Research on Security Evaluation Index System for Video Surveillance Network

Jinping Cao, Tao Chen*, Jiao Wan, Simin He, EIken Guriz hot

State Grid Xinjiang Electric Power Co., LTD. Information and Communication Company, Urumqi, Xinjiang 830000

Corresponding E-mail: 2438396213@qq.com

Abstract. With the deepening of information technology, risk assessment has become increasingly important in the field of information security. In view of the current situation that China lacks quantitative evaluation technology in terms of network terminal security status evaluation, this paper proposes a set of evaluation index system for network terminal security status, which covers network terminal assets, threats, vulnerabilities and other aspects. Based on the safety evaluation method, an evaluation model is established by using multi-level fuzzy comprehensive evaluation method, focusing on how to reduce human subjective factors and how to provide objective safety condition evaluation factors.

Keywords: network terminal; data System function module; Quantitative model

1 Introduction

With the popularization of computer network and the advancement of information technology, the problems of network and information security are becoming increasingly prominent, and China's dependence on network information systems is deepening. Foreign countries have decades of experience in studying network and information system security risk assessment, and IT developed countries have become very mature in information system risk assessment standards, technology, architecture, organization, etc. At home, more attention is paid to the security protection of the internal data of the network system [1]. The network terminal is the source of important files and data. Many security incidents often originate from the network terminal, and the leakage incidents and security threats from the terminal also appear frequently. The network terminal security management has become the weak link of the information security management system [2].

The objective and systematic evaluation of network terminal security is the basis for ensuring information security [3]. Through the analysis of potential security risks and future risks, and the assessment of the potential security threats and impact of these

H. Wu et al. (Eds.): CSIEDE 2022, ACSR 103, pp. 839–847, 2022.
https://doi.org/10.2991/978-94-6463-108-1_93

risks, it will help security personnel to specifically resist threats, comprehensively improve the security protection capability of network information systems, and maximize the protection of information assets.

At present, there is no uniform standard for evaluating the security status of network terminals in China, and the key points of network terminal security are still unclear [4]. This paper will make a beneficial discussion on the evaluation index system of network terminal security, try to quantify the network terminal evaluation system index, control the network terminal security risk at a reliable level, so as to maximize the terminal security level.

2 Network terminal security assessment method

The choice of safety assessment method will directly affect all aspects of the assessment process and may affect the final assessment results. The existing risk assessment methods can be roughly divided into quantitative risk assessment, qualitative risk assessment and comprehensive risk assessment [5-6].

2.1 Quantitative risk assessment

Quantitative assessment assigns numerical values to each element of risk and potential loss level. After all elements of equivalence risk are assigned, a mathematical model for comprehensive assessment is established to complete the quantitative calculation of risk [7]. The quantitative assessment data is relatively intuitive and the analysis method is relatively objective, but some risks may be misinterpreted after being quantified. The commonly used quantitative evaluation methods include fuzzy comprehensive evaluation, BP neural network, grey system, etc.

2.2 Qualitative Risk Assessment

Qualitative assessment is mainly based on the knowledge and experience of researchers, or non quantitative assessment of industry standards, historical lessons, policy trends, etc [8].

It is a fuzzy analysis method to evaluate the system risk by data. The operation of qualitative analysis is relatively simple, and the conclusion is relatively comprehensive, but it is highly subjective and easily affected by the intuition and experience of the appraisers [9]. Common qualitative evaluation methods include expert evaluation, historical comparison, fault tree analysis, cause and effect analysis, logic analysis, etc.

2.3 Comprehensive risk assessment

Comprehensive risk analysis is an analysis method that combines qualitative and quantitative assessment. Qualitative analysis is used when accurate data is not easy to obtain. Quantitative methods are adopted on the basis of qualitative analysis to reduce subjectivity [10]. The most commonly used comprehensive risk analysis and assessment

method is the Analytic Hierarchy Process (AHP for short), which is a decision-making method that combines qualitative and quantitative analysis and is the modeling of human brain decision-making thinking.

3 Research on the index system of network terminal security evaluation

3.1 Principles of establishing evaluation system

China's Code for Information Security Risk Assessment defines the basic elements of risk assessment as assets, threats, vulnerabilities, risks and security measures [11]. The security assessment of network terminals mainly involves three elements: assets, threats and vulnerabilities. When establishing the network terminal security evaluation index system, the following four principles need to be considered: (1) The international and domestic information security evaluation specifications must be followed. The evaluation index system should also meet the business requirements and application characteristics, and try to meet the user and application environment requirements for network terminal security. (2) The set indicators should cover all risk factors of terminal security, covering all levels of technology and management, as well as subjective and objective factors. (3) The meaning and objectives of indicators should be clear, the overall indicator system should be clear, and the data collection channels should be realistic and operational to ensure the feasibility of quantitative analysis. (4) The evaluation index shall be independent of the specific content of network terminal security and shall not overlap with other indexes [12].

3.2 Design of network terminal security assessment framework

This paper follows the principle of establishing an evaluation system, and establishes a hierarchical evaluation index system for the security status of network terminals [13]. The index system is proposed to be divided into four layers, as shown in Table 1.

Table 1. Security Assessment Index System of Layer 4 Network Terminal

first floor	The second floor	The third floor	The fourth floor
Information assets	Hardware	equipment	Server, storage device
		Transmission line	Optical fiber, twisted pair
	Software	systems software	Operating system, development system
		Application software	Database software and business system
	data	Business data	Database data, log documents and system data. user 's manual
	file	Paper, electronic	
threaten	Environmental threats	Physical threats	Natural disasters, electromagnetic interference, dust, static electricity
		Technical fault	Hardware failure, system software failure, application software failure, and storage medium effectiveness

	Man made threats	Management defects	System, authorization and resource monitoring
		Human error	Operation error and maintenance error
		Malicious act	Viruses, spyware, eavesdropping software, attacks
Vulnerability	technology	physical environment	Machine room, electromagnetic and communication lines
		systems software	Patch, account policy, event audit, access control
		application system	Password protection, audit mechanism, access control
	Administration	technical management	Communication, operation, business continuity, development and maintenance
		Organizational management	Safety training, personnel safety, asset control

The implementation of the network terminal security evaluation index system is divided into three steps: first, establish a hierarchical evaluation index system; second, determine the evaluation index; third, assign weight to each evaluation index. There are many sources of indicator data, including questionnaires, personnel interviews, field surveys, auxiliary tools and document reviews [14-15]. Then, referring to the terminal security evaluation index system, the security status data is obtained by means of document review, questionnaire, etc., and then the assets, threats and vulnerabilities are identified and analyzed by using vulnerability scanning tools, intrusion detection tools and other technologies.

3.3 Establishment of quantitative evaluation model for network terminal security

In this paper, the multi-level fuzzy comprehensive evaluation method is used to establish the evaluation model. The fuzzy comprehensive evaluation method first quantifies the fuzzy indexes of the evaluated things by constructing a hierarchical fuzzy subset, and then comprehensively evaluates each index by using the fuzzy transformation principle.

3.3.1 Establishment of evaluation object factor set.

Let the hierarchical evaluation index system be U, divide the factor set U into n groups, and record it as U={U1, U2,.., Un}, where $Ui \rightarrow Uj \neq \varphi$, $i \neq j(i, j=1,2, ..n)$。 Let the ith subset be Ui={Ui1, Ui2,.,. Uin}, where i represents the number of single factors in the ith group.

3.3.2 Set evaluation set and assign weight coefficient.

Let V={VI, V2,. Vn} be the evaluation set, which is composed of descriptions of different levels. M generally takes an odd number, and the evaluation set is applicable to the evaluation of any level and any factor.

3.3.3 Single level fuzzy comprehensive evaluation.

Set up an evaluation expert group, and the experts will evaluate each evaluation index, and determine which level of the evaluation index belongs to the grade evaluation set [16]. Count the number of experts whose evaluation index is evaluated to the corresponding level, and the percentage of the number of experts at the corresponding level in the total number of experts, that is, get the membership of the evaluation index at this level, and then get the fuzzy relationship matrix Rj. According to the single factor fuzzy relation matrix Rj, the comprehensive evaluation result of sub factor Ui is obtained by compound operation: Bi=AiOri=(bilbi2.. Bim), i=1,2,., n.

3.3.4 Calculation of final comprehensive evaluation results.

A high-level fuzzy comprehensive evaluation is conducted on the single factor evaluation result Bi, and the lower level comprehensive evaluation result Bi forms a high-level single factor fuzzy relation matrix R. After that, the multi-level factor set is comprehensively evaluated, and the final evaluation result of evaluation factor U is: B=AOR=(bl b2... bm). This round of calculation can be repeated according to the hierarchy of evaluation indicators until the most satisfactory comprehensive evaluation results are obtained.

3.3.5 Analysis of comprehensive evaluation results.

The final result of fuzzy comprehensive evaluation is not a single value, but a fuzzy subset, which can accurately reflect the fuzzy status of the object itself. It can be seen from the specific process of quantitative evaluation of multi-level fuzzy comprehensive evaluation method that the lowest level indicators need to be judged by human membership, and the membership of all upper level indicators are calculated according to the lower level [17]. Network terminal security assessment is mainly to identify and analyze asset value, threat and vulnerability. According to the different degree of confidentiality, integrity and availability requirements of asset (A), the three attributes are divided into five levels, and different values are assigned to different levels; According to the frequency of threat (T), the threat is assigned and divided into five levels: vulnerability (V) identification. For each asset, it is also divided into five levels. The network terminal security evaluation value is divided into five grades, namely good, good, medium, poor, and very poor. The higher the grade, the greater the impact on the terminal and network. Table 2 shows the classification table and corresponding safety conditions.

Table 2. Classification of network terminal security status

Grade	Safety assessment value	identification	describe
5	51 to 100	range	It will cause significant economic and social impacts and serious impacts on the normal operation of terminals and networks

4	31 to 50	difference	It will cause great economic and social impact and damage the normal operation of the terminal
3	21 to 30	in	Will cause certain economic and social impact
2	11 to 20	good	The impact is low, which can be solved by one set of safety measures
1	0 to 10	good	The probability of occurrence is extremely low, and simple measures can be taken to remedy it

According to the final assignment of the three basic elements and the network terminal security assessment model, the network terminal security assessment value is analyzed and calculated. The calculation process is divided into four steps: (1) The network terminal security assessment value is determined by A, T, V and the probability of risk occurrence. (2) Calculate the probability P of terminal security event caused by threat using vulnerability, which is recorded as P=F1 (T, V), P=T+V. (3) The degree of loss caused to assets is related to threat value, vulnerability and asset value, and is recorded as L=F2 (P, A), L=PXA.

(4) Considering the probability R of the loss and risk caused by the threat to assets, the terminal security assessment values S, S=F (L, R), S=LXR are obtained.

3.4 Design and implementation of network terminal security assessment system

3.4.1 System requirement analysis.

Security assessment analysis focuses on assessing the possible threats and impacts of risks, submitting detailed and reliable analysis reports to the system administrator, allowing the administrator to master policy vulnerabilities and security conditions, and proposing targeted protection countermeasures against threats. The network terminal security assessment system needs to meet seven requirements: (1) Identify network terminal assets. (2) Scan network terminals for vulnerabilities and provide accurate and objective quantitative evaluation data. (3) Dynamically monitor the terminal resources of network operation, and analyze the possible threats and possibilities. (4) Carry out terminal security assessment and obtain comprehensive quantitative assessment conclusions.

(5) Output the data and quantitative evaluation results in the form of report. (6) Give security solutions or reinforcement suggestions to improve the security of network terminals. (7) Manage users using the evaluation system and assign different permissions [18].

3.4.2 Design of network terminal security assessment system.

In order to reduce the system resource occupation, the evaluation system is designed on a server in the intranet. The software running environment is Windows 2002/2003 Server, and the server is required to access the core switch. The system architecture is shown in Figure 2.

3.4.3 Realization of system function modules.

The network terminal security evaluation system is mainly divided into five modules: asset identification, vulnerability management, threat management, terminal security evaluation, and evaluation response [19].

(1) Asset identification module. The asset identification module mainly includes asset information management sub module and asset identification and assignment sub module. The former mainly manages the basic information of the local terminal and the remote terminal. The latter reads the terminal IP address, user name, password and other information from the asset database, establishes the host object, and transfers the host object to the callback function.

(2) Vulnerability management module. This module includes two sub modules: vulnerability scanning and vulnerability assignment. Scan the assessed local terminal and remote terminal, and determine the vulnerability of application programs and operating systems, as well as assign the vulnerability weight of terminal assets.

(3) Threat management module. This module includes two sub modules: resource monitoring and threat assignment. The resource monitoring module dynamically monitors local and remote terminal resources to obtain resource status information.

(4) Terminal security assessment module. It is divided into two sub modules: fast and complete evaluation. The quick evaluation evaluates the terminal security according to the quantitative evaluation model; the complete evaluation evaluates the terminal security according to the set of index factors in the established security evaluation index system using the multi-level fuzzy comprehensive evaluation method.

(5) Response module. According to the evaluation results, match the rules defined in the response library and give solutions or reinforcement suggestions.

In the aspect of system interface design, the system is divided into three layers: user interface layer, logic processing layer and data intermediate layer. The interface layer is used to accept user input and display evaluation reports; The logic processing layer realizes the functions of the above five modules; The data middle layer shields database details and connects the system with multiple databases.

4 Conclusion

This paper proposes a set of network terminal security evaluation index system, establishes a quantitative evaluation model for network terminals, and quantifies the evaluation items as specific as possible to reduce the subjective impact of human beings. In the next step, we can further explore and improve the terminal security quantitative evaluation model according to the security evaluation system, improve the system design and expand the evaluation function.

References

1. Ma L , Lv X Y , Fu S . Education Information Network Terminal Big Data Analysis Response and Monitoring System[C]// 2021.

2. Xin Y , Wu Y , Li Y , et al. Data processing method and system to associate data of a terminal distributed on different network elements:, US11115802B2[P]. 2021.
3. Liang M . Optimization of Quantitative Financial Data Analysis System Based on Deep Learning[J]. Complexity, 2021, 2021(1):1-11.
4. Song J , Zhang Y , Cheng J , et al. Non-invasive quantitative diagnosis of liver fibrosis with an artificial neural network[J]. Neural computing & applications, 2022(34-9).
5. Vaziri M . Antitrust Law and Business Dynamism[J]. Cambridge Working Papers in Economics, 2022.
6. Yang Y , Komatsu M , Oyama K , et al. Real-Time Cattle Interaction Recognition via Triple-stream Network[J]. 2022.
7. Xu X , Chen Y , Du Y . DATA TRANSMISSION METHOD, TERMINAL, AND NETWORK DEVICE:, US20210212093A1[P]. 2021.
8. Chen X , Liang Y , Wang G , et al. A control parameter analysis method based on a transfer function matrix of hybrid multi-terminal HVDC system with flexible adaptability for different operation modes[J]. International Journal of Electrical Power & Energy Systems, 2020, 116:105584-.
9. Du Y , Si S , Cai Z , et al. Bayesian Importance Measures for Network Edges Under Saturated Lagrangian Poisson Failures[J]. IEEE Transactions on Reliability, 2021(70-1).
10. Seong HwanKim · HayomKim · Jung BinKim. differences in functiona1 network between foca1 onset nonconvu1sive status epi1epticus and toxic metabo1ic encepha1opathy app1ication to machine 1eaming mode1s for differentia1 diagnosis[J]. 2022.
11. Peng J , Tang Q L . Application of NARX Dynamic Neural Network in Quantitative Investment Forecasting System[J]. 2020.
12. Gyamfi J , Cooper C , Barber A , et al. Needs assessment and planning for a clinic-community-based implementation program for hypertension control among blacks in New York City: a protocol paper[J]. Implementation Science Communications, 2022, 3(1).
13. Abane J A , Adamtey R , Ayim V O . Does organizational culture influence employee productivity at the local level? A test of Denison's culture model in Ghana's local government sector[J]. Future Business Journal, 2022.
14. Sueki K , Nishizawa S , Yamaura T , et al. Precision and convergence speed of the ensemble Kalman filter-based parameter estimation: setting parameter uncertainty for reliable and efficient estimation[J]. Progress in Earth and Planetary Science, 2022, 9(1):1-18.
15. Peng Y , Zhong G C , Zhou X , et al. Frailty and risks of all-cause and cause-specific death in community-dwelling adults: a systematic review and meta-analysis[J]. BMC Geriatrics, 2022, 22(1).
16. Korolev V , Nevolin I , Protsenko P . A universal similarity based approach for predictive uncertainty quantification in materials science[J]. Scientific Reports, 2022, 12(1).
17. ジャーン, プオン. Terminal device, network device, data transmitting method, and wireless communication system:, JP6639680B2[P]. 2020.
18. Zhang P. TERMINAL DEVICE, NETWORK DEVICE, DATA TRANSMISSION METHOD, AND WIRELESS COMMUNICATION SYSTEM:, EP3389327B1[P]. 2020.
19. Song Y, Chen X . DATA ACQUISITION METHOD, SERVICE PROVIDER TERMINAL, SERVICE USER TERMINAL, AND NETWORK FUNCTION ENTITY:, EP3751820A1[P]. 2020.