2023 IEEE 3rd International Conference on Power, Electronics and Computer Applications (ICPECA) | 978-1-6654-7278-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICPECA56706.2023.10075946

Research on Network Information Security Service Model Based on User Requirements under Artificial Intelligence Technology

Xu Li
School of Intelligent Manufacturing and Information Engineering
Sichuan Technology & Business College
Chengdu, China
470792941@qq.com

***Abstract*—This paper proposes a general network security framework based on artificial intelligence technology. Then the relationship between security objectives, security boundaries, security system elements, security services and security risk assessment are described. The modeling methods of security objectives, security boundaries and security system elements are given by using the power and universality of Unified Modeling language (UML). On the basis of building the network scenario, this paper sets up the association rules of network information security event detection and constructs the information security risk measurement model from the three perspectives of network database security vulnerability, data islanding risk and network security protection ability. Finally, a typical network example is given to analyze the application of the above model and algorithm in network security evaluation and optimal active defense. The analysis results show that the model and method presented in this paper are feasible and effective.**

Keywords—artificial intelligence, user requirements, network information, the security services

I. Introduction

The network security system is a complete system covering "attack, prevention, detection, control, management, evaluation" multi-stage combination of security management and security technology. In view of the importance of network security system, domestic and foreign research organizations and personnel have carried out a wide range of research, according to the different main research objects, can be divided into three categories: security technology system research, security management system research, comprehensive security system research [1]. Many researchers have made great achievements in hierarchical protection. Some scholars combined the information security performance measurement and information security level allocation, and established a multidimensional information security index system. They proposed a quantification model of information security level protection based on security index. Some scholars put forward a software security requirement analysis method based on threat modeling combined with the Implementation Guide, and integrated the hierarchical protection idea into the software security design stage by evaluating attacks through threat-attack graph (TAG). In this way, the solution can improve the software design more efficiently to enhance software security. Some scholars have proposed the implementation scheme of enterprise network security level protection, which includes three layers of security domain, network boundary and network environment. It has been applied in a specific case to realize the division of enterprise server domain and desktop terminal domain, the dynamic calculation of inter-domain routes, and the hot spare redundancy of each gateway and link. The fault tolerance and stability of network and business system are improved comprehensively, and good results are obtained. Some scholars have used DeMatel-ANP method and grey system theory to establish information security risk assessment model. The safety risk level is obtained by grey correlation analysis of the uncertainty relationship between control measures, so as to find out the control measures that need to be improved. This will reduce the risk within an acceptable range. However, most of the current industrial information security systems deployed by enterprises are based on traditional information security theory, and they establish static passive defense systems based on cryptography, antivirus and network boundary protection [2]. In the face of increasingly complex network environment and continuous large-scale network attacks, this static passive defense system can no longer meet the needs of users for industrial information security defense. In order to realize the dynamic active defense of industrial information security system, it is necessary to introduce new information security defense theory to enrich the traditional information security theory system. This paper introduces the concept of association rules. Association rules reflect the interdependence between one thing and other things. The application of association rules is expected to reduce the difference between the output results of network information security risk measurement analysis model and the actual risk value, that is, to improve the accuracy of the risk measurement analysis model.

II. Information Network Security Content under Artificial Intelligence Technology

In view of the above threat analysis to cloud computing network information security, combined with China's network security level protection work, the paper propose cloud computing network security strategy, the model is shown in Figure 1.

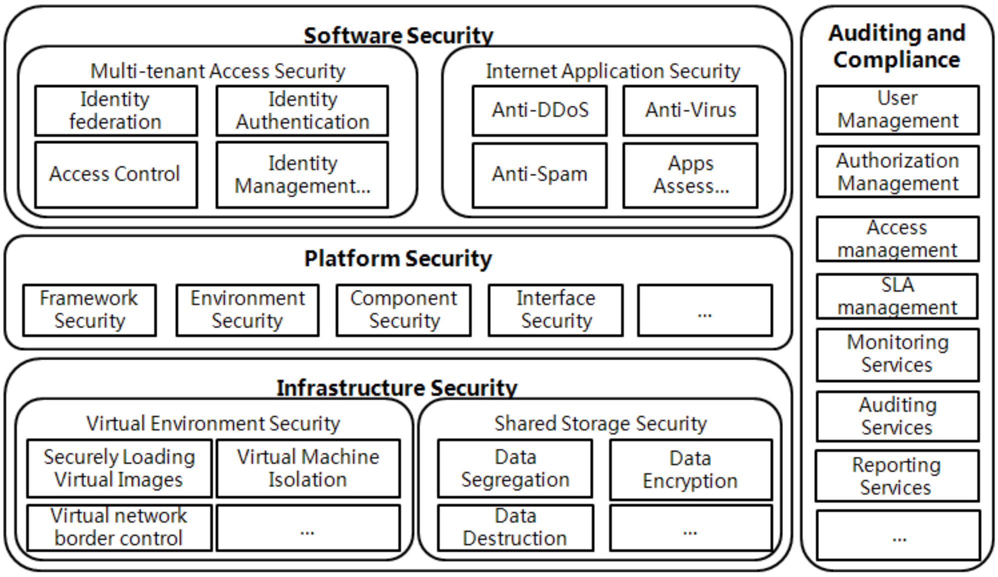

Fig. 1. Cloud Computing network information security architecture

A. Physical and Environmental Security

In terms of physical and environmental security, it provides security protection for physical location selection, physical access control, theft and damage prevention, lightning protection, fire prevention, water and moisture protection, ESD prevention, temperature and humidity control, power supply, and electromagnetic protection [3]. Due to the distribution of physical locations in the cloud computing environment, each equipment room must meet the same physical security protection requirements.

B. Network and Communication Security

In terms of network and communication security, it mainly protects the network architecture, communication transmission, border protection, access control, intrusion prevention, malicious code prevention, security audit, and centralized control at the network level. In cloud computing, virtualization technology is used to abstract physical resources into virtual networks, virtual computers, virtual storage and other resources. Therefore, the security protection of both physical resources and virtual resources should be considered.

C. Device and Computing Security

In terms of device and computing security, it protects hosts and operating systems from identity authentication, access control, security audit, intrusion detection, malicious code prevention, and resource control.

D. Application and Data Security

In terms of application and data security, it is necessary to consider application-level identity authentication, access control, security audit, software fault tolerance, resource control, interface security, as well as data integrity, data confidentiality, data backup and recovery, residual information protection and other aspects of security protection.

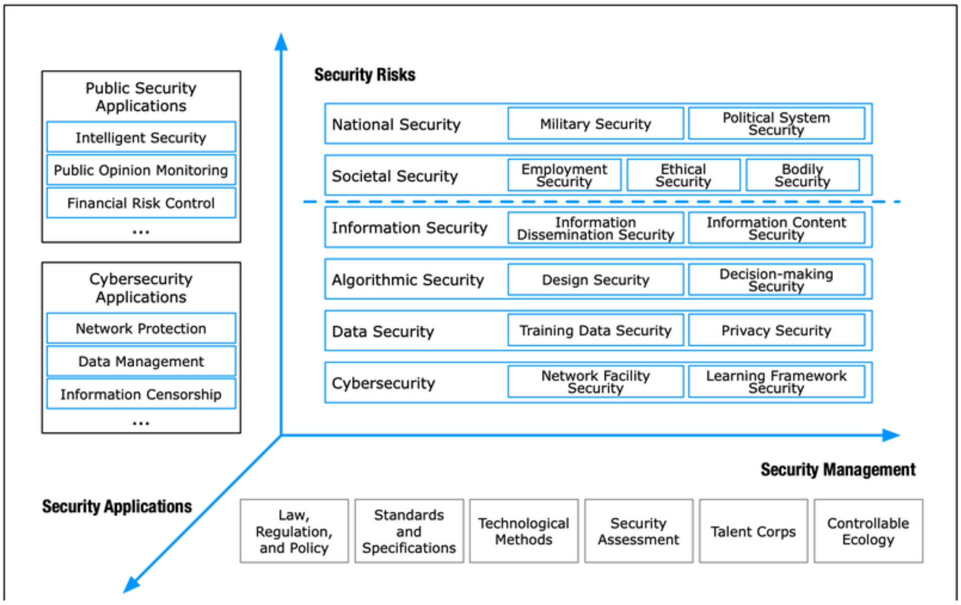

Fig. 2. Network security architecture diagram

III. NETWORK SECURITY SYSTEM FRAMEWORK

The security system framework shown in Figure 2 includes security objectives, security boundaries, security system elements, security services, security risk assessment and OSI reference model, among which security objectives are divided into business requirements objectives and security requirements objectives, and security system elements are divided into security technology elements and security management elements [4]. According to the classification method of OSI security architecture, security technology elements can be divided into 8 types: data signature mechanism, encryption mechanism, access control mechanism, data integrity mechanism, authentication exchange mechanism, anti-service filling mechanism, notarization mechanism and routing control mechanism. Security management elements are divided into information security organization, network information security management, human resource security, physical and environmental security, communication and operation management, access control, information system acquisition development and maintenance, information security event management, business continuity management, compliance, etc., according to the requirements of ISO 27000 series standards. This classification method can ensure the compatibility with the above standard system, so it is easy to extend the scope of application of the security system framework constructed in this paper.

In Figure 3, the security boundary and security system elements of the security system framework can be determined according to the security objectives, and the division of security boundary and the establishment of security system elements will provide support for the realization of security objectives. On the one hand, security services are determined by specific security system elements, and on the other hand, they are affected by the demarcated security boundaries [5]. Security risk assessment provides a means to dynamically improve and improve the framework of the security system, which is implemented by analyzing the security system elements within the security boundary to meet the security objectives. The establishment of security system elements needs to meet the requirements of OSI reference model to ensure the security of all levels.

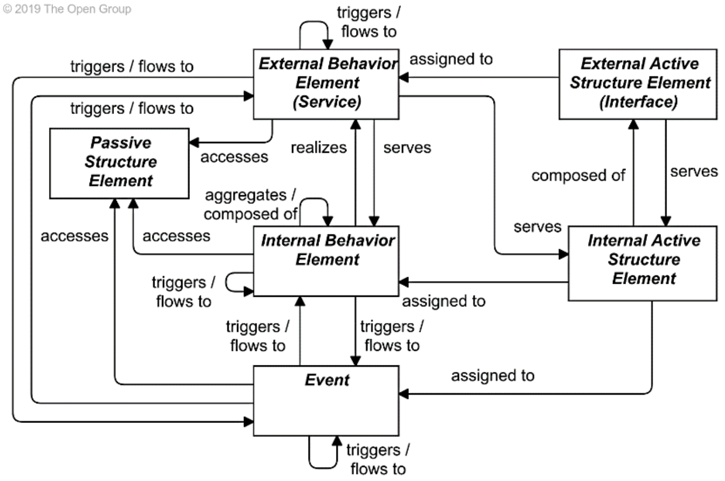

Fig. 3. Diagram of the security architecture framework elements

IV. DESIGN OF NETWORK INFORMATION SECURITY RISK MEASUREMENT ANALYSIS MODEL

A. Risk analysis

In general, the value of information security risk is related to the value, threat and vulnerability of information network security. According to the above theory, the basic framework of network information security risk measurement and analysis model is shown in Figure 4.

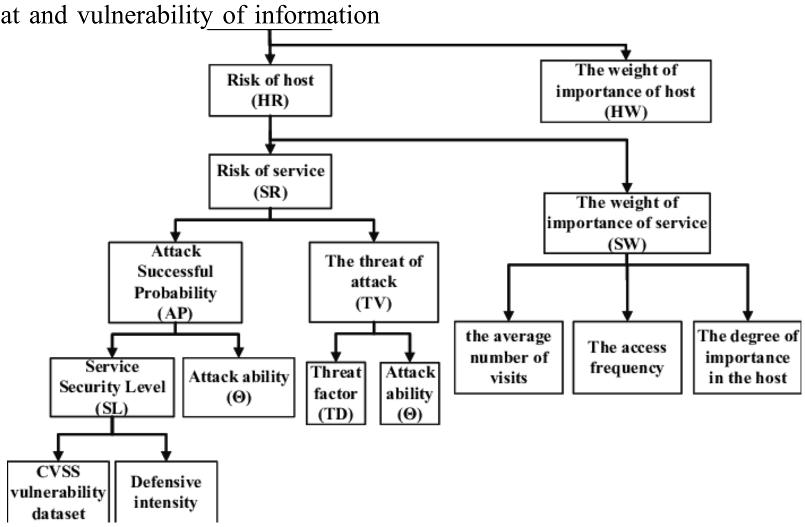
Risk of host (HR)
The weight of importance of host (HW)
Risk of service (SR)
The weight of importance of service (SW)
Attack Successful Probability (AP)
The threat of attack (TV)
the average number of visits
The access frequency
The degree of importance in the host
Service Security Level (SL)
Attack ability (Θ)
Threat factor (TD)
Attack ability (Θ)
CVSS vulnerability dataset
Defensive intensity

Fig. 4. Network information security risk measurement analysis model framework

Network information security, threat and vulnerability are three elements of risk. Property is anything of value to an enterprise, including physical assets and intangible network information security such as software, data, and the ability to provide services [6]. The loss caused by risk can be quantified by analyzing the damage degree of the network information security mentioned above. Network information security risks can be expressed as follows:

$$R \equiv \{(E_1, L_1), \cdots, (E_i, L_i), \cdots, (E_n, L_n)\} \tag{1}$$

Where: E_n and L_n are security risk events and their occurrence probabilities respectively. Loss caused by risk can be measured by network information security value and loss share [7]. The value of network information security of the j network information is defined as A_j, then the loss caused by security risk event E_i is:

$$D_i = \sum_{j=1}^{m} P_{ij} A_j \tag{2}$$

Where, P_{ij} is the share of loss caused by information security of the j network. m is the number of network information security. On this basis, the absolute loss effect caused by security risk event E_i is defined as:

$$U_i = \mu(D_i) \tag{3}$$

Where: $\mu(\cdot)$ is the degree of dissatisfaction caused by risk events. Similarly, relative loss effect can be obtained as follows:

$$F_i = \mu\left(\frac{D_i}{\sum_{j=1}^{m} A_j}\right) \tag{4}$$

Relative loss effect in the sense of probability, considering the probability of the occurrence of security risk events, the expected loss effect should be calculated, and the expression is:

$$\begin{cases} U = \sum_{i=1}^{n} \mu(D_i) L_i \\ F = \sum_{i=1}^{n} \mu\left(\frac{D_i}{\sum_{j=1}^{m} A_j}\right) L_i \end{cases} \tag{5}$$

The final calculation results U and F of Equation (5) are expected absolute loss effect and expected relative loss effect, respectively. In the actual security risk measurement process, the quantitative results of risk can be obtained according to the loss and benefit of network information.

The process of scientific security measurement generally includes the steps of proposing the measurement target, determining the measurement requirement, setting the measurement index, establishing the measurement model, setting the security measurement standard, implementing the security measurement and so on [8]. Following the basic steps of security risk measurement above, the association rules are used to mine the real-time information data of the network, analyze the association relationship between network risk events, determine the running status of the current network, and then ensure the accuracy of security risk measurement.

B. Network security information model based on association rules

First, association rules are used to detect network security events, and the basic process is shown in Figure 5.

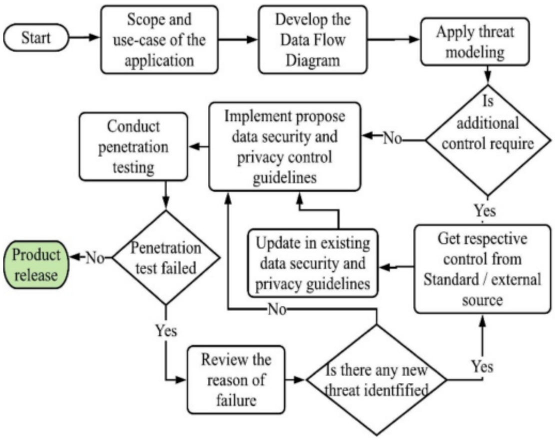
Start
Scope and use-case of the application
Develop the Data Flow Diagram
Apply threat modeling
Is additional control require
No
Yes
Implement propose data security and privacy control guidelines
Conduct penetration testing
Penetration test failed
No
Product release
Yes
Update in existing data security and privacy guidelines
Get respective control from Standard / external source
No
Review the reason of failure
Is there any new threat identfified
Yes

Fig. 5. Flow of association rules detecting network security events

The risk measurement of data islanding risk is mainly analyzed from the perspective of the impact degree of data islanding, and the process is as follows:

$$Atd_d = Atn_d V_{atn} + Ast_d V_{ast} + R_+(Asd_d) V_{asd} \tag{6}$$

Where: Atd_d is the impact degree of data islanding. Atn_d is the quantified value of the degree of data islanding. Ast_d is the quantified value of information importance in the island. Ast_d is the proportion of information in the island in the total information network information security. V_{atn}, V_{ast} and V_{asd} are respectively the severity of data islanding, the importance of information network information security and the weight value of information loss efficiency. R_+ is the loss function.

V. Application of Network Information Security Risk Model

The application of network information security risk association rule model is divided into four steps: network information security assessment, threat assessment, vulnerability assessment, and risk calculation [9]. The evaluation functions accomplished by these four sections are described in detail below.

A. Network information security assessment

Network information security assessment is mainly based on the results of network information security survey to determine the type of network information security in the information system under test, that is, to determine each element Na_i in set A. According to the relevant attributes that determine the value of network information security obtained from the security survey results, the value of each network information security is calculated, that is, $\{a_i \mid value\}$ is determined.

B. Threat Assessment

Threat assessment is mainly based on the results of IDS detection and questionnaire survey to determine the threat facing the information system under test, that is, to determine each element t_i in the set T. Calculate the threat frequency, that is, determine $\{t_i \mid fren\}$. Analyze threats to network information security, that is, determine $AT(a_i, tj)$.

C. Vulnerability Assessment

Vulnerability assessment is mainly based on vulnerability scanning results, BIOS security detection results, WLAN detection results, and device effectiveness detection results to determine the vulnerability of the information system under test, that is, to determine each element v_i in the set$V$. Determine the severity of each vulnerability and the degree to which it can be exploited, that is, determine $\{v_i \mid serious, diff\}$. To analyze the vulnerability that a threat can exploit, that is, to determine $TV(t_i, v_i)$.

D. Risk Calculation

Risk calculation mainly analyzes the interaction between vulnerabilities, that is, to determine $VV(v_m, v_n)$. Analyze the security dependence relationship between network information security, that is, determine $AA(a_m, a_n)$. According to the calculation method of network information security risk determined by the process of the model, the risk value of network information security is calculated.

VI. Experimental detection

The network data of a big data platform operator in a province is selected as the test sample of this experiment, and a set of data is saved every 10 minutes in a one-month collection period, so as to evaluate the information security of the operation network [10]. The selected data resources were divided into samples and processed into three groups of data packets according to the principle of equal allocation. Before the test, 10 experts were invited to select and score network security indicators, and network security evaluation Settings under different indicator levels were carried out. In order to ensure the accuracy of the experiment, a group of traditional models is introduced for comparison. After the test platform obtains the grade results, the two groups of models are connected to the test platform in turn to evaluate the security level of network information samples respectively. The specific grade evaluation results are shown in Table I.

TABLE I. Evaluation results of network information security level of operators

The sample number	Sample 1	Sample 2	Sample 3
security	0.2387	0.1073	0.2185
The safer	0.3864	0.3585	0.0298
General safety level	0.0461	0.0467	0.1777
dangerous	0.2552	0.2732	0.1707
Very dangerous	0.0736	0.2143	0.4033
The actual results	The safer	The safer	Very dangerous
The new model	The safer	general	general
The original model	security	The safer	Very dangerous

According to the original model shown in table I in the level of information security evaluation, its dangerous nature generally lower than the actual results in a level. The application of the model in this paper can match the grade results of the actual data, and the equivalence of the internal data is related under the comprehensive consideration of the subjective factors of each index, so as to obtain more accurate evaluation results. The comprehensive experimental results show that the model designed in this paper can re-describe the level characteristics through the selected indicator types and comprehensively consider the important properties of different level indicators, so as to evaluate the security level of network information with practical application effect.

VII. Conclusion

In order to measure the network information security risk comprehensively and accurately, the reference of association rules effectively improves the measurement accuracy of network information security risk. However, in different network environments, due to the different attack methods on network information, the security risk measurement results will be quite different.

References

[1] Zuo Xiaojun, Chen Ze, Dong Limian, et al. Research on network security evaluation method based on information security framework "Golden Triangle Model". Bond Bonding, vol. 41, pp.54-59,February 2020.

[2] Yang Zhiyuan, Zhang Shipeng, Sun Hao, Guan Xiaohong. Risk assessment of substation network threat based on Cyber-net and learning algorithm. Automation of Electric Power Systems, vol. 44, pp.:91-94,December 2020.

[3] Zhang Kai, Liu Jingju. Network intrusion path analysis method based on vulnerability dynamic exploitability. Information Network Security, vol. 11, pp.62-72,April 2021.

[4] Zhang Xin, Dong Liming. Quantitative simulation of network node information security under the game model of attack and defense. Computer Simulation, vol. 037, pp.18-21,98,June 2020.

[5] Zhang Xiangyun, Zhou Zi, Jiang Youxin, et al. Measurement of defocus particle size and position based on convolutional neural network. Acta Optica Sinica, vol. 42, pp.191-200,December 2022.

[6] Fang Shaofeng, Zhou Renjun, Peng Yuanyuan, et al. A balanced market trading model for electricity retailers with risk aversion. Journal of Electric Power Systems and Automation, vol. 32, pp.69-74,February 2020.

[7] Qin Zhongyuan, Hu Ning, Fang Lanting. Network anomaly detection method based on immunobionic mechanism and graph neural network. Information Network Security, vol. 11, pp.10-16,August 2021..

[8] Li Weigang, Li Qiang. Security analysis of environment monitoring network based on zero trust network model. Sichuan Environment, vol. 40, pp.49-51,March 2021.

[9] Meng Jin. Risk Assessment model of information systems based on factor analysis and neural networks. Modern Electronic Technology, vol.43, pp.58-62,December 2020.

[10] Peng Zixiang, Jiao Ke, Wang Junjie, et al. Building structure safety assessment model based on Bayesian network. Building Technology, vol. 52, pp.49-59,October 2021.