Transactions on Computer Science and Intelligent Systems Research
ISSN: 2960-1800, eISSN: 2960-2238 | Volume 1
AIEA 2023

Research On the Current Situation and Technical Exploration of Network Security in Power Monitoring System

Lulu Wang [1, a, *], Zhijun Wang [2, b]

[1] State Grid of China Technology College, Jinan, 250002, China

[2] Shandong Boxin Energy Technology Co. Ltd, Jinan, 250002, China

[a, *] 409598960@qq.com, [b] 18660109200@163.com

* Corresponding Author: Lulu Wang

Abstract. This paper analyzes the current situation of the network security of the power monitoring system, and discusses the weak link in the network security protection of the power monitoring system from the perspective of technical exploration. From the perspective of application, the application of trusted computing technology and malicious code technology in the security protection system of power monitoring system is discussed, so as to further ensure the network security of power monitoring system.

Keywords: Power Monitoring System; Network Security; Security Zone III; Malicious Code; Trusted Computing.

1. The Importance of Network Security in Power Monitoring System

The power monitoring system refers to a business system and intelligent equipment based on computer and network technology used to monitor and control the process of power production and supply, as well as communication and data networks as the basic support. The power monitoring system is used to support the safe and stable operation of the power system and ensure the reliable supply of electricity. However, with the continuous development of information technology and communication networks, the network security situation faced by the power monitoring system is becoming increasingly complex. In recent years, incidents such as the power grid blackout in Ukraine and the paralysis of Iran's nuclear power plant caused by the virus have once again fully demonstrated that cyber attacks have the characteristics of covert means, low attack costs, difficulty in obtaining evidence, and huge destructive power, which have a significant impact on society and the state [1-2]. As an important attack target in network warfare, the power monitoring system has always been at the forefront of network attack and destruction.

Once network security issues occur in the power monitoring system, it will threaten the normal operation of the system and even hinder the normal operation of the power production system. Therefore, the network security protection of the power monitoring system is of great importance.

2. Analysis of the Current Situation of Network Security in Power Monitoring Systems

State Grid Corporation of China has established a comprehensive power monitoring and security protection system in accordance with the overall security protection strategy of "security zoning, network dedicated, horizontal isolation, and vertical authentication", covering five levels of power grid dispatch agencies, various substations, and power plants. From the perspectives of security management, protection technology, and emergency backup, a multidimensional grid dynamic security protection system has been formed, achieving good protection effects. However, with the development of new technologies and the increasingly complex network situation, there are still risks.

Security Zone III provides information exchange between production control areas with stricter internal and protection requirements, and connects to internal networks and even the internet with relatively lower external protection requirements, which is a key link in the deep security defense

system. Security Zone III is located between the production control area and the information intranet, serving as a transit station for exchanging data between low security level areas and high security level areas. It is also a necessary path for hackers to penetrate from low security level areas to high security level areas.

The front-end servers carrying external access functions and back-end servers carrying business processing functions, office terminals, operation and maintenance workstations, and security equipment in Security Zone III are mixed in the same area. The equipment does not have differentiated protection, and the hosts and equipment that interact with data in the production control area are not provided with key protection. Security Zone III access terminals include office and operation and maintenance types. There are a wide range of office terminal users and their environments are complex. In terms of functionality, in addition to accessing Zone III business, they also access secure Zone IV portals, collaborative work, emails, etc., making them vulnerable to attacks against user terminals such as phishing emails. Security Zone III has not refined internal network access control, becoming a weak link in security protection. The operation and maintenance terminal has the highest control over the server, and different systems' operation and maintenance personnel, R&D personnel, and other personnel are mixed in use, posing risks such as personnel misoperation, malicious operation, and inability to audit and trace the source. There are various ways to connect to the public network, with many exposed areas. The security protection strength of the connection method accessed by the operator's dedicated line cannot be guaranteed. Once it is breached, it will directly enter the security zone III. Due to the lack of deployed web application protection measures in Security Zone III, the ability to resist web attacks is weak. Attackers can exploit vulnerabilities without hindrance and carry out various destructive operations.

3. Technical Exploration of Network Security in Power Monitoring Systems

3.1. Reasonable Division of Security Zones in Zone III

Strengthen the internal network structure of Security Zone III, improve security protection technical measures, improve the level of software and hardware autonomy and controllability, ensure the confidentiality, integrity, and availability of Security Zone III business, and prevent security risks from spreading through Security Zone III to production control areas. Take targeted measures to protect against differences based on the business characteristics of different network domains; Focus on protecting systems and equipment with wide exposure areas and critical locations.

Based on logical isolation methods such as firewalls, switch VLANs, and VRF, Security Zone III is divided into six domains: external service domain, backend support domain, real-time exchange domain, control cloud domain, operation and maintenance domain, and office domain. External service domain mainly includes web application server, data proxy server, Domain Name System server (DNS), load balancing (GSLB, SLB), etc. The backend support domain mainly includes backend servers in business systems that do not directly interact with users, servers that transmit data to production control areas, security management servers, etc. The real-time exchange domain is only used for servers that carry data exchange between the production control region and the security zone IV. The front-end of the regulatory cloud domain mainly includes application service virtual hosts allocated through computing resource pools, while the back-end mainly includes platform level virtual hosts allocated through computing resource pools, such as model management, data management, public components, platform management, and application services, as well as physical devices such as databases and storage resource pools. The operation and maintenance domain mainly includes various on-site operation and maintenance workstations, printers, etc. The office domain mainly includes the office terminals (including temporary offices), printers, etc. of employees in the regulatory department.

According to the principle of merging devices with the same business characteristics and protection requirements into domains, optimize the network structure of Zone III, reasonably divide security

domains, set strict access control policies between each domain based on the principle of minimizing and whitelisting, clarify business access paths, establish a minimum domain level access control strategy, and strengthen defense in depth. The access control strategy is shown in the figure. The backend support domain, real-time exchange domain, and control cloud domain backend and production control region business use forward and reverse isolation devices for access control; The operation and maintenance domain uses specific ports to achieve access control over the backend support domain, external service domain, and regulatory cloud domain; The external service domain uses specific ports to access the backend support domain; For the security IV area business, the office domain is directly accessed, and the real-time exchange domain is accessed through specific ports. The business of the factory and other Zone III must use specific ports to access external service domains. Adopting different access control strategies for protection based on the business characteristics of different security domains has refined network access and strengthened security protection in Zone III.

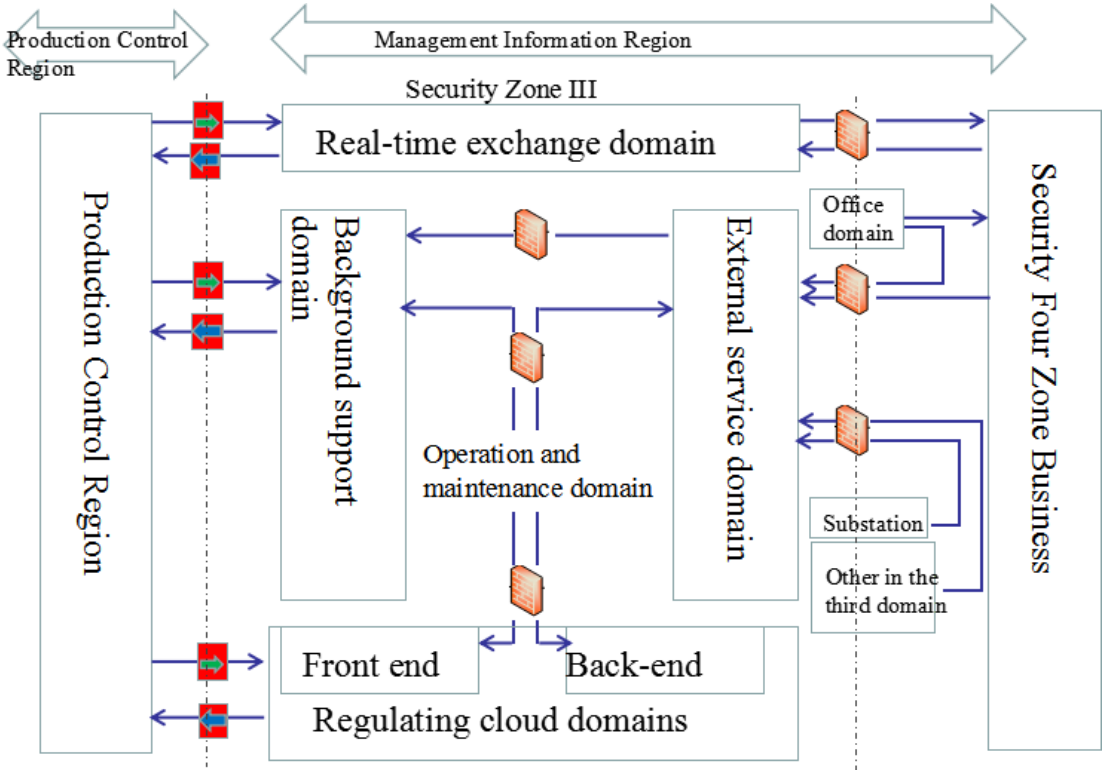

Figure 1. Schematic diagram of security domain information interaction

3.2. Malicious Code Protection Technology

The core advantage of malicious code protection technology is three-dimensional deep malicious code detection technology. The malicious code protection technology integrates three core technologies: traditional static analysis, AI analysis, and dynamic behavior analysis. These three detection technologies mainly analyze files, including executable files, exploit documents, web pages, scripts, etc. The core of traditional static analysis technology is an antivirus engine. Artificial intelligence analysis mainly extracts and models features such as files, codes, and behaviors of accumulated billions of virus samples, and uses machine learning and other technologies for continuous training to determine the reputation of suspicious files. The TSA traffic probe integrates this achievement, known as the RDM+engine. This engine is also purely localized and does not require cloud support. It only achieves a very high detection rate through a trained model of tens of megabytes.

Dynamic behavior analysis technology is implemented through an intelligent sandbox analysis system, abbreviated as sandbox. The sandbox is also a hardware device, each containing dozens of virtual machines that execute samples and monitor the behavior and risks during the sample execution

process. The sandbox has a large number of built-in decision rules and AI models, which have a very good effect on discovering unknown malicious code. At the same time, it can help users understand the risk behavior and malicious IP, domain name and other resources in the sample through analysis reports.

The intelligent sandbox, as an independent hardware device, has a standard interface for linkage with products such as TSA flow probes. Sandbox can automate security analysis of viruses, compare them with empirical rules and models, and output reports of malicious and suspicious files.

Deploy malicious code protection software to uniformly protect various hosts and terminals in Security Zone III from malicious code. Malicious code protection software should be able to detect and remove viruses, trojans, malicious programs, etc. At the same time, malicious code protection software should have self-protection function to avoid unauthorized uninstallation or exit. Prohibit sharing malicious code protection software between Security Zone III and Production Control Zone.

3.3. Trusted Computing Technology

Trusted Computing is a new computing mode for security protection. It has the functions of identity recognition, status measurement, confidential storage, etc., using passwords as gene antibodies, and can identify "self" and "non self" components in a timely manner, thus destroying and rejecting harmful substances entering the body, which is equivalent to cultivating immunity for network information systems [5-6].

The trusted verification architecture of the power monitoring system mainly consists of a trusted verification module, a trusted verification management module, and so on. The trusted verification module consists of a trusted root and a trusted software base. Trusted roots come in two forms: hardware and software, with hardware boards and software integration, providing password support and policy protection functions. The trusted software base implements trusted verification of boot programs, system programs, application programs, and important configuration parameters. The trusted verification module should be transparent to the operating system and business system, without affecting the functionality of the system and business. The trusted verification management module achieves centralized management of multiple trusted verification nodes, improving control efficiency.

By deploying a trusted verification module, key servers and workstations in the power monitoring system are equipped with active immune capabilities to prevent malicious code attacks. Through Trusted Computing technology, the protection and measurement evaluation of system software and application software in the operation environment of power monitoring system are realized, and the passive defense is changed into Active Defense. Utilize the existing network security monitoring system to achieve horizontal trusted information communication and vertical trusted collaborative defense in zones I, II, and III. The trusted verification management module is deployed on a dedicated server or workstation in the network area where the trusted verification module is located, directly communicating with trusted verification nodes, centrally managing trusted policies, updating applications, and viewing audit information.

The trusted operation status information, audit alarm information, policy change information, etc. of trusted verification nodes are collected through network security monitoring devices and submitted to the network security management platform. Realize information exchange with the network security management platform, and comprehensively evaluate and analyze the network security situation through the network security management platform.

4. Summary

This article analyzes the current situation of network security in power monitoring systems, proposes a protection strategy for security domain division in Zone III, which is a weak link in network security protection of power monitoring systems. It optimizes the network structure of Zone III and reasonably

divides the security domain; Clarify business access paths, establish a minimum domain level access control strategy, and strengthen defense in depth. At the same time, the application of malicious code technology and Trusted Computing technology in power monitoring system is introduced, so as to further ensure the network security of power monitoring system.

References

[1] Tong Xiaoyang, Wang Xiaoru. Network attacks caused by power outages in Ukraine and considerations for grid information security prevention [J]. Power System Automation. 2016, (7). 144-148.

[2] Qing Lai, Xin Shujun, Wang Jianhui, et al. Comprehensive Security Assessment of Information Energy Systems from the Ukraine Power Outage Event [J]. Power System Automation, 2016, 40 (5): 145-147.

[3] Meng Qingdong, Li Manpo, An Tianyu, et al. Design and Implementation of a Network Security Management Platform for Power Monitoring Systems [J]. Experimental Technology and Management, 2020, 37 (7):53-57.

[4] Xiao Annan, Zhu Hong, Zhang Weixiang, et al Research on Network Security Protection in the Power Internet of Things Environment [J] Electrical Automation, 2021, 43 (4): 94-97.

[5] Jin Xuecheng, Sun Wei, Liang Ye, et al. Design and implementation of an internal network security monitoring platform for power secondary systems [J]. Power System Automation. 2011, (16). 99-104.

[6] Li Man. Research on Network Security Situation Awareness and Prediction of Power Monitoring System [J]. Cyberspace Security. 2017, (10). 60-62.