Design of security domain partition system for multi-domain optical fiber communication network based on optical encryption topology

Hanshuang Jia[1]*, Ka Zhang[2], Suiming Yang[3]

[1]School of Civil Engineering, Xi'an Traffic Engineering Institute, Xi'an, 710300, China

[2]China Chemical Engineering 14th Construction Co., Ltd, Nanjing, 210044, China

[3]ZTE College, Xi'an Traffic Engineering Institute, Xi'an, 710300, China

Keywords: Communication network security; Security domain division; Boundary integration

Abstract: With the rapid development of the economy, the business needs are multiplying, the functions of the computer system are continuously enhanced, and the complexity of the network is also increasing. At present, the main problems of the network are as follows: the network boundary is not clear enough, there is no unified planning for the security requirements of each part of the network, and the access to the core business system is not well controlled; there is no clear access control between the access systems, Networks can access each other, and the local security problems of the system can easily spread to the whole system. A scheme of dynamic security domain division is proposed to realize the dynamic security domain division of a system. From the perspective of depth, the deployment and application of security are comprehensively considered, and the network security is improved.

1. Introduction

With the development and progress of society, optical fiber communication technology, wireless communication technology, wired communication technology, etc., have been widely used, and the technical level and technical means are becoming more and more perfect, which have very good significance and function for the development of social economy [1]. In the construction of modern communication network, optical fiber transmission is one of the most important ways. Therefore, the security of optical fiber transmission in communication network is particularly important [2]. Based on the current security problems of optical fiber transmission in communication network, effective protection measures should be taken to ensure the good operation of communication network.

As the national basic information network, the information system attaches great importance to the network security work from the consideration of the enterprise's own business requirements and national requirements, so it is urgent to improve the level of information security [3]. In recent years, telecom enterprises have carried out a series of network security construction work in terms of technology, management, system and security organization. The main security work here refers to strengthening basic security management, including six pilot projects such as port service, patch management, terminal protection and security domain division [4]. It is necessary to build a three-dimensional, multi-level communication network security protection system from application systems, networks, hosts and other different levels; At the same time, on the basis of unifying borders and dividing security areas, we will realize key isolation and protection, and build a centralized and unified network security protection means. Under this background, in order to establish a good information security mechanism and telecommunications network, this paper defines the boundaries of security domains of each system [5]. Security domain refers to the set of regions or network entities in the network that have the same security protection requirements and trust each other. Because the application directions of different boundaries in the telecommunication network are different, the application requirements for security are also different. For example, the connection with business partners and the general extranet connection have different requirements for security [6]. After the principle of security domain division is formulated,

  DOI: 10.25236/icceme.2022.027

according to the requirements of security level protection, the protection level of each security domain is determined, and the corresponding security measures are deployed, among which the protection of security domain and border isolation are the key points.

2. The security domain of the communication network system and the problems existing in the network transmission process

Security domain division and boundary integration are the basis of security work [7]. A larger security domain can be divided into several security subdomains. At the same time, a security subdomain can also be divided into secondary security domain, tertiary security domain and so on. The division of security domain is to divide the system into different areas from the perspective of security and implement classified protection for the system [8]. After the security domain division principle is formulated, the protection level of each security domain is determined according to the corresponding level protection requirements, in which boundary integration and security protection are the focus of attention [9]. At present, there are some problems of unclear boundary and chaotic connection in the support system of telecom enterprises. In order to ensure the stable operation of business and improve the overall security of the network, the transformation and integration of network boundaries is a task that must be completed at present.

2.1. Security domain definition description

The security domain of the telecommunication network is divided horizontally and vertically. From a horizontal perspective, the support network is divided into three parts: service support domain, network management support domain, and management support domain. From a vertical perspective, each support system domain is divided into five security domains: core domain, switching domain, access domain, service domain, and terminal domain. The core domain is to divide the security domain according to the business function realization mechanism and protection level of each support system. That is, the core business system can be further refined according to the business area. The access domain is divided into three sub-security domains according to the overall network architecture of each supporting system: Internet interface sub-domain, external interface sub-domain, and internal interface sub-domain. Internet interface subdomain, the opposite end is the Internet, for example, the external Internet site of the business support system is the Internet interface subdomain of the business support system; external interface subdomain, the opposite end is a non-China Mobile system, accessed via a dedicated line; internal interface subdomain domain, the peer is inside China Mobile, and it is accessed through the mobile data communication network or other internal network.

The service domain is the area that provides security technical services for the support system, including authentication audit services, log audit services, patch upgrade services, antivirus services, and IDS monitoring services. Finally, through the hierarchical management model of security products, an independent secondary security service domain is established within each support system, and a primary security management domain is established in the company management support system domain, and then evolves into a security management center. The terminal domain, that is, the user domain, is divided into security user domains according to the classification of access users of the business system. User terminals that access the same type of data need to be protected at the same level and are classified as a type of secure user domain, including external user domains, business user domains, etc. There are three types of sub-security domains: domain and administrative user domain. The management user domain is the production and maintenance terminal, that is, the terminal that performs routine maintenance operations and management on the host, network, database, storage, and application systems; the business user domain, that is, the business terminal, refers to the service belonging terminal that accesses the applications of this support system. , differentiated according to the support system; the external user domain includes development and testing terminals, partner terminals and remote access terminals. The development and testing terminal is mainly used for development and testing, and is owned by the manufacturer, but is used in the support network; the remote access terminal is mainly used for system

maintenance, and the objects used include mobile employees or the maintenance personnel of the manufacturer. The terminal that accesses the support system for access by VPN, dial-up, dedicated line, etc. The switching domain refers to a switching area composed of high-performance switches that connects the above domains and provides inter-domain data exchange. It is the core of inter-domain data exchange. The security domain division of ordinary networks is mainly the division of logical functional areas, which distinguishes different user groups or objects to be protected. The most common way is the "3+1" division, as shown in Figure 1.

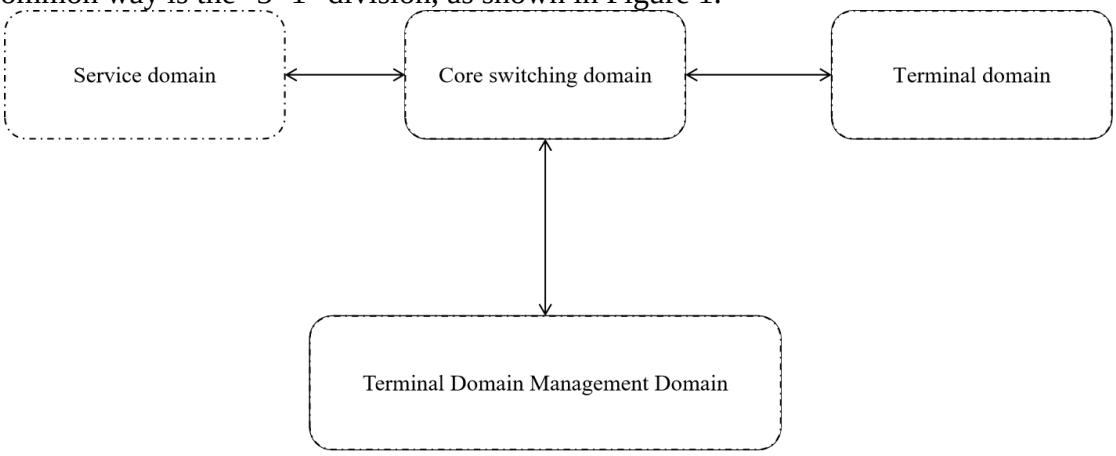

Figure 1 "3 + 1" security domain division

2.2. Problems in optical fiber transmission of communication network

(1) External causes in the process of optical fiber transmission in communication network. The so-called external factors are mainly some negative effects brought by natural weather, and its natural disasters often include typhoons, thunderstorms and hailstorms, etc. Under such natural weather, communication network signals are inevitably damaged in the actual transmission process, and its signals can't be transmitted on time to some extent.

(2) Internal problems in the process of optical fiber transmission in communication network. The so-called internal problem is often a factor opposite to external factors. To some extent, the internal factor is mainly the unreasonable installation process, maintenance process and technical detection process of the communication system, which leads to certain security problems in signal transmission. The internal problems existing in the process of optical fiber transmission in communication network are mainly reflected in the following points: ① Low automatic monitoring technology. Generally speaking, the communication network has a long distance of optical fiber communication. Once there is a problem in a certain link, to some extent, it will affect the transmission of the whole distance signal. In the process of fault determination, the signal transmission process will be difficult to get substantial guarantee, which will bring huge economic losses and fundamentally affect the overall development of our national economy. ② Uneven skills of maintenance personnel. Different maintenance personnel often have different levels of technical level. At the same time, in the process of optical fiber communication maintenance, the professional skills of the staff often play a direct and decisive role, which fundamentally seriously affects people's daily communication in the process of repairing a certain optical fiber fault. ③ The reliability of the signal is relatively low. In the actual safe transmission process of communication optical fiber, due to the different areas assumed by communication optical fiber, there will inevitably be various flaws in the signal transmission process, overlapping and hesitation in the signal transmission process, which to some extent has brought some troubles to the normal communication of local people. At the same time, in the actual communication process, it is inevitable to need a certain amount of electricity as the essential basic guarantee, and to some extent, the loose management mode of the power supply station is also the main internal influencing factor leading to the low reliability of the signal.

3. Security Domain Division

3.1. Division scheme

The division of security domain adopts sunflower structure, namely: flower heart: unified core bearer network, providing IP accessibility and restricted IP accessibility; Wreath: IP Bearer Network boundary; Calyx: the interaction area between the service module and the bearer network; Petals: define a single business function module. Security domain division is the basic work of security protection, which is mainly aimed at each business system. It combs out the security domain division scheme and protection strategy requirements of the business system. Its process mainly includes security domain division, relevant boundary integration and protection strategy implementation. Before security domain division, it focuses on combing the business process, clarifying the system functions, modules and relevant business network elements, and finally determining the security domain of the business system. The PFPE model of dynamic security domain division is shown in Figure 2.

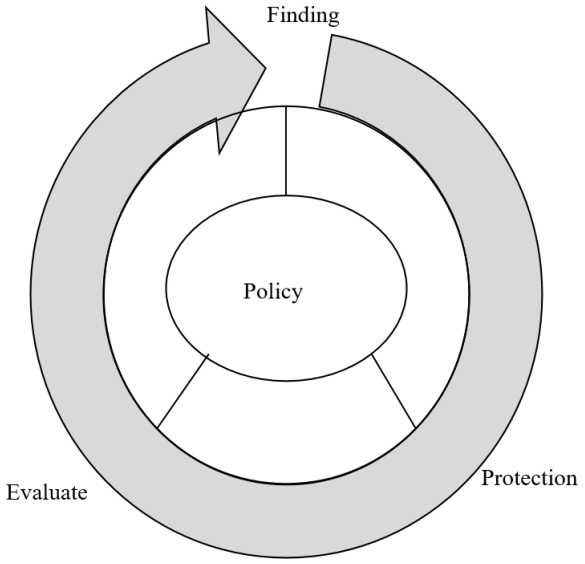

Figure 2 PFPE model of dynamic security domain partition

Partition steps:

(1) Clarify the basic topology of the security domain: The network topology is a necessary tool to understand the system network status and system composition. The network topology should include the constituent network elements of the system and the connection method between the network elements.

(2) Clarify the network exit of the security domain: sort out the current network exit situation, clarify the services and ports used by each business system, and clarify the target address.

(3) Sort out the current business process: conduct investigations and interviews on the data flow and processing activities of the system, and clarify the clear ownership of the system asset host.

(4) Security policy collection: Security policy collection is mainly to understand the security protection policy of the existing system when performing boundary integration and adjustment.

(5) Develop a network division plan: By dividing the network of the business system, focus on sorting out the asset ownership and division of each region.

(6) Discussion on the implementation of the transformation plan: After it is clear that the relevant safety domain transformation will be carried out, the specific safety transformation plan should be discussed, and the relevant participants and units of the implementation of the transformation plan should be confirmed.

3.2. Adjust and merge the security domain accordingly

(1) Make physical adjustments and merge. The physical integration of security domains is the physical adjustment and consolidation of the current system or multiple systems and corresponding

security domains. Its purpose is to improve the security level of the whole system through effective physical adjustment and consolidation. At the same time, it is more convenient to manage the whole system and fundamentally prevent network hazards. In practical work, some resources are often wasted, and this situation is not conducive to the overall security of the system. For example, when a system is in normal operation, sometimes multiple nodes inside the system need to be connected with the network outside the system. When connecting, due to the different communication ports used by each system, other auxiliary equipment is required to coordinate and connect, which not only increases the workload, At the same time, it is not conducive to the safety of the system. In view of this situation, it is necessary to adjust and merge the ports at the level in time. In this process, various types of ports should be unified first, and the system equipment used should also be unified accordingly. Moreover, through further integration, different systems with the same type of security domain can be adjusted and merged. Through such integration, the investment cost of different port construction can be effectively reduced, and the security domain can be unified after integration. On this basis, it is more convenient for staff to concentrate the protection forces together, so as to improve the protection level.

(2) Make logical adjustment and consolidation. Generally speaking, logical adjustment and merging refers to the full integration of a single logical boundary of the current system, in order to maintain high integrity and organization of the boundary of the system through effective boundary adjustment and merging. There will also be some specific security areas in the system. For this kind of area, the boundary should be handled flexibly according to the specific relevant requirements, so that it can be organically unified. The boundary between the network domain and the Internet, special line and intranet is the network boundary, which is an important boundary of the security domain.

(3) Security sub domain boundary integration: in addition to the boundary integration of security domains, there are also corresponding boundary integration between security sub domains, such as the integration between computing domains, service domains and maintenance domains.

With the development of information technology to the present stage, the invasion of network viruses not only has the characteristics of high speed, but also has the characteristics of long incubation period. In order to better realize the protection of network security, we must first set up an effective firewall in the system, and because the virus updates quickly, the corresponding firewall should be updated in time. On the other hand, we should pay attention to the long incubation period of viruses. Nowadays, electronic viruses can lurk in the system for 10 years without triggering. Once the trigger source appears, the virus will start immediately and cause harm to the system. Therefore, we can check the system itself while carrying out security protection, and remove all viruses to prevent them from the root.

4. Conclusions

After the security domain is divided, the network structure is clear, and the corresponding security protection strategy and security baseline configuration are established, which is more conducive to security protection deployment and daily operation and maintenance. In short, based on the division of security domains, the management and technical specifications of the security policy system are gradually implemented in the actual work of network security operation and maintenance, and the process of continuous improvement of the security policy system is completed through the accumulation of practical experience and data analysis. In addition, the establishment of safety maintenance management team is an important guarantee for the implementation of safety strategy system. Finally, the overall goal of "professionalization of network security operation, institutionalization of network security work, and visual management of the whole network security" will be realized.

References

[1] Guo Yunchao. Division and application of network security domain in telecom CRBT system

[J]. China New Communication, 2018, 020(011):167.

[2] Li Guilin, Jiang Fuhuan. On the idea of network security domain division of small and medium-sized state-owned industrial enterprises [J]. Digital Design, 2019, 8(18):1.

[3] Fan Jinjian, Xie Yifei. Design of Network Security System Based on Security Domain Division - Ensuring Safe Production of Tobacco Industry Enterprises [J]. Industrial Technology Innovation, 2019, 6(2):7.

[4] Wang Sheng, Jin Zhigang, Wang Pingjian. Energy Internet Routing Algorithm Considering Security Domain [J]. Power Information and Communication Technology, 2018, 16(10):7.

[5] Zhang Jiange, Huang Yanyan, Li Zhibo, et al. Research on Situational Awareness Data Management and Control Methods Supporting Cross-Security Domains [J]. Journal of the University of Information Engineering, 2018, 19(2):8.

[6] Liu Jiayu, Xun Guanglian, Cao Meng, et al. Research on network security construction of provincial agricultural scientific research units based on security domain [J]. Jiangsu Agricultural Science, 2018, 46(6):3.

[7] Ni Jian. Research on city network architecture based on security domain [J]. Wireless Internet Technology, 2021, 18(14):2.

[8] Zhong Lei, Liang Yeyu, Ning Jianchuang, et al. Research on the security of VoLTE-SBC network [J]. Communication Technology, 2019, 52(4):6.

[9] Zhang Jianquan, Li Jie. Research on network security system design based on security domain [J]. China New Communication, 2021, 23(3):2.