Analysis of Power Network Behavior Security Analysis Technology

Kai Fan[1],Hang Yang[2],Aidong Xu[2]

[1]China Southern power grid,Guangdong,510700,China
[2]Electric Power Research Institute.CSG,Guangdong,510700,China

Abstract. Nowadays, with the rapid development of science and technology, network information technology is widely applied to various enterprise departments. In order to meet the increasing social needs, power companies have also built power network information systems. The establishment of the network information system has been put into use, which has greatly improved the efficiency of the power enterprise. However, the security risks of network information systems have followed. Once the network is damaged by the attack, it will cause the power system to fail to operate normally, which will inevitably cause significant losses. Power system information security issues threaten the security of the power system and the entire power industry. Studying the information security of power systems, how to protect the power information network from threats, how to ensure the safe and stable supply of electricity to the whole society, and striving to develop a safe and effective power network information system is an important issue facing the development of information technology.

1 Introduction

In today's era of rapid development of information technology, computer network technology is indispensable in all fields. The establishment of power network information systems is highly valued by power companies and society as a whole. However, the information security of computer networks has many potential risks, and it is vulnerable to viruses and hackers, causing damage to the power system. As the basic industry of the national economy, the power industry is closely related to people's lives. Whether the safety of the power network system is related to the overall operation of the power company is the key to providing sufficient power supply for the power industry. Therefore, ensuring the safety of power network information to the greatest extent is an imperative for every power company. The author has the following views on the investigation of security issues with power network information systems.

2 Factors that threaten the security of power network information systems and their impact

Network information system security is a systematic project. There are many factors affecting the security of power network information systems. The author thinks that it can be divided into the following two reasons:

2.1 Subjective human factors

Among the threats faced by power network information systems, human error and malicious attack damage account for the vast majority.

The human error is mainly due to the imperfect management system of the power enterprise or the lax management system. The security awareness of users or administrators is not strong. Not fully aware of the risks of network insecurity. The password level set is not high, the account is logged in without the security control, or the account and password are loaned to others; the security of the computer or system is improperly set, and resources are shared with other networks at random, etc. The operation is the most vulnerable to security breaches, resulting in malicious attacks on the power network information system.

Malicious attack damage mainly involves hacker attacks and virus attacks. The hacker's attack methods are mainly backdoor programs, information bombs, denial of service, network monitoring and password cracking. According to the length, rate, traffic and type of encrypted data, the hacker can analyze and combine the transmitted data to obtain the system authority and directly manipulate the power equipment in the whole system, which poses a serious threat to the power network information system. As far as the current development trend of the network is concerned, hacker attacks are becoming more and more forms and activities are becoming more frequent. The data shows that in the first two months of this year alone, 5,324 overseas hosts have remote control of 1,141 websites in China through the implantation of the back door. Among them, 1959 hosts in the United States control 3,579 websites in

China, 132 in Japan.

2.2 Objective factors

There are two main reasons for objective factors:Because the network is still in the development stage and has the characteristics of openness and non-primacy, the network information system itself lacks security mechanisms in many places. For example, the settings of the software system[1].Natural disasters cause system failures and data corruption, resulting in services being unavailable. Such as: fire, typhoon, flood, earthquake, tsunami, etc. The blackout accident in the United States and Canada that occurred on August 14, 2003 was caused by a sudden failure of the power transmission line, which was a safety accident caused by the failure of key components.

3 Measures for the security of power network information systems

3.1 Focus on host protection, using firewall and anti-virus technology

In the power network information system, the host has a wide range of security coverage, so the security of the host system has an important role and value for increasing the security of the server. First, make local security settings for the computer, start local security policies, and control objects. Hacker and virus infringement, usually using authentication technology and encryption to protect the computer network security of the power system, the host protection system in the power system can effectively prevent and control various computer known viruses or unknown viruses, various malicious programs and Trojan invasion. At present, the system security of the host protects the main firewall[2].The power security network architecture is as follows.

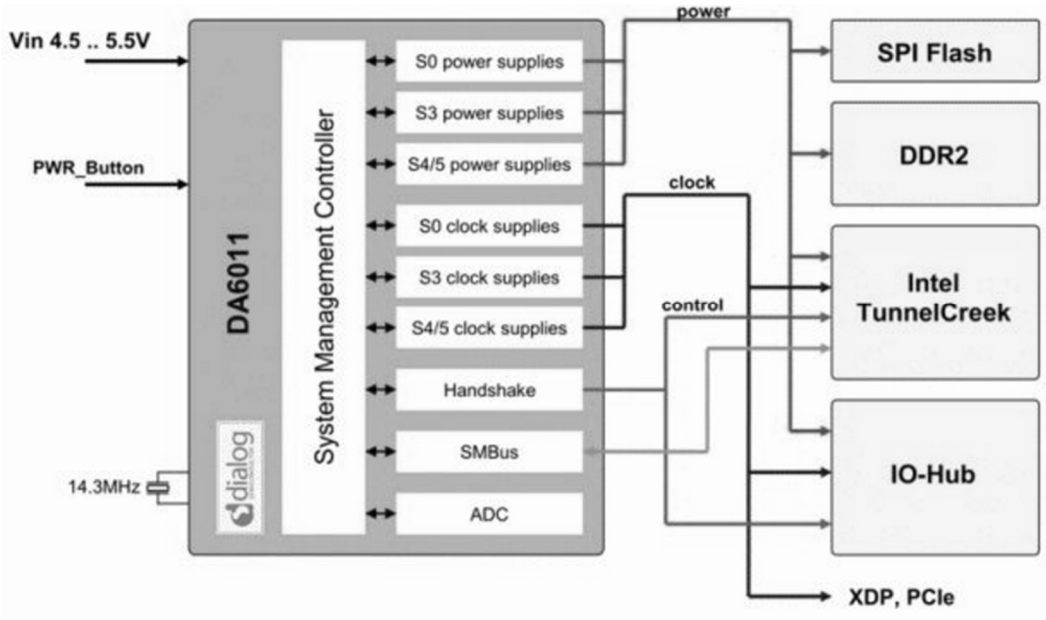

Fig.1 Power security network architecture

The firewall has a good protection. It greatly enhances the security of an internal network and reduces risk by filtering unsecured services. The intruder must first pass through the firewall's security line to reach the target computer. A firewall is a barrier used to block the intrusion of hackers on the network. It is responsible for detecting information from the Internet. By using the firewall to partition the internal network, the isolation of the key network segments of the internal network can be achieved, thereby limiting the impact of local key or sensitive network security issues on the global network. The types of firewalls mainly include network layer firewalls and application layer firewalls. Scientific and rational configuration of network layer firewalls and application layer firewalls is an important measure to ensure the security of power network information systems.

The virus is currently the biggest disease that destroys the power network information system, and it has caused great destructive power to various types of information security. Clients with appropriate anti-virus products should be deployed in the power system for servers and workstations in all systems. For the handling of virus problems, power companies should install safe and effective anti-virus software, and deal with them through various anti-virus and anti-virus methods to create a stable operating environment for information systems. For example, install an anti-virus software client on each PC and install server-based anti-virus software on the server.The working principle of the power security network server is as follows.

Fig.2 Working principle of the power security network server

3.2 Strengthening the security management of power network information and improving the security system

Strict management system is one of the important measures to ensure the security of enterprise information network. At present, in the safety management of power network information systems, the lack of operability of the management system is a prominent problem. People are the key factor in information security, and people are also the weakest link in information security. Strengthening the management of security systems must first improve the security awareness of leaders and operators. Many power enterprise networks have a tendency to rebuild, emphasize technology, and manage lightly. Practice has proved that the imperfect safety management system and the low quality of personnel are one of the important sources of cyber risks. As the saying goes: "No rules are not square." Managers should develop relevant network security management systems to constrain employees. Regularly train employees on safety knowledge, improve the ability to deal with accidents, and improve the overall quality of employees. Strengthen supervision and inspection, and the safety management system must be implemented. The management system is serious, authoritative and compulsory. Once the management system is formed, it must be strictly enforced.

Improving the level of information security protection technology First, it attaches great importance to network firewalls. The firewall is the only exit for the power enterprise information network. All access will be through the firewall, and no connection bypassing the firewall is allowed. Therefore, it is especially important to do a good job in this channel. We should pay attention to this technology and develop a higher level of protection software to meet the needs of information network security work. The second is to attach great importance to the intrusion detection system[3].

It is necessary to deploy an advanced distributed intrusion detection architecture to ensure the security detection of power enterprise information systems.

The third is to attach great importance to the network hidden danger scanning system. Scanning network devices include: servers, workstations, firewalls, routers, routing switches, and so on. After the scan is completed, a detailed safety assessment report is generated, and the scan results are analyzed in the form of reports and graphs, so that the user can be visually evaluated and checked for safety performance. The fourth is to attach great importance to the data encryption system. Security measures such as file encryption, message digest, and access control are required to achieve confidentiality and integrity requirements for file storage and transmission, and to control file access. For communication security, security measures such as data encryption, message digest and digital signature are used to protect the information in the communication process, and to realize the confidentiality, integrity and non-repudiation security requirements of the data in communication. The fifth is to attach great importance to database security. To ensure the confidentiality and integrity of database data through data storage encryption, integrity verification and access control, and to achieve secure access to database data. In short, the security technology of network information is especially important for maintaining the true security of network information, so the work in this area needs to be strengthened[4].

4 Summary

The society continues to improve and information technology continues to develop. Under the situation of power informatization, the application of power system network informatization has developed with the development of society and the development of scientific technology. In the period of rapid development of information technology, the security of computer network information is also gradually changing[5]. The security and reliability of the system's computer network information poses greater challenges, and the security of the power network information system is particularly important[6]. At present, the security protection of power systems is mainly caused by attacks on hackers and viruses. In the future, the use of computer networks in power companies will become more widespread, while the destruction of network information systems will also become diversified. When introducing network information systems, power companies must pay attention to the control of various risks and prevent enterprises from economic losses caused by network security problems. As a pillar industry of the country, electricity plays an extremely important role in the national economy and is closely related to people's lives. Furthermore, due to the needs of business development, the power system requires connection with external networks. At present, there are more and more insecure factors such as viruses, hackers and illegal access. The security of information networks has become the key to affect the safe operation of power systems[7].

References

1. Dmytro Matsypura,Anna Nagurney,Zugang Liu. Modeling of Electric Power Supply Chain Networks with Fuel Suppliers via Variational Inequalities[J]. International Journal of Emerging Electric Power Systems,2011,8(1).
2. Gang Chen,Hua Tian,Wei Xie,Wei Zhong. Joint Network Selection and Discrete Power Control in Heterogeneous MIMO Networks: A Game Theoretical Approach[J]. Frequenz,2013,67(9-10).
3. Sorin Dan Volosciuc,Monica Dragosin. Neural Networks Used In The Evaluation Of Power Quality[J]. ACTA Universitatis Cibiniensis,2015,66(1).
4. Du Xinhui,Wang Shuai,Zhang Juan. Research on Marine Photovoltaic Power Forecasting Based on Wavelet Transform and Echo State Network[J]. Polish Maritime Research,2017,24(s2).
5. Dong Hwan Kim,Daniel A. Eisenberg,Yeong Han Chun,Jeryang Park. Network topology and resilience analysis of South Korean power grid[J]. Physica A: Statistical Mechanics and its Applications,2017,465.
6. Guanping Xiao,Zheng Zheng,Haoqin Wang. Evolution of Linux operating system network[J]. Physica A: Statistical Mechanics and its Applications,2017,466.
7. Ioannis P. Panapakidis,Athanasios S. Dagoumas. Day-ahead natural gas demand forecasting based on the combination of wavelet transform and ANFIS/genetic algorithm/neural network model[J]. Energy,2017,118.