follows:

Table 1 Packet filtering rule

Source	Destination	Permit	Protocol
Host A	Host C	Pass	TCP
Host B	Host C	Discard	UDP

The proxy service is the "proxy" program that is open on the firewall host, including applications and server programs. The agent receives the user's request to access the corporate website, instead of the power network connection, creating an illusion between the internal user and the external service. So that the users think that they connect a real server.

### 3.3 Improvement of information backup and recovery technology

Data backup and disaster recovery are important components of information security. The ideal backup system should be comprehensive and multi-level. The hardware system backup is used to prevent hardware system failure. The combination of network storage backup system and hardware fault tolerance can be used to prevent data failure caused by software failure or human error. Damage. This multiple protection against the system not only prevents physical damage, but also effectively prevents logical damage. The data backup mode is generally divided into two types: local backup and off-site backup. The first is that the system's business data is damaged or lost due to system or human error, and the data can be restored in production locally. Second, in the case of a sexual disaster (earthquake, fire, machine damage, etc.), recovery of data and the entire system can be achieved locally or remotely. The network data storage management system refers to centralized management of data backup of the entire network through professional data storage management software combined with corresponding hardware and storage devices in a distributed network environment, thereby realizing automatic backup, file archiving, data tiered storage and disaster recovery.

### 4. Conclusions

In summary, with the development of computer network technology, people's awareness of the use of the Internet is getting higher and higher, and the awareness of information security protection of power monitoring systems by power companies has gradually strengthened. Through the use of passwords and digital certificates, the user's identification system is improved. By using firewall technology to control the access of criminals to the corporate network and intercept malicious intrusions. In the future development of power companies, higher requirements of the technology for preventing and controlling network intrusion will be put forward, and it is necessary to continuously improve the technical level to cope with the test of information security.

### References

- [1] WANG Dong, CHEN Chuanpeng, YAN Jia, et al. *Pondering a new-generation security architecture model for power information network [J]. Automation of Electric Power Systems*, 2016, 40(2):6-11.
- [2] YU Ping. *Design and implementation of information security technology supervision and management system for electric power enterprises [D]. University of Electronic Science and Technology of China*, 2011.
- [3] ZHONG Zhichen. *The technical discussion of power big data information security analysis [J]. Electric Power Information and Communication Technology*, 2015, 13(9):128-131.
- [4] CUI Ajun, ZHANG Huafeng, FAN Dilong, et al. *Research on security protection technologies for internet of things for power corporation [J]. Electric Power IT*, 2013, 11(3):98-101.