New Active Defense Technology under the Background of Power Information Network Security

Jing Li1*, Jie Huang1, Li Tian2, Jie Wang2

1State Grid Hubei Electric Power Co., Ltd, Hubei Wuhan, China, 430077
2Electric Power Research Institute of State Grid Hubei Electric Power Co., Ltd, Hubei Wuhan, China, 430070

*Corresponding author e-mail: lijing8@sghec.org

Abstract. With the rapid development of the national power industry, the security of power information network has been widely concerned by the society, and the related impact has also been prominent. At this stage, the development of power information technology is more and more inseparable from the network, so network security has become more and more important, if the network has a serious threat in practical application, the loss caused will be unbearable. In the process of controlling the network security of power information industry, one of the most important and effective methods is active defense. Based on this, this paper puts forward the research of active defense technology under the background of power information network security, expounds the defects of firewall technology and intrusion trap technology in passive network security defense technology, and introduces the pitfalls of active defense new technology. In addition, the paper discusses the new active defense technology and its application in power information network security, and puts forward reasonable suggestions. Therefore, the use of information technology to solve the hidden danger of power network security is important.

Keywords: Active Defense, Power Information, Network Security, Trap Technology

1. Introduction

With the rapid development of the Internet, the resistance to viruses [1] and hacker attacks [2] has become a global problem. In the traditional network security technology, passive protection technology [3-4] is used, such as firewall technology and interference detection technology. With the development of network technology, this technology will gradually expose its shortcomings. It includes network security, viruses, access restrictions, threats and hackers, so it cannot provide high-strength protection. In addition, intrusion detection [5] is not feasible in all possible cases; it has high false positive rate and false positive rate response, and provides little information after analysis.
China's power network development has become a part of the rapid development of the country, at the same time; it will have a significant impact in many aspects. Relevant analysis of electric power information network security [6-7] in the development, there are still some network vulnerabilities. First of all, the network at this stage shows a high degree of openness. Although the power network has established a defense platform by combining various defense technologies with the implementation of checkpoints, the overall situation is regarded as a passive defense mode, which does not conform to the development trend of power information network. In this process, we cannot actively find the loopholes and hidden dangers, and always wait until the problems appear. This method is not compatible with the development trend of power information network and is not easy to operate in some cases. If there is a loophole in the interior, it will have a devastating impact. Secondly, when dealing with the related vulnerabilities, we still use the old technology to complete, without any positive discovery. In the long run, especially in the power network, it is easy to cause serious security risks, and it is difficult to conduct in-depth investigation.

To sum up, this paper puts forward the research of new active defense technology [8-10] under the background of power information network security, expounds the defects of firewall technology and intrusion trap technology in network security passive defense technology, discusses the importance of network security in power information industry, analyzes the current network construction status of power information industry, and puts forward the implementation of network security technology defense Methods to provide reference and suggestions for the improvement of the current power industry.

2. Implementation of New Active Defense Technology under the background of Power Information Network Security

2.1. New Technology of Active Defense
1. Trap technology.
   The main purpose of trap technology is to attract attackers by creating vulnerability simulation. However, since there is no useful information in the system, no one will find it when the actual system is running. As a result, all attempts to access this network's communication capabilities are suspect. Another purpose of this technology is to delay the attacker's attack time and identify the attacker's position to achieve reversal.
2. Forensic technology.
   There are two kinds of forensics technology in active defense technology: static forensics technology and dynamic forensics technology. Fixed forensics technology is mainly used to collect evidence for attackers after system intervention. Flexible legal investigation technology can provide real-time data analysis to provide strong evidence that the connection between the two parties is broken or to induce the enemy to collect evidence more deeply.

2.2. Construction of Active Defense Subsystem
   Principle design of active defense subsystem: information about current security status of power network. Integrating with the actual situation, the deployment of three-dimensional network security system can prevent viruses from invading the external network and internal network. The initial deployment of the new system and the existing network system has little impact, and the calculation formula of the impact score of the new system is as follows:

   \[ \text{Scope}=\text{fixed}, \quad \text{Impact score}=6.42 \times ISCh_{\text{base}} \]  

   \[ \text{Scope}=\text{change}, \quad \text{Impact score}=7.52 \times (ISCh_{\text{base}}-0.029) -3.25 \times (ISCh_{\text{base}}-0.02)^{15} \]
Among them, $ISC_{base}$ are temporary variables. The design of the new system follows the following principles:

1. Safety and reliability: safety products can be used for stable and reliable operation system;
2. Advanced technology: safety technology must be advanced enough;
3. Technology maturity: correct application of safety technology and products;
4. Management: safety products must be properly managed. It can also ensure the safety of non-technical personnel according to the guidelines.
5. Scalability: The system is improved or extended to maintain certain generalization.

3. Experimental Thinking and Design

3.1. Experimental Ideas

This paper puts forward the research of new active defense technology under the background of electric power information network security, expounds the defects of firewall technology and intrusion trap technology in network security passive defense technology, discusses the importance of network security in power information industry, analyzes the current network construction status of power information industry, and puts forward the implementation methods of network security technology defense.

3.2. Experimental Design

With the continuous progress of network technology, the security of power information network will get more innovation. However, the simulator of power information network security system can make it work normally in the face of actual attack without proper practice. Power network security can use real-time defense technology to simulate the attack and defense environment to implement attack and defense practice, and provide better solutions for new network vulnerabilities and attack forms.

Power grid should not only prevent external attacks, but also strengthen internal network user management. For internal user management: the network has real name system, which can prevent the spread of virus attack or internal man-made outbreak. Visit security review; fully implement the layout, installation, maintenance and control of illegal software of security terminal and computer terminal. Active defense system can prevent external attacks or viruses from spreading to LAN network. Table 1 shows the composition of the defense subsystem.

| Time of attack | Action |
|----------------|--------|
| Before the attack | Using vulnerability scanning tools and hacker tools to conduct a comprehensive inspection of the system |
| Time of attack | Attacker lures trap network |
| After the attack | Analysis, evidence of aggressive behavior |

4. Discussion

4.1. Discussion on Experimental Results of New Active Defense Technology for Power Information Network Security

The main premise of the application of active defense technology in the network security of electric power information industry is risk assessment. This kind of network security assessment is not only to analyze the collected data information, but also to pay more attention to the whole power network structure, so as to effectively ensure the comprehensiveness of the evaluation function. Active defense technology is mainly used to collect evidence for attackers after system intervention. Flexible legal
investigation technology can provide real-time data analysis to provide strong evidence that the connection between the two parties is broken or to induce the enemy to collect evidence more deeply. The main purpose of trap technology is to attract attackers by creating vulnerability simulation. However, since there is no useful information in the system, no one will find it when the actual system is running. As a result, all attempts to access this network's communication capabilities are suspect. Another purpose of this technology is to delay the attacker's attack time and identify the attacker's position to achieve reversal. It is very important for the development of power information system to adopt positive and defensive measures to the security of power network. There is no real defense and simulation experience in traditional power information network security, and only the actual security system experience in actual defense is not enough. In the active defense technology, dynamic forensics technology is used to analyze and solve the attacks on attackers and defense practices, and record them in the security system database, so as to better protect the power network in practice.

![Figure 1. Hazard clearance capability of active defense technology](image)

Due to the particularity of the network environment, some network loopholes are considered inevitable. The three major hazard sources are data theft, extortion virus and DDoS. The common nature of these three types of hazard sources is to control and attack the power information system and reduce the efficiency of data processing of power information system. In this paper, questionnaire is used to evaluate the ability of vulnerability scanning, baseline scanning, application security scanning and attack and defense drill in active defense technology to remove the three major hazards. The evaluation results are shown in Figure 1. It can be seen that the technical operation of active defense technology and its application in power information network security have been greatly improved compared with the past, and there are no serious deficiencies and deficiencies in all aspects of work.
Figure 2. Composition of active defense subsystem

It can be seen from Figure 2 that the active defense subsystem can be composed of active defense strategy library, Honeynet module, forensics module, analysis module and control module. Active defense strategy library can support intelligent improvement and store the latest active defense strategy. Honeynet module can attract hackers into fake systems and analyze their behaviors. The forensics module is "acceptable to the court, reliable and persuasive enough, existing in the computer and related peripherals, confirming the electronic evidence, protecting, extracting and filing; the control and analysis module is deployed at the boundary of the power network.

4.2. Active Defense Strategy to Strengthen Network Security of Power Information Industry

1. Strengthen network data collection

With more and more data information included, in order to ensure the safe transmission of information, it is important to effectively collect network information to ensure network security. Whether it is log information, equipment information or electricity fee information, effective statistics must be carried out, and relevant database and appropriate access principles need to be established. For example, some pre initialization principles can be designed to analyze collected information in real time and quickly. Store the latest updated information in a preferred location so that the collected information can be quickly accessed and sent to the hazard analysis module.

2. Network security risk analysis

Using advanced analysis and data mining technology to complete network data collection is the standard and premise of establishing two-dimensional network risk information matrix. Then combined with the analysis index to analyze the security threat, in this process, there are many data mining technology can be used. At the same time, in order to reduce the structural damage leakage, in principle, we need to select the appropriate performance subdivision as the discriminant function, and introduce the adaptive enhancement theory to further improve the network data. Some potential risk information is extracted by data mining and data classification.

3. Network security assessment

The main premise of the application of active defense technology in the network security of electric power information industry is risk assessment. This kind of network security assessment is not only to analyze the collected data information, but also to pay more attention to the whole power network
structure, so as to effectively ensure the comprehensiveness of the evaluation function. Generally speaking, power network security managers want to more intuitive, comprehensive understanding and grasp the resources of all software and hardware, can be divided into serious, mild, general, good and good several different levels, so that in the process of network security management will be more targeted to ensure the effective implementation of active defense.

5. Conclusions
In the research of active defense technology under the background of power information network security, this paper expounds the defects of firewall technology and intrusion trap technology in the passive defense technology of network security, introduces the trap technology and Forensics Technology in the new technology of active defense, and discusses the new technology of active defense and its application in power information network security, and puts forward reasonable suggestions. According to the research, the software and hardware carried by the power information industry network not only include individual users, enterprise users and the State Grid, so it is necessary to build a multi-level active defense system

References
[1] Liangjun, H. U, Daode, W., Xiaofeng, L. I., Hongmei, W., & Rui, S. (2018). Research and measures on the security of internet of things. International Journal of Plant Engineering and Management, 23(03), 27-32.
[2] Islam, M. S., Ivanov, S., Robson, E., Triona Dooley-Cullinane, & Balasubramaniam, S. (2019). Genetic similarity of biological samples to counter bio-hacking of dna-sequencing functionality. Entific Reports, 9(1).
[3] Nazeran, R., Sokhango, N. R., Kalat, A. N., Ostad-Ali-Askari, K., & Dalezios, N. R. (2018). Urban network analysis and pathology in central texture of mashhad metropolis from a passive defense point of view, case study of mashhad municipality, mashhad, iran. International Journal of Civil Engineering and Technology, 4(1).
[4] Goethals, P. L., & Hunt, M. E. (2019). A review of scientific research in defensive cyberspace operation tools and technologies. Journal of Cyber Security Technology, 3(1), 1-46.
[5] Liu, Z, Jin, X, Rongtao, S. U., Pengfei, M. A., & Zhou, P. (2019). Development status of high power fiber lasers and their coherent beam combination. Ence China Information ences, 62(04), 1-32.
[6] Zeng, H, Liu, Z., & Cai, H. (2020). Research on the application of deep learning in computer network information security. Journal of Physics: Conference Series, 1650(3), 032117 (7pp).
[7] Liu, H., Hussain, F., Shen, Y., Morales-Menendez, R., Abubakar, M., & Yawar, S. J., et al. (2019). Signal processing and deep learning techniques for power quality events monitoring and classification. Electric Machines & Power Systems, 47(14-15), 1332-1348.
[8] Sun, Q., Shen, M., Gu, X., Hou, K., & Qi, N. (2019). Evasion-pursuit strategy against defended aircraft based on differential game theory. International Journal of Aerospace Engineering, 2019, 1-12.
[9] Jing, X., Zhiping, C, Gang, H. U., & Ming, X. U. (2019). an active defense solution for arp spoofing in openflow network. Chinese Journal of Electronics, 28(01), 176-182.
[10] Zhou, Z., Kuang, X., Sun, L., Zhong, L., & Xu, C. (2020). Endogenous security defense against deductive attack: when artificial intelligence meets active defense for online service. IEEE Communications Magazine, 58(6), 58-64.