Research on Information Security Threats and Defense Strategies of Smart Grid

Jianxuan Zhang^{1*}

¹ Curtin University, Perth, Western Australia, WA 6102, Australia

Abstract. In view of the increasingly important position of information security in the development of smart grids, this paper studies the threats and defense strategies of smart grids to information security, and provides guidance for how to solve the information security problems of smart grids. At the same time, the concept and threat of smart grid are described. On this basis, several defense strategies are proposed, including encryption, digital signature recognition, firewall, antivirus, intrusion detection, physical isolation and in-depth defense of information security. The analysis shows that the threat faced by human beings is information security. Information security should focus on the development and construction of smart grids. Several defense strategies are feasible and can provide effective support for the safe and stable operation of smart grids.

1 Introduction

With the continuous increase of global resource and environmental pressures and the continuous development of the power marketization process, users have higher and higher requirements on performance quality and reliability. N-GAS smart grid is considered to be the future development direction of the grid, and the smart grid is reliable, safe, high-quality, flexible and efficient, which will become the top priority in the development and construction of power grids in the future. Information technology and information systems play an important role in the smart grid, and the related information security has become increasingly important. Information security has become an important foundation for the safe and stable operation of smart grids and reliable power supply in society, and is an important part of the production and operation management of power enterprises. On this basis, this paper analyzes the threats faced by smart grid information security, and on this basis, puts forward an effective and practical information security strategy, which provides technical support for the safe and stable operation of smart grid.[1]

2 Definition of smart grid

The smart grid is a digital grid based on modern information technology and built on an integrated, high-speed, two-way network. It is also called "upgraded version of traditional power grid", covering all aspects of power generation, transmission and distribution, dispatching, power distribution, and users. It is a closed system based on a powerful network structure, supported by a communication information platform and intelligent control.[2]

3 Smart grid information security threats

The threats to smart grid information security can be divided into natural threats and human threats. Natural threats mainly come from natural factors such as lightning, which can cause electromagnetic interference, damage the accuracy of information, and even damage equipment, thereby endangering the safety of information systems. The human threat is an attack that results in improper operation of the device, refusal to move, and incorrect system parameters. This will damage the confidentiality, integrity, reliability and availability of the information, damage the safe and stable operation of the information system, and cause economic losses or even serious consequences. The main types and characteristics of smart grid information security threats are shown in Table 1.

Table1. Information security threat

Internal staff misoperation	Unintentionally leaking sensitive information such as 11 orders or carelessly matching, operation
Integrity breach	IE authorized to modify system programs and control instructions
Bypass control	Intruder sends IE law control instruction, causing system accident
IE authorized use	Unauthorized use of computer and network resources

*Corresponding author's e-mail: hdzjx2014@163.com

Scam attack	Spoofing attacks based on IP addresses and Web services
Disguise	Intrusion into the system with the disguise of "legal identity"
tamper	Change transmission information, change remote control instructions, modify fixed value instructions
monitor	Etc., threatening the safety of grid operation
Communication interrupted	Illegal interception of system communication and contact information
computer virus	System communication is intermittent or unavailable
Denial of service	Computer malicious programs or codes such as Muwu and worms
Lightning strike	Sending large amounts of V crash data, causing network paralysis
Main features	Cause electromagnetic interference or damage to the corresponding equipment

As shown in Table 1, human threats are divided into two categories: one is the unintentional threat caused by the abuse of authorized personnel, but the use of financially authorized data and resources is illegal; the other is the deliberate threat of malicious threats to cybercrime, external interference And unauthorized internal illegal intrusion. An unauthorized user is an unauthorized intrusion system inside the system.[3]

In addition, with the development of smart grids, the remote application technology of control systems has gradually been applied. However, the design and development of control systems often lack the construction of a secure kernel, which leads to an attacker's illegal deletion without being aware of the system. The user-friendliness and information integrity of the system are severely damaged, leading to adverse security consequences.

4 Smart grid information security defense strategy

As mentioned earlier, for traditional power networks, the only communication between the grid and users is to transfer control information from the grid to the users, and there is no information between the grid and users. However, as a power supply system, the smart grid replaces the bilateral communication digital network and provides users with real-time information interaction. At this time, it is directly exposed that the terminal can be attacked on the user side. The goal of the information security defense strategy is to protect the availability, reliability, controllability, confidentiality and integrity of information, and to ensure the safe and stable operation of the smart grid information system. Combined with the analysis of information security risks, several effective and feasible defense strategies are proposed.[4]

4.1 Encryption measures

Encryption measures include processing the information sent by the system with a specific algorithm, and recovering the data by decryption after sending. Even if the attacker receives the encrypted information, but the encryption method is unknown, it is still difficult to crack and master the original information content, effectively preventing and avoiding illegal attacks on the information, and hiding information is the basis of encryption measures, starting from reversible mathematical transformation to information, It is difficult for an attacker to understand the

original real information. The original real information is also known as plain text, which is cipher text after disguise, and encryption is also a process of disguise. The encryption algorithm can reverse the mathematical transformation that effectively implements encryption.

4.2 Firewall measures

As an infrastructure, the firewall connects the public network with the private network. It can store and isolate unreliable networks for servers, gateways, routers, or devices with multiple functions to control information packets and information in and out of the network, track specific header file protocols of data packets, and ensure network information security and corresponding information security. Hidden network structure and internal IP address, mobile address book and audit firewall and other services prevent illegal attackers from attempting to penetrate the network system through the core of "containment point" to ensure the continuity and confidentiality of network services. The corresponding transformation of network construction can strengthen non-public ownership. Although the benefits are obvious, sometimes there are still some shortcomings that cannot completely prevent the spread of infectious viruses and cannot deal with network security problems. According to the development requirements of the smart grid, the implementation strategy of the firewall should be as narrow as possible in scope and complexity, and should be adopted according to the actual business needs such as business data flow and Internet egress, and the firewall should be deployed between the border and different security zones.[5]

4.3 Antivirus technology

With the rapid development of global information technology and Internet technology, computer viruses have shown obvious update and spread characteristics. According to statistics, there are currently more than 200,000 computer viruses in the world, such as hard disk drive sector infection viruses, Trojan horse infection executable files, and worm viruses. If the virus cannot be discovered and eliminated in time and effectively, it will bring huge security risks and even catastrophic consequences. It is possible to design and use antivirus programs to effectively control and kill viruses, identify whether viruses have infected execution files, and point to "appropriate standards" to accurately analyze alarms,

eliminate false alarms, check and kill viruses or block, reject A request to run an executable file with a virus. At the same time, the correct use of anti-virus programs, less CPU running time, will not affect the operation of the whole machine, in the smart grid, accurate detection of anti-virus standards and efficient anti-virus technology is mainly used to protect the safety of the system. The operating system is the supporting platform for various application systems in the smart grid. Its security is the basis of system security management, and antivirus technology has played a better role.

4.4 Physical isolation

The information security of confidential data in the secret network cannot be completely based on the logic of basic software protection mechanisms, such as the above encryption measures, firewall measures, antivirus technology, etc. Intrusion detection is such a logic mechanism, we need to establish an absolutely reliable information security The tower, that is, physical isolation, ensures that confidential data of the secret network is not leaked or destroyed. The absolute isolation between this external network, the internal network and the external network in the physical unit are completely separated, and there is no connection to ensure absolute security. Based on self-sacrifice in unreliable networks, it can respond positively and effectively to attacks, fully protect the physical isolation and moderate control of internal and external networks, eliminate and avoid all types of attacks from operating systems and networks, and provide a ratio Firewall level higher protection level.

5 Conclusion

With the development of smart grids, the importance of information security has become increasingly prominent. By classifying, analyzing and summarizing the threats faced by smart grid information security, we have a clear understanding of the severe reality of information security, construct information security defense strategies, encryption, digital signature authentication, real-time detection of firewalls, anti-virus, and illegal intrusions. It can better defend from the software level to avoid corresponding system and network attacks; based on physical isolation strategy, it can effectively defend from the history of hardware; Based on the software and hardware defense strategy, combined with information security, it provides a comprehensive guarantee for the safe and stable operation of smart grid. At the same time, we should also see that the threats to smart grid information security are constantly evolving and changing, and the emergence of new viruses is extremely hidden and destructive. In order to adapt to the application of trust computing in the smart grid under the new situation, it is necessary to strengthen the research on trusted network security technology.

References

1. Song Xiaofang, Xue Feng, Li Wei, et al.

- Comprehensive Frontier Technology of Smart Grid [J]. Power System Communication, 2010, 31(7): 17.
2. Xiao Shijie. Construction of China's smart grid technology thinking [J]. Power system dynamics, 2019, 33(9): 1.
3. Liang Zhixian, Qiu Xiaogeng, An Ran. The Influence and Demand of Smart Grid on Communication[J]. Power System Communication, 2010,31(9):1-4.
4. Teng Wenjing. Key points of smart grid security construction [J]. Electric Power Informatization, 2010, 8(12): 27-29.
5. Chen Shuyong, Song Lian, Li Lanxin, et al. Comprehensive Smart Grid Technology [J]. Power Grid Technology, 2017, 33(8): 1-7.