Application of Zero Trust Framework in Security Protection of Power Internet of Things

Hong Xu[1](✉), Leichun Gu[2], Shuhan Liu[1], Zhi-wei Hua[1], and Xin Li[1]

[1] State Grid Tongxiang Electric Power Supply Company, Tongxiang 314500, China
zhanghan@wudun.net

[2] Tongxiang Electric Power Engineering Co., Ltd., Tongxiang 314500, China

Abstract. Aiming at the problems that the security boundary of power information system is gradually blurred, and external attacks and internal threats are increasingly serious, the theory and practice of zero trust architecture at home and abroad have constructed a smart grid security protection architecture based on zero trust. The architecture mainly includes terminal trusted sensing Agent, multi-source data aggregation platform, intelligent trust evaluation platform, dynamic access control platform and trusted access agent. Finally, taking two typical application scenarios of terminal equipment data transmission and business office scenario as examples, the deployment scheme of power grid security protection architecture based on zero trust in power grid application provides suggestions for improving the security architecture of subsequent power information system.

Keywords: zero trust · Internet of things · Safety protection

1 Introduction

Human-computer interaction is a way for people to communicate with machines. For example, it needs five senses to feel the world. This is a way for people to communicate with nature, including vision, hearing, smell and taste. The way of human-computer interaction is very important. In the computer era of the last century, the Internet era mainly depended on mouse, keyboard and display screen, and then in the 21st century, it was mainly touch screen, which defined the entire era of smart phones, that is, the era of mobile Internet. The Internet of Things technology includes 5G, which belongs to the Internet of Things technology. In order to realize the interconnection of everything in the power Internet of Things, safe and convenient identity authentication is a necessary prerequisite.

With the rapid development of computer network and information technology, emerging technologies such as "the edge of the big cloud moves the wisdom chain" have been widely used in the electric power industry. The construction scale of electric power information system is constantly expanding, the complexity is constantly increasing, the types and quantities of equipment connected to the network are greatly increased,

N. Akhtar et al. (Eds.): PMIS 2023, AHIS 8, pp. 839–846, 2023.
https://doi.org/10.2991/978-94-6463-200-2_87

and the services and functions provided by the system are diversified, high-quality and precise. However, with the rapid development of emerging technologies and the extensive deployment of information industry, the security boundary of power information network is gradually blurred, and external attacks and internal threats are increasingly serious. The traditional grid security architecture, which focuses on network boundary protection and gives default trust to users, equipment and applications in the system to a certain extent, can no longer fully meet the security protection requirements of power information system, and the security situation of power information system is not optimistic. In order to solve the problem that the traditional security protection system based on network boundary gradually fails, the concept of zero-trust security architecture that dynamically builds security boundary by continuously measuring identity came into being.

2 Literature Review

The proposal of Pan-power Internet of Things has aroused strong repercussions from all walks of life, especially the construction of Pan-power Internet of Things, which has become a hot issue by introducing new network security issues. With the development of ubiquitous Internet of Things business, the introduction of new technologies makes the network boundary more and more blurred, and the existing boundary-based security protection methods are no longer applicable; At the same time, with the increasing number of Internet of Things terminals, the traditional digital certificate authentication system based on the center cannot meet the demand of the ubiquitous power Internet of Things for reliable and efficient interconnection, and a new identity authentication method needs to be established urgently. In addition, in the application scenario of ubiquitous power Internet of Things, a large amount of sensitive data and user information are stored in the cloud, and the whole life cycle of the data is beyond the scope of traditional network security, which poses a huge security risk [1, 2].

3 Security Protection System of Ubiquitous Power Internet of Things Based on Zero Trust

3.1 The Concept and Advantages of Zero Trust Security

Zero trust was first put forward by John Kindervag in 2010. Its core idea is that by default, no one, equipment or system inside or outside the network should be trusted, and the trust foundation of access control needs to be reconstructed based on authentication and authorization. After years of practice, Google released BeyondComp, a zero-trust architecture, in 2014, and the zero-trust architecture was gradually recognized by the industry. Zero-trust subverts the paradigm of access control, and guides the security architecture from network-centric to identity-centric. Its essential appeal is to conduct access control with the role as the center. In the process of the ubiquitous power Internet of Things, the application of modern information technology such as “big cloud, intelligent chain” realizes the interconnection of all things and man-machine interaction in all links of the power system, and the boundary of the terminal side network will become blurred and complicated, so the traditional boundary-based security architecture is difficult to protect. The assets of power grid are huge, scattered, diverse and complex. The construction of pan-power Internet of Things will be based on the construction of a unified identity. The security protection based on "zero trust" can break the traditional border protection thinking and help the "three-type, two-network, world-class" energy Internet. Based on the "zero-boundary" ubiquitous power Internet of Things security protection system, taking the zero-trust network security architecture as a reference, unified identity management is carried out to realize the identity authentication between ubiquitous Internet of Things devices and services. According to the environment attribute and access attribute of the equipment, dynamic permission control is carried out [3].

3.2 Perception Layer Identification and Identity

With the continuous development of the company, at present, there are more than 500 million terminal devices connected to the company's system. It is planned that by 2030, the number of devices connected to the ubiquitous power Internet of Things system will reach 2 billion, and the entire ubiquitous power Internet of Things will be the largest IoT ecosystem with connected devices. In addition to the diversification of equipment, users and applications are constantly increasing. To solve the above problems and improve the company's information security capability, it is necessary to fully identify and complete identity management. By constructing the unified identification library of ubiquitous power Internet of Things, it provides basic key identification for business, and ensures the standard unification of the main body of business system. Establish a unified identification system for all physical objects, and provide a unified identification technology and operational basis for identity and access control management. A comprehensive identity cross-application management mechanism is implemented between business systems with a unified user identification central database of internal and external personnel, terminal equipment, business applications and other dimensions.

3.3 A Credible Unified Identity Authentication Mechanism

After the realization of full identity, in order to meet the unified identity authentication needs of the ubiquitous power Internet of Things, it is necessary to improve the existing identity authentication system, build a secure, reliable, flexible and lightweight identity authentication mechanism, and improve the company's information security guarantee capability. In the aspect of identity authentication based on zero-trust architecture, it takes identity as the center, completes centralized identity management by fully identifying users, devices and applications, achieves the continuity of authentication through device list service, and evaluates trust through continuous authentication means. Initial login is based on ease of use, and multi-factor authentication elements are improved. According to the safety level or continuous certification risk assessment, the secondary certification needs multi-factor certification. In this usage scenario, the key identification and authentication technology based on FIDO, Fast Identity Online) has a good applicability to solve the identity authentication problem. O FIDO is based on asymmetric cryptographic algorithm, and adopts local biometric authentication method to realize the rapid identification of user identity, without certificates or passwords, and without transmitting biometric information to the server, thus effectively preventing user privacy leakage. Multi-dimensional identification (including user identifier, public key identifier, biometric identifier, device identifier, application identifier, trusted application list identifier, etc.) is provided for all kinds of entity objects (personnel, equipment, applications, etc.), and a unified identification mechanism decoupling authentication mode from authentication protocol is realized, which can make full use of various electronic certificate, such as biometric features (fingerprint, face, voiceprint, iris, etc.). The FIDO specification generalizes the terminal security policy control principle of the power Internet of Things, and converts the traditional biometric identification technology of symmetric key into the biometric identification technology of asymmetric key system. This not only guarantees the privacy of users, but also improves the security and convenience. A fast, flexible and mutual authentication mechanism based on password infrastructure is constructed, which solves the security problems such as the password naturally exists in weak password, hits the database, and it is difficult to confirm the true identity of users, as well as the usability problems such as being difficult to remember and maintain. It can be embodied in the trusted interconnection of power Internet of Things [4–6].

4 Power Grid Security Protection Architecture Based on Zero Trust

The purpose of security protection of the power Internet of Things is to protect against various potential security risks that may occur in the power grid, so as to ensure the normal operation of the power grid, protect the legitimate rights and interests of users, solve the problems of network paralysis, system damage, data loss, information leakage, virus infection and harmful information transmission, and play its maximum role in the safe and stable operation of the power Internet of Things, and continue to promote the development ability of power enterprises. Facing the current security situation of power information system with increasingly serious attack threats and urgent security protection requirements, this paper adds zero-trust security components to its existing security architecture, and combines it with security devices such as firewalls and power monitoring systems already deployed in the power grid to construct a grid security protection architecture based on zero trust (see Fig. 1). The architecture mainly includes terminal trusted sensing Agent, multi-source data aggregation platform, intelligent trust evaluation platform, dynamic access control platform, unified security management platform and trusted access agent [7].

4.1 Terminal Trusted Sensing Agent

In power grid, typical terminal access scenarios include users, equipment terminals and application systems. Users include employees of power grid enterprises, suppliers, power users and other users, equipment terminals include on-site acquisition components, intelligent service terminals, etc., and application systems include power grid push or company-built application systems. Trusted sensing Agent senses the environmental risks of power intelligent terminals, user equipment terminals, external application

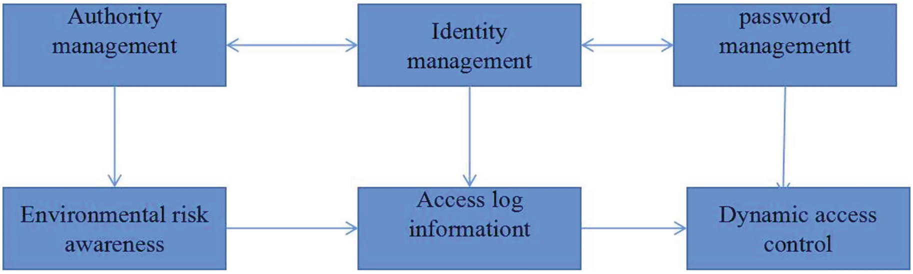

Fig. 1. Zero-trust power grid security protection architecture

servers and other devices, identifies and collects the status of users, devices and applications, and reports the status and identity information of devices to the environmental sensing system [8, 9].

4.2 Intelligent Trust Evaluation Platform

The intelligent trust evaluation platform can continuously evaluate the trust level and risk level of network entities and access requests based on the trust evaluation algorithm, combined with multi-dimensional real-time attribute information such as perceived detection data reported by the multi-source data aggregation platform, trusted access agents and reported access logs, and push the evaluation results to the dynamic access control platform to provide a judgment basis for access authorization. The access level of each user or device can be changed at any time according to the change of environmental information, thus realizing the dynamic construction of security boundary. The core of the intelligent trust evaluation platform is the trust evaluation algorithm, which maintains the normal operation of the whole security access control platform (see Table 1).

The input of trust algorithm includes user information, device information, device status, access information, behavior attributes and external threat information. The design of the algorithm can measure the information attributes, match the static rules, compare with the corresponding benchmark values, calculate the deviation, summarize and analyze the risks, so as to obtain the trust level of the visit, and then make the final judgment according to the attributes of the resources to be visited, and the benchmark values can be dynamically adjusted. You can also use neural network, artificial intelligence and other initiating methods, first extract the characteristics of the input system state data, and then continue to learn and train, so as to establish a trust evaluation model, and then output the trust level after the model evaluation. The output results can also feed back the calculation process of the model, thus improving the accuracy of the model output. This method can realize the intelligence and automation of trust evaluation, and can also have certain response effect to unknown network threats. In addition, in order to simplify the access process, you can also set a part of the white list, which allows users to access the application in the original way.

Table 1. Trust evaluation model and algorithm

userinfo	Behavior attribute	Equipment information	elicitation/heuristic method (of teaching) way
User ID	User access Business behavior	Equipment ID	visit information
User credentials	User access Operation habit	Location of equipment	Trust level
Users and roles	User access Equipment analysis	Algorithm process	output

4.3 Deployment Scheme of Typical Business Scenarios of Power Grid

Taking two typical application scenarios, data transmission of terminal equipment and business office scenario, as examples, this paper expounds the ground deployment scheme of power grid security protection architecture based on zero trust in power grid application.

1) Security construction of data transmission scenario of smart grid terminal equipment.

The security construction of terminal equipment data transmission scenario in smart power grid relies on access control area, through the strategies of terminal trusted perception, security authentication, etc., combined with the landing of zero-trust security architecture. This solves the problem of identity authentication and access control of the terminal, and allows the identity to be trusted. The trusted terminal with dynamic authorization can access and transmit data, and find and deal with illegal connections in time. The deployment scheme of smart grid terminal equipment data scene is shown in Table 2.

2) Safety construction of business office scene. In the security construction of smart grid business office scene, the terminal trusted sensing Agent and secure desktop are deployed to ensure the secure access of the terminal, and the trusted access agent is used to access the access control area. Deploy multi-source data summary platform, intelligent trust evaluation system, dynamic access control platform, etc. in the access control area, and conduct dynamic trust evaluation on access subjects to realize fine-grained access control [10].

Table 2. Smart Grid Terminal Equipment

Secure access area	Logical isolation	data centre
Access control area	Data upload	Control request
Dynamic access control	Issue instructions	Terminal security check
Intelligent trust evaluation	Credit agency	Terminal security check

5 Conclusion

In this paper, the combination of zero-trust protection and the traditional border protection framework of power information system not only solves the problem that the traditional border security protection gradually fails, but also realizes the double protection effects of important power information systems, applications and data. Under the dynamic security policy, the credibility of the visiting subject is continuously evaluated according to its identity, historical behavior, current visiting behavior and environment; The access subject's permission is dynamically given according to the principle of minimum permission, while the access object is hidden. This active defense mechanism can improve the ability to resist any threats, and can control each visit by changing the authorization policy. However, the authorization management policy does not involve the specific access business security policy and the access businesses are independent of each other, so they can develop independently.

References

1. Sharma, U. , & Gupta, D. . (2021). Analyzing the applications of internet of things in hotel industry. Journal of Physics: Conference Series, 1969(1), 012041 (11pp).
2. Juhi Jasiha E & Dr Rajeswari R. (2021). Implementation of abms with cuk converter for enhanced battery life using internet of things. International Journal for Modern Trends in Science and Technology, 7(5), 107-111.
3. Stone, D. , Michalkova, L. , & Machova, V. . (2022). Machine and deep learning techniques, body sensor networks, and internet of things-based smart healthcare systems in covid-19 remote patient monitoring. American journal of medical research.36(1), 9.
4. Tolba, A. , & Al-Makhadmeh, Z. . (2022). Modular interactive computation scheme for the internet of things assisted robotic services. Swarm and Evolutionary Computation 25(70-), 70.
5. Stergiou, C. L. , & Psannis, K. E. . (2022). Digital twin intelligent system for industrial iot-based big data management and analysis in cloud. Virtual Reality & Intelligent Hardware, 4(4), 279-291.
6. Hasanov, M. , Isakhanyan, G. , Dolfsma, W. , & Mahdad, M. . (2022). A smart web of firms, farms and internet of things (iot): enabling? collaboration-based business models in the agri-food industry. British Food Journal, 124(6), 1857-1874.
7. Choomyen, P. B. , Muangmeesri, B. , & Maneetham, D. . (2022). Management of water treatment systems automatically via the internet of things. Engineering, 14(9), 13.
8. Xie, X. . (2021). Construction of innovative computer training education mode under the environment of multiple intelligences internet of things. Journal of Intelligent and Fuzzy Systems43(13), 1-11.
9. Duraisamy, M. , & Balamurugan, S. P. . (2021). Multiple share creation scheme with optimal key generation for secure medical image transmission in internet of things environment. International Journal of Electronic Healthcare, 11(1), 1.
10. Sreelatha., P. . (2021). Smart and effective environment monitoring using internet of things. Bioscience Biotechnology Research Communications, 14(7), 258-262.