Advances in Computer Science Research, volume 78

3rd International Workshop on Materials Engineering and Computer Sciences (IWMECS 2018)

The Design of Network Information Security Based on Port

Rigui Zhou[1, a], Hao Wang[1, b, *]

[1]Shanghai Maritime University, Shanghai 201306, China;

[a] rgzhou@ shmtu.edu.cn, [b] wanghao@shmtu.edu.cn

Keywords: Information security, Security architecture, Security solution

Abstract: In recent years, network information security incidents occur frequently, network information security has risen to a national strategy. In order to ensure corporate network information security and prevent data leakage, the great harm caused by network infiltration attacks, this article designs the enterprise network information security architecture which takes 'Baseline for Classified Protection of Information System' and other standards as the basic guidelines.By combining the different regions and different levels of security measures into an organic security system, implementing of physical security, network security, host security, application security and data security aspects of the basic requirements, this design maximize the protection of security measures. The designed network information security architecture includes two aspects of management and technology, which ensure the security of enterprise network information in terms of data integrity, application and data security, device and computing security, network and communication security.

1. Introduction

All manuscripts must be in English, also the table and figure texts, otherwise we cannot publish your paper. Please keep a second copy of your manuscript in your office. When receiving the paper, we assume that the corresponding authors grant us the copyright to use the paper for the book or journal in question. Should authors use tables or figures from other Publications, they must ask the corresponding publishers to grant them the right to publish this material in their paper.

Ports are the hub for resource mobilization and resource allocation around the world on a global scale and play an important role in the development of urban economy and regional economy. With the development of Internet technology, the modern port is no longer just a transportation hub, nor even a logistics center, but an international shipping center. It is complemented by international economic centers, financial centers and trade centers. The development of technologies such as the Internet, cloud computing and big data, as well as the diversity and complexity of the development of the port business as well as the state's key protection regulations on key infrastructures all place higher demands on the information security of port networks.

2. Design Principles

As a port enterprise, once an enterprise network is invaded or data is leaked, it may bring great harm to national economy, people's livelihood and public interest. Compared with the traditional Internet, the technologies of attack, attack and protection in the era of big data are different from those in the Internet, cloud computing and big data era. Therefore, based on 'Baseline for Classified Protection of Information System' [2], 'Baseline for Classified Protection of Cloud Computing Information' [3], 'Specifications of Emergency Response Plan for information Security' [4] as the basic criteria for the overall design of the security architecture, by the different regions, different levels of security measures combined to form the final Organic information security protection and management system. Implementation of the basic requirements of physical security, network security, host security, application security and data security, so as to maximize the protection of security measures. Through the new design of safety technology, a comprehensive and effective safety

protection system is formed to maximize the protection of safety measures.

2.1 Safety Target

As the port business is 7×24 hours with many types of business and large volume of business. To build a secure architecture, not only ensuring functional safety, but also information security. Business sustainable, efficient and reliable, intelligent management are three basic indicators to achieve [5].

2.1.1 Business Sustainable

No matter what kind of emergencies happen to the links, networks, servers, applications, and data centers, the continuity of internal and external services needs to be ensured and the original data and services should be restored as soon as possible [6].

2.1.2 Efficient and Reliable

Publishing internal and external services requires efficient and efficient access, especially for core applications such as video conferencing, which need to be ensured the reliability and stability of use.

2.1.3 Intelligent Management

With a system to achieve user access effects, links, networks, servers, applications, databases and other comprehensive monitoring and intelligent early warning, it can achieve the fastest emergency response in the event of user access abnormalities, interrupts.

2.2 System Design Principles

Network security system in the overall design process should follow the following 9 principles:

2.2.1 Barrel Principle

The principle of network information security barrel refers to the balanced and comprehensive protection of information. "The maximum volume of a barrel depends on the shortest piece of wood." Network information system is a complicated computer system. Its inherent physical, operational and management vulnerabilities constitute the system security vulnerabilities. Especially the complexity of multi-user network system, resource sharing makes simple technology Protection is hard to detect. "Easiest Penetration Principle" used by attackers necessarily attacks the weakest part of the system. Therefore, the full, comprehensive and complete analysis of system security vulnerabilities and security threats, assessment and detection (including simulated attacks) are the necessary preconditions for designing information security systems. The primary purpose of security mechanisms and security services design is to prevent the most common types of attacks, with the fundamental goal of improving the "security floor" of the entire system.

2.2.2 Integrity Principle

In the event of a network attack, destruction of event, the network information center must be as soon as possible to restore the service and reduce losses. Therefore, the information security system should include security protection mechanism, security detection mechanism and security recovery mechanism. Security protection mechanism is based on the specific system of various security threats to take appropriate protective measures to prevent the illegal attacks. Security detection mechanism is to detect the operation of the system, timely detection and suppression of attacks on the system. Security recovery mechanism is the case of failure in the security protection mechanism, can take emergency response and try to recover information in a timely manner to reduce the extent of damage to supply.

2.2.3 Safety evaluation and balance Principle

For any network, the absolute security is difficult to achieve, nor is it necessary, so we need to establish a reasonable practical security and user needs evaluation and balance system. Security system is designed to correctly handle the relationship among needs, risks and costs, to be compatible

with security and availability and organizationally executable. There is no absolute judging criteria and metrics to evaluate the information is safe or not. It can only be determined by the system user needs and specific application environment, depending on the size and scope of the system, the nature of the system and the importance of information.

2.2.4 Standardization and Consistency Principle

System is a huge system engineering, the design of its security system must follow a series of standards, so as to ensure the consistency of all subsystems, so that the entire system can be interconnected securely and share information.

2.2.5 Combination of Technology and Management Principle

Security system is a complex system engineering, involving people, technology, operations and other elements. It is impossible to achieve by technology alone or by management alone. Therefore, we must combine all kinds of safety technology and operation management mechanism, personnel ideological education and technical training, and construction of safety rules and regulations.

2.2.6 Overall Planning, Implementing Step by Step Principle

Due to the unclearness of the policy requirements and service requirement, changes in environment, conditions and time, and advances in attack methods, security protection can not be achieved in one step. Under a more comprehensive security plan, we can establish a basic Security system to ensure basic and necessary safety. With the expansion of the network scale and the increase of applications, the changes of network applications and complexity, the vulnerability of the network will continue to increase in the future. Adjusting or enhancing the security protection can ensure the most fundamental security requirements of the entire network.

2.2.7 Hierarchy Principle

A good information security system must be divided into different levels, including the classification of the degree of confidentiality of information, the grading of user operation authority, the classification of network security (secure subnet and secure area), the classification of system implementation structure (Application layer, Network layer, Link layer, etc.) to provide comprehensive and optional security algorithms and security systems for different levels of security objects to meet various actual needs at different levels in the network.

2.2.8 Dynamic Development Principle

According to the changes in network security, it should constantly adjust the security measures to adapt to the new network environment, in order to meet the new network security needs.

2.2.9 Easy Operating Principle

First of all, the safety measures need to be done artificially. If the measures are too complicated and the demands on people are too high, safety will be reduced themselves. Second, the adoption of measures can not affect the normal operation of the system.

3. Requirements Analysis

In the era of cloud computing, the network threat characteristics, computing environment and security defense priorities have undergone great changes. The demand for network information security of large port enterprises relied on by China's export-oriented economy has also changed. Through the analysis of network information security incidents at home and abroad and the investigation of enterprise network security architecture, this paper presents the current network information security needs in the cloud era, including data security, software security, hardware security, physical and environmental security, comprehensive security, emergency response to safety and so on.

All manuscripts must be in English, also the table and figure texts, otherwise we cannot publish

your paper. Please keep a second copy of your manuscript in your office. When receiving the paper, we assume that the corresponding authors grant us the copyright to use the paper for the book or journal in question. Should authors use tables or figures from other Publications, they must ask the z

As the port business is 7×24 hours with many types of business and large volume of business. To build a secure architecture, not only ensuring functional safety, but also information security. Business sustainable, efficient and reliable, intelligent management are three basic indicators to achieve [5].

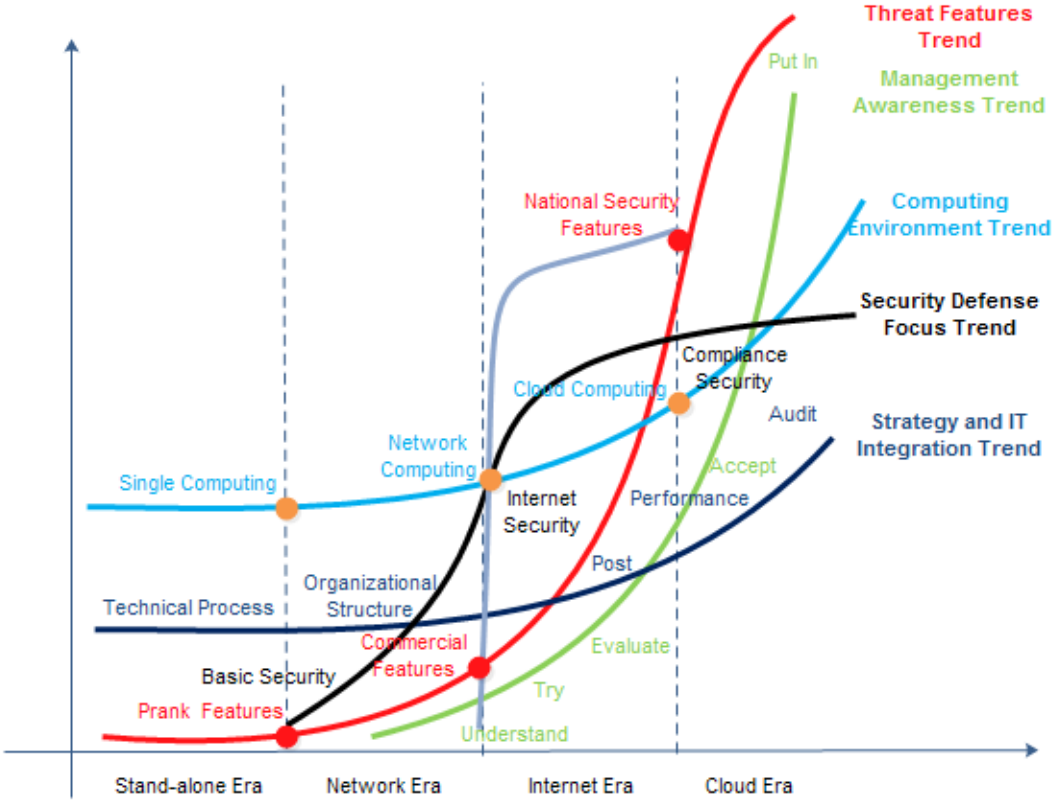

Fig. 1 Information security and defense system development trend

3.1 Data Security Requirements

Large port business will produce a huge amount of business data, at the same time have a data interaction with the customs, the national seizure, and the Port Authority. Large amount of data, large attack surface brings great challenge to the data security. The data security requirements mainly include two aspects. One is the security of the data itself, such as data privacy, data integrity, two-way strong authentication and so on, and the other is the security of data protection, which mainly uses the modern information storage means to data proactive protection, such as through the disk array, data backup, disaster recovery and other means to ensure data security. It need to ensure data confidentiality, integrity and availability.

3.2 Software Security Requirements

The port has a great deal of business, and interacts with government departments and business supervisors, which needs to install more application software. The applications that other departments require to install do not control its source. However, in addition to meeting the functional requirement and the performance requirement, the application software required by the enterprise also needs to meet the requirement of security and the software attributes related to preventing the unauthorized or intentional or unintended access of the program technical office to ensure that there are no vulnerabilities and safe back door and so on. Software security requirements are identified by reference to Secure Coding Specification and best practices.

3.3 Hardware Security Requirements

The key information infrastructure and key technology equipment play a key role in the network information security, and hardware is an essential component of data storage and computing. Therefore, we must make "autonomous control" of the key information infrastructure and key core technology and equipment - domestic equipment should be chosen. For non-critical infrastructure, to meet the performance, price and other conditions, should also give priority to the choice of domestic equipment.

3.4 Physical and Environmental Safety Requirements

To ensure the safe and reliable operation of the information system can provide a safe operating environment, the information system is physically tight protection, thereby reducing or avoiding various security risks.

3.5 Comprehensive Security Requirements

In addition to hardware and software security and physical environment security, there is one issue that needs to be considered, that is system and strategy security. The most secure software and hardware also need people to operate, so "human" is the most important factor in information security. Therefore, enterprises should establish a complete and complete leading agency of information security, management system, security strategy, professionals and so on.

3.6 Emergency Response Requirements

Due to the continuous operation of 7×24 port business, variety of businesses and traffic volume, once a hardware or software fails, data breach or other information security incident occurs, the security team needs to make emergency response in time, restore the normal operation of the system and fix the vulnerability, investigate the incident, and finally conduct security reinforcement.

4. Program Design

According to the characteristics of the port business, we put forward the data security, software security, hardware security, physical and environmental security [7], comprehensive security and emergency response security requirements of network information security. According to these requirements, we propose the network information security for our enterprise and other ports program design, which can be divided into technical requirements and management requirements, and further refinement for the protection requirements.

4.1 Management Program Design

Because "human" is the most important factor in the network information security incident, it is necessary to establish the leading organization of information security and the corresponding rules and regulations, including organizational management, mechanism construction, safety planning, safety inspection, emergency response, situational awareness and capacity building, Technical testing, safe and controllable, team building, education and training and funding support.

4.2 Technical Program Design

Technology program is to build a new generation of security system - active defense system. Active defense system using the basic equipment firewall, OfficeScan, online antivirus software, IPS, access systems, fortress machine, two-factor authentication, vulnerability scanner and database firewall.

Through the establishment of such a set of active defense and safety system, we will eventually achieve overall defense and zoning segregation; actively guard both internal and external defense; self-defense and active immunization; and defense in depth, with equal emphasis on technology and management.

Table 1 Active defense system

Active Defense System	APT, Dynamic Perception, SOC
	Professional Security Services: Penetration Test, System Security Test, Secure Operation and Maintenance .etc
	Vulnerability scanner, Database firewall, Two-factor authentication, Firewall, OfficeScan, Anti-virus software, IPS, Access, Fortress Machine
	Servers, Switches, Load Balancing, Data Backup, Disaster Recovery, Gatekeepers, Encryption Machines

Active defense system is divided into four levels, the bottom is the server, switch, load balancing, data backup, gatekeeper, encryption and other basic network equipment; the second layer for vulnerability scanner, database firewall, two-factor authentication, firewall, Software, IPS and other conventional security services; the third layer for penetration testing, system security testing, security operations and other professional security services and security management system; the top layer is the APT (Advanced Persistent Threat), situational awareness, security Management platform (SOC) and other professional security team and services.

In this defense system, we emphasize the basic supporting role of data (internal and external data), emphasize the central role and value of personnel in this security system[8], emphasize the importance of security operations as a daily safety task, and emphasize situational awareness as a monitoring and warning, emphasize the importance of coordination and linkage among equipment, equipment, people and data, emphasize the enhancement and improvement of the security system by threat intelligence and offensive and defensive drills[9].

4.2.1 Network Architecture

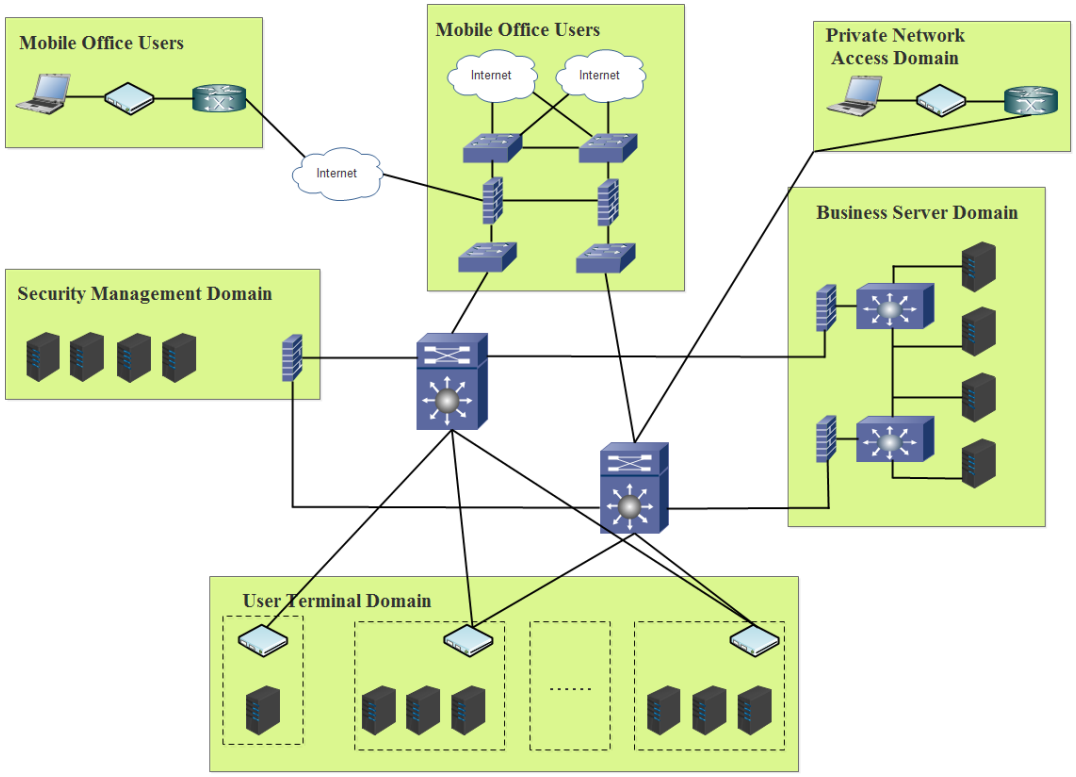

Fig. 2 Network Architecture

The newly proposed network architecture design is as shown in Figure.2. The corporate network is in regional division, namely Internet access domain, security management domain, business server domain, mobile office domain, user terminal domain, private network access domain. Among them,

the Internet access domain, security management domain, business server domain, mobile office domain, and user terminal domain are similar to the ordinary enterprise network. The special one is the private network access domain [10]. Due to the data interaction with the government administration department and the business regulatory department [11], so it need to access the corresponding private network. And the private network is part of the enterprise network architecture, but the protection level of the security protection especially the data security is high, requiring special attention to protection.

4.2.2 Security Architecture

The security architecture further subdivides the domain based on the network architecture and divides it into a private network external domain, an Internet export domain, an external service domain, a terminal access domain, an operation and maintenance management domain, a core service domain, and other service domain, adding security products to different domains to ensure network and system architecture security [12]. For example, the operation and maintenance management domain includes the security awareness platform, the log audit system, the operation and maintenance bastion host, the antivirus server and the vulnerability scanning system [13]. The terminal access domain accesses the office equipment so that the Internet behavior management is performed [14]. Private network outside the domain is mainly connected to the Port Authority, the national inspection, customs supervision business systems and other external private network. Except the corporate portal in foreign service domain, there are external web business services for online business server.

Security products deployed in different regions in the security architecture have different roles and meet the security needs. Through the deployment of security products such as firewalls, intrusion prevention, anti-virus modules and online behavior management, the requirements for network information security such as access control, intrusion prevention, malicious code filtering, structural security, resource control, and communication security are met [15].

5. Conclusions

According to the development trend of network information security at home and abroad, this paper puts forward the network information security requirements of port enterprises under the era of big data, Internet, cloud computing and so on. Based on the "Baseline for Classified Protection of Information System" and "Baseline for Classified Protection of Cloud Computing Information", the construction of network information security of port enterprises is carried out. The construction of network information security system is proposed from two aspects of management and technology.

In the management of "human" as the basis, the establishment of information security leadership and the corresponding rules and regulations, including organization and management, mechanism construction, safety planning, safety testing, emergency response, capacity building, team building, education and training and funding guarantee. Technically, it has set up a set of active defense system based on professional security services such as basic network equipment such as gatekeepers and encryption machines, vulnerability scanners, database firewalls, firewalls, IPS and other regular security services, penetration testing, and security operation and maintenance. Through this set of active defense and safety system, it will eventually achieve the overall defense and zoning isolation; active protection, both inside and outside; its own defense, active immunization; defense in depth, both technology and technology. This system into a network of information security programs, to achieve a systematic construction will not only improve the efficiency of safe operation and maintenance, but also from the source to improve the security of port enterprise network architecture.

References

[1] People's Republic of China Network Security Law 2016-11-08.

[2] GB/T 22239-2008.Baseline for Classified Protection of Information System Security[S].

[3] GB/T 22239-2008.Information Security Technology-Baseline for Classified Protection of Information System Security[S].

[4] GB/T 24363-2009.Information Security Technology-Specifications of Emergency Response Plan for information Security[S].

[5] Li Hui, Sun Wenhai, Li Fenghua, Wang Boyang. Secure and Privacy-Preserving Data Storage Service in Public Cloud[J]. Journal of Computer Research and Development, 2014, 51(7):1397-1409.

[6] Fan Xiaoguang, Chu Wenkui, Zhang Fengming, Surveys of Software Safety[J]. Computer Science, 2011, 38(5):8-13. Yang Chuang.

[7] Wang Dong, Network Security Hardware Platform Development Trend[J]. Information Security and Communications Privacy, 2006(9):35-36.

[8] China Standard Press Room 4. Information Security Standard Assembly. Technology and Mechanism Volume. Physical Security Technology Volume [M]. China Standard Press, 2009.

[9] You Shuangyan, Research on Establishing of State Specifications of Emergency Response Plan for Information Security[D]. Xi Dian University, 2009.

[10] Zhou haigang, Qiu Zhenglun, Xiao Junmo, Network Active Defensive Security Model and Architecture[J]. Journal of PLA University of Science and Technology, 2005, 6(1):40-43.

[11] Zhao Hongjing, Zhou Chongming, Zhai Pingli, et al.Intrusion Decoy Based on Network Active Defense Security Model [J]. Journal of Air Force Engineering University (Natural Science Edition), 2010, 11 (3): 76-79.

[12] Dai Chao, Pang Jianmin, Shan Zheng, et al. Design and Implementation of Border Malicious Code Prevention System [C], First National Information Security Level Protection Technology Conference.

[13] Meng Zhaoguang, Application of Firewall in Security Border Protection[J]. Information and Communications, 2015(2):169-169.

[14] Li yanrui, Zhao Zheng, An Enterprise Security Framework Based on PKI/PMI[J]. Computer Engineering and Design, 2003, 24(12):95-96.

[15] Tanja Zseby, Michael Kleis, Thomas Hirsch. Self-Protecting Networks – How Cooperation Strategies Can Strengthen Network SecuritySelbstschützende Netze – Netzwerksicherheit durch Kooperation[J]. Methoden und innovative Anwendungen der Informatik und Informationstechnik, 2008,50(6).