2026 World Journal of Innovation and Modern Technology, Vol.9, Issue 7 (Jul)
ISSN 2682-5910
DOI: 10.66069/ojspub.26820709

A Defense-in-Depth and Zero-Trust Based Boundary Security System for Thermal Power Plant Information Areas

Ting Xu

Inner Mongolia Guohua Jungar Power Generation Co., Ltd., Inner Mongolia 017100

Abstract: ***Addressing the escalating boundary security risks in thermal power plant information areas (Zone III) due to remote O&M and Internet connectivity, traditional static defenses are inadequate against stealthy multi-stage attacks. This paper proposes a defense-in-depth system integrating identity authentication, channel encryption, behavior perception, and policy linkage, grounded in defense-in-depth theory, zero-trust architecture, and the MITRE ATT&CK model. Simulation experiments involving remote command execution and lateral penetration show a 92.7% detection rate and 89.3% lateral interception rate, while maintaining high availability for critical business systems. The study further provides an evaluable deployment strategy and indicator system, offering a replicable and implementable pathway for enhancing the security framework of thermal power plant information areas.***

Keywords: Thermal power plant information area, Boundary security, Defense-in-depth, Zero-trust, ATT&CK, Intrusion detection.

1. INTRODUCTION

In the information area (i.e., Zone III) of thermal power plants, with the deep integration of operation and maintenance systems, management systems, and the Internet environment, network attack threats have become increasingly severe, especially in typical scenarios such as remote maintenance, file exchange, and operation and maintenance terminal access, exposing significant boundary security risks [1]. The information area often opens external services such as VPN, Web portals, and email interfaces. After attackers invade Zone III through social engineering, network scanning, and credential abuse, they are highly likely to penetration into higher-privilege areas, threatening the stability and data integrity of the overall information system of the power plant [2].

Given that the attack scenarios in the information area of thermal power plants exhibit characteristics such as multi-channel entry, cross-platform interaction, and concealed behaviors, a single protection method is difficult to cover their complexity and dynamics [3]. Therefore, it is necessary to introduce a theoretical system with both multi-layer perception and strategy linkage capabilities. As the power industry continues to advance digital transformation, the interaction between industrial control systems and office information networks has become increasingly frequent, and the trend of network boundary blurring has become more obvious. As a critical energy infrastructure, the information area (i.e., the "Third Zone") of thermal power plants not only hosts core services such as management systems and operation and maintenance platforms but also has a high degree of connectivity with the Internet. In typical scenarios such as remote maintenance, file exchange, and terminal access, the exposed boundary surface continues to expand, becoming an important entry point for attackers to break through defenses and infiltrate high-privilege systems [4]. Attack behaviors often enter the Third Zone through social engineering, network scanning, credential abuse, etc., and then carry out lateral penetration or data leakage operations, seriously threatening the stability and data integrity of the power plant's information system. Therefore, studying the attack chain and its key behavioral characteristics, and constructing a protection model with identification and response capabilities, has become a key task for information security in thermal power plants.

2. RESEARCH STATUS AT HOME AND ABROAD

As the power industry continues to advance digital transformation, the interaction between industrial control systems and office information networks has become increasingly frequent, and the trend of network boundary blurring has become more obvious. As an important interface area connected to the Internet, the information systems in the Third Zone are facing unprecedented security challenges.

Domestically, research efforts are evolving from early isolation protection to a comprehensive in-depth defense system. Typical achievements include trusted terminal access architectures, bidirectional isolation mechanisms, and refined control strategies for service interfaces such as Web and VPN. Relevant studies emphasize enhancing the overall security and response capability of systems through unified identity authentication, security auditing, and behavioral analysis [7, 8]. In recent years, the zero-trust concept has also been gradually introduced to build more adaptive security perimeters in areas such as multi-factor authentication, dynamic authorization, and behavioral awareness. Internationally, NIST's SP800-207 "Zero Trust Architecture" and the IEC 62443 standard provide structured guidance for boundary isolation and secure communication between information systems and control systems [5, 6 10]. Meanwhile, some studies focus on multi-stage attack chain modeling, behavior-based intrusion detection mechanisms, and dynamic policy adjustment frameworks, forming a complete The whole process management system covers "identification defense response coverage"

Overall, both domestic and international studies indicate that the core of information area security lies in: constructing a boundary security mechanism with sustainable perception and dynamic response capabilities to limit attackers' latent space and lateral movement capabilities.

3. RESEARCH APPROACH AND TECHNICAL ROUTERESEARCH APPROACH AND TECHNICAL ROUTE

To address the above issues, this paper takes "attack identification-model construction-strategy deployment" as the main line. First, based on the MITRE ATT&CK framework, it systematically models common attack paths in the information zone of thermal power plants, forming an attack chain view that spans pre-attack reconnaissance, mid-attack penetration, and post-attack persistence. Combining real cases and security log analysis, it summarizes typical attack processes including phishing inducement, remote command execution, lateral privilege escalation, data exfiltration, and backdoor implantation, extracts behavioral indicators such as abnormal IP connections, a surge in login failure frequency, and abnormal behavior during non-working hours, constructs a risk database as the core feature input for subsequent dynamic detection mechanisms, and improves the system's ability to identify attacks characterized by "legitimate appearance, malicious behavior".

In the design of the protection system, this paper integrates the zero-trust architecture and the concept of defense-in-depth, and proposes a boundary protection model for the information area of thermal power plants, which is deployed around the four core principles of "trusted identity, channel encryption, behavior perception, and log auditing". On the one hand, it strengthens the user identity recognition mechanism through multi-factor authentication and a centralized permission control platform to ensure the legitimacy of the access source; on the other hand, it comprehensively adopts encrypted channels and dynamic access control strategies in the communication path to block illegal connection channels; at the same time, combined with Endpoint Detection and Response (EDR) and User and Entity Behavior Analytics (UEBA) methods, it establishes continuous monitoring capabilities based on behavioral characteristics, and relies on the SIEM platform to build a linkage audit mechanism to realize in-event identification and post-event traceability of attacks. In addition, through micro-segmentation and fine-grained policy control, it realizes the least privilege access within the information area, limits the scope of lateral movement, and compresses the attack surface from the system structure. The model has the advantages of clear policy layering, high compatibility, and flexible deployment, and can provide a replicable and evaluable technical path for the network security protection of the information area of thermal power plants.

To verify the actual effect of the proposed protection model, this paper constructs a simulated information area network environment including typical components such as VPN gateways, Web management platforms, and file transfer channels, and conducts empirical tests on the protection system by simulating various attack behaviors (such as remote command execution, session hijacking, lateral penetration, etc.). The experimental results show that after deploying zero-trust-oriented access control and behavior monitoring strategies, the system's detection rate for unauthorized access behaviors reaches 92.7%, and the interception success rate for lateral movement attacks increases to 89.3%. At the same time, with the help of the log centralized analysis platform, visual tracking of the attack chain is realized, and the average delay of incident response is reduced from the original 5 minutes to 1.8 minutes. In the comparative test, the average availability of the baseline system without this model was maintained at 83.6% when encountering combined attacks, while the system stability after integrating the protection model increased to more than 95%, and the false positive rate was controlled within 3%.

In conclusion, the boundary defense-in-depth security model proposed in this paper not only has transferability and scalability in theoretical structure, but also shows strong attack interception and incident response capabilities in actual deployment environments. Future research can further combine AI-driven behavior recognition models and automated policy adjustment mechanisms to improve the dynamic adaptability and intelligent linkage level of the model, providing more robust technical support for the network security construction of the information area of thermal power plants.

4. DEFENSE-IN-DEPTH PROTECTION MODEL FOR INFORMATION AREA BOUNDARIES

Based on the aforementioned attack chain modeling and strategy analysis results, this paper constructs a boundary in-depth protection model for the information area of thermal power plants. The model adopts an overall structure of "layered isolation, identity authentication, behavior recognition, and policy linkage", aiming to integrate the entire process of identification, analysis, protection, and response, so that attack behaviors are dynamically intercepted regardless of their entry point or internal propagation path.

The first layer of the model is the access control and identity authentication layer, which is mainly used to block unauthorized access attempts or credential abuse. At this stage, the system introduces a multi-factor authentication mechanism (such as dynamic token + device binding) and conducts real-time permission verification and policy matching for accessors through a centralized identity management platform. All access requests must pass through a unified access control gateway, which embeds Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) engines to dynamically authorize from multiple dimensions including identity source, access context, and behavior pattern, ensuring the access process has the least privilege, shortest duration, and narrowest access path.

The second layer is the channel encryption and communication control layer. The system uses the TLS 1.3 standard to perform end-to-end encryption for data transmission, ensuring that attackers cannot sniff or tamper with communication content during transmission. For VPN remote access channels, the platform enables distributed firewalls and VPN behavior audit modules to conduct path tracing and policy adaptive configuration for access behaviors. This mechanism can identify behaviors such as "abnormal switching of tunnel protocols", "high-frequency connection attempts", and "deviation of data packet encapsulation characteristics", and issue alerts and trigger policy restrictions in the first place.

The core layer of the model is the behavior perception and dynamic recognition layer. By introducing the UEBA (User and Entity Behavior Analytics) module, this layer constructs multi-dimensional portraits of user and device behaviors, and uses machine learning algorithms (such as cluster analysis and outlier detection) to conduct real-time identification of unexpected behaviors. For example, the model can quickly identify characteristic patterns such as "login behavior during non-working hours", "low-privilege accounts accessing highly sensitive data", and "terminals frequently jumping across regions in a short period". Once matched with existing attack chain characteristics, subsequent linkage response mechanisms are triggered. With the continuous update of the risk database, the behavior recognition module can significantly improve early threat detection capabilities in actual deployment.

The fourth layer is the in-depth isolation and policy implementation layer. This layer divides the systems in the information area into multiple logical subnets by deploying micro-segmentation technology, and core resources are only open to explicitly authorized terminals or users. The model deploys Policy Enforcement Points (PEP) at the boundary of each isolation zone to perform flow-level access control on network traffic. This mechanism ensures that even if an attacker compromises a node, their subsequent lateral movement is limited by policy isolation and cannot continue to expand the attack path.

The final layer is the strategy orchestration and coordinated response layer. The system uses the SIEM platform to uniformly collect log, behavior, strategy, and alert data, conduct threat level assessment, and trigger response processes. Through preset response templates and scripts, the platform achieves a closed-loop of functions such as automatic isolation, strategy adjustment, alert notification, and traceability analysis. In actual deployment, when the system identifies high-risk behavior in an account, it can complete access interruption, strategy convergence, and event reporting within 5 seconds.

Model implementation verification shows that in a simulated attack environment, the protection system achieves a 92.7% recognition rate for remote command execution attacks, increases the success rate of lateral penetration interception to 89.3%, and effectively reduces the success probability of attacks carried out through abnormal behaviors under legitimate identities. At the same time, the average false positive rate of the system is controlled within 3%, and critical business systems can maintain over 95% service availability when under attack, demonstrating the model's high reliability, timely response, and depth of security protection in actual combat environments.

In summary, through the synergy of multi-level linkage, dynamic response mechanisms, and sustainable learning strategies, the model constructs a highly operable, evaluable, and iterable in-depth security protection system for the information area of thermal power plants, and has good promotion and application value in improving overall network resilience and emergency response capabilities.

5. CONSTRUCTION AND DEPLOYMENT SUGGESTIONS FOR STRATEGY EVALUATION SYSTEM

To further promote the implementation and sustainable optimization of the information area boundary in-depth protection model, this paper constructs a security strategy evaluation system for thermal power plants and proposes hierarchical deployment suggestions based on previous experimental evaluation results and industry actual needs.

In terms of practical application adaptation, this paper proposes differentiated deployment suggestions based on the scale of the power plant and the complexity of the information system. For small or single-operation power plants, it is recommended to focus on lightweight boundary protection, with key deployment of VPN access control, behavior audit modules, and multi-factor authentication components, prioritizing the implementation of external access control and account permission cleanup. On this basis, combined with micro-segmentation strategies to perform network segmentation on key nodes, effectively improving the initial protection level. For enterprise types with multiple plants and a centralized group operation and maintenance model, the focus should be on a centralized control platform as the core, unified management of authentication access, strategy distribution, and log collection, and the construction of a cross-regional, orchestratable, and visual security operations center (SOC). This model achieves unified management and dynamic risk response for subordinate sites by introducing a strategy orchestration engine and automated analysis tools.

In terms of promotion path, this paper suggests adopting a phased deployment strategy of "core first, gradual expansion". The first phase should focus on key access entry points such as VPN gateways, email systems, and Web services, deploying a centralized authentication platform, UEBA behavior analysis system, and EDR terminal response mechanism to quickly establish an initial protection system. The second phase expands to cross-system access control and dynamic policy update functions, introducing micro-segmentation gateways and policy linkage platforms to achieve multi-dimensional policy response and attack chain cascading analysis capabilities. The final phase combines AI-assisted policy generation and adaptive detection models to realize the intelligentization and closed-loop optimization of the protection system. In terms of policy maintenance, a continuous update mechanism based on threat intelligence should be established, combined with security incident drills and policy version control, forming a "deployment-evaluation-optimization" trinity closed-loop management of the policy lifecycle.

6. CONCLUSION AND OUTLOOK

Focusing on the boundary security challenges faced by the information area (Zone 3) of thermal power plants, this paper proposes and verifies an information area network security protection model that integrates attack chain modeling, behavior feature extraction, and in-depth defense strategies. The research results show that the identification mechanism established based on the MITRE ATT&CK attack chain view can efficiently extract typical threat paths such as remote command execution, lateral penetration, and session hijacking, and combined with key behavior features such as abnormal login and off-hours operations, a risk database with practical value is constructed, providing reliable data support for model deployment.

By introducing the concepts of defense-in-depth and zero-trust architecture, this paper constructs an overall model architecture of hierarchical isolation, identity authentication, behavior perception, and policy linkage, realizing a closed-loop mechanism from access control, channel encryption, behavior modeling to policy response.

Simulation results show that the model outperforms traditional firewall-based boundary policies in multiple key indicators such as attack interception rate, response delay, false positive control, and system availability, effectively curbing attack paths disguised with legitimate shells and internal lateral movement behaviors, and significantly enhancing the security resilience and management capabilities of Zone 3 in high-threat environments.

At the same time, combined with the actual operating environment of power plants, this paper designs a differentiated deployment strategy and an evaluable policy implementation indicator system, providing a phased and replicable promotion path for the security construction of information areas in power plants of different scales and organizational structures. In particular, the technical framework constructed in terms of centralized authentication, micro-segmentation policies, behavior recognition, and policy linkage has good compatibility, maintainability, and scalability, and has met the conditions for engineering implementation.

Looking ahead, as the digitalization level of the power industry continues to improve, the Third District Information System will undertake more tasks of remote collaboration, data interaction, and intelligent control, and the challenges faced by network security protection will continue to evolve. In this context, it is suggested that future research focus on the following aspects: First, further integrate AI-driven adaptive detection mechanisms to improve the system's ability to identify complex behavior patterns and unknown threats; second, explore a dynamic strategy adjustment mechanism based on threat intelligence and attack graphs to achieve continuous optimization and closed-loop management of the model; third, carry out research on the design of multi-plant collaborative defense mechanisms and cross-regional situational awareness to enhance the information security collaborative guarantee capability of the overall power system.

REFERENCES

[1] Zhang Tao, Zhao Dongyan, Xue Feng, Zhang Bo, Zhang Rui. Research Framework of Information Security Protection Technology for Intelligent Terminals in Power Systems [J]. Automation of Electric Power Systems, 2019, 43(19): 1-8.
[2] Chen Tiezheng. Current Situation and Suggestions of Network Security Protection for Power Monitoring Systems [J]. Telecom Power Technology, 2020, 37(4): 109-110.
[3] NIST. Guide to Industrial Control Systems (ICS) Security: NIST Special Publication 800-82 Revision 2 [EB/OL]. National Institute of Standards and Technology, 2015.
[4] IEC. Industrial communication networks - Network and system security - Part 1-1: General requirements (IEC 62443-1-1) [S]. Geneva: International Electrotechnical Commission, 2018.
[5] Ten C. W., Liu C.C., Manimaran G. Cybersecurity for Critical Infrastructures: Attack and Defense Modeling [J]. IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans, 2010, 40(4): 853-865.
[6] Knapp E. D., Langill J.T. Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems [M]. Waltham: Elsevier, 2011.
[7] Gao Xiang, Liang Zongyu. A Brief Discussion on the Research of Network Security Protection Technology for Power Monitoring Systems [J]. Network Security Technology and Application, 2021(9): 123-124.
[8] Liu Rui, Hong Sheng, Li Wei, Wang Xin. A Review of Intrusion Detection Technologies for Industrial Control Systems [J]. Information Technology and Network Security, 2021, 40(3): 1-7.
[9] Sun Yanbin, Wang Hongyi, Tian Zhihong, Fang Binxing. Research on the Development of Security Protection Technology for Industrial Control Systems [J]. Engineering Sciences, 2023, 25(6): 126-13.
[10] NIST. Zero Trust Architecture: NIST Special Publication 800-207 [EB/OL]. National Institute of Standards and Technology, 2020.

Author Profile

Ting Xu (1999-), male, Han nationality, from Gansu Province, bachelor's degree, assistant engineer, research direction: application of network security in thermal power plants.