Research on Comprehensive Evaluation System of Network Security Management Based on Multi Dimensional Extension Fuzzy Technology

Aiyue Xia[1,a]

[1]Department of Force Management, The Armed Police Academy, Langfang, HeBei Province, China

[a]52859624@qq.com

Keywords: Multi dimensional fuzzy technology; Network security management; Comprehensive evaluation system.

Abstract. Objective: to improve the network security management. Method: using multi dimension extension fuzzy technology. Process: build a multi dimensional model to comprehensive evaluation of network security management level. From network security management systems, human input, technology effect three aspects, comprehensive evaluation of network security management level. The weights of the various indicators and the evaluation values of each dimension are obtained by the analysis of Extension Association. Results and analysis: The application shows that the model can be integrated with the factors of management, technology, manpower, etc. has a significant effect on the improvement of network security management. Conclusion: in this paper, the use of multi dimensional extension based fuzzy technology is helpful to improve the network security management.

Introduction

Network and information security is to ensure the information security of the network space, involving information confidentiality, integrity, authenticity, availability, non repudiation, can be controlled, and can be reviewed, etc. Network protection technology must ensure that the legitimate users can access to the network system and get resources from the network, refuse the unauthorized access to unauthorized users of the network, or steal information, damage system.

Network security management technology involves a lot of aspects. In network security management framework, various network security technologies complement each other, detection and control the network, these techniques form a security policy centralized management, security check mechanism for distributed security architecture [1]. Network security management is a comprehensive, unified management concept, it is the network system security technology based on a variety of network security analysis technology and management technology. Therefore, the network security management is the key and difficult point of information security management, and is the important basis of improving the information security management system (ISMS).

Unsafe Factors in Network Management

With the high degree of the network, the behavior of the specific attack is divided into two types: distributed and combined. The attack graph is a typical combination attack method. The attack graph describes all the paths that an attacker reaches from the start point to the target, which provides a visual method for representing the process of attack. In the network security analysis, the attack graph can be used for intrusion detection, defense, forensic analysis [2].

Attack Scenario. The attack scenario describes the causal relationship between aggressive behaviors. An attack is not an isolated, but a different phase of a sequence of attacks. That is to say, in front of the attack behavior may be the premise or prepare for the later attack, the attack behavior is the direct or the result of the attack. The construction of the attack scene is realized by the correlation analysis technology, which mainly has two kinds of technology： data mining and rule based.

Attack Tree. The attack tree model provides a formal method for describing the system vulnerabilities, which is an extension of the fault tree model and a kind of attack based on change [3].

Using formal methods, systematic description of system security, make a model with the security system. The attack tree is a recursive or incremental way to express the change of the attack, it can reflect the steps of the attackers, especially suitable for describing the multi stage network attacks.

Attack Network. Attack network is a kind of special type of attack graph, which is composed of position, change, arc and token. Its location is relative to the nodes in the attack graph. The attack behavior is described by the change of the token in the position [4]. The description of attack method in the attack network model mainly solves the problem of how to successfully implement the method in which a certain attack method can be successfully implemented. The attack net model describes the logic and sequence of the various attack methods that can be implemented. The distribution of the token in the model is characterized by the process of the dynamic operation of the attack process.

Attack Graph. The method of attack graph, the main difficulty lies in the attack graph structure, the study of early in the attack graph is by security experts artificial analysis. With the increase of network scale and the expansion of security vulnerabilities, manual analysis method becomes very difficultly, the automatic generation of attack graph has become a research direction. At present, the automatic generation method of attack graph is mainly based on the method of model checking and the forward search method based on the attacker's angle.

Multi Dimension Extension Fuzzy Technology

This paper is based on the standard family of COBIT, NIST, SP800, ISO/IEC27000, the paper puts forward multi dimension extension Fuzzy Technology. Comprehensive evaluation of network security management level from the network security management system measures, human input, technical effect 3 dimensions. Weight of each index and evaluation value of each dimension were further analyzed by means of extension association analysis [5].

Extension Fuzzy Comprehensive Evaluation Algorithm

Assessment Level of Membership

Evaluation index intends to select six aspects: policy and strategy (including network security risk assessment, making network security management strategy), environmental safety, including room arson, waterproof, lightning), hardware security, including power supply, equipment monitoring, security software (including operating systems, databases, application software security settings), communication security, such as firewall, intrusion detection, etc.) and data security, including data backup, disaster recovery, etc.)

At present, most of the evaluation index of the evaluation depends on the experience of the experts, so it can be used to evaluate the degree of membership of the fuzzy mathematics, see Table 1.

Table 1. Assessment Levels and Their Membership Degrees

Class	Subjective evaluation	Membership degree
1	Low	1.0-4.0
2	General	4.0-6.0
3	Higher	6.0-8.0
4	Very high	8.0-9.0

Related concepts of extension theory

Extension theory is a mathematical tool to solve the problem of uncertainty, which is founded by Cai Wen. Evaluation, recognition and information processing based on the matter element and the correlation degree. The classical domain, the section area, the pending evaluation element are the basic concepts of extension evaluation[6].

Classical domain is:

$$R_j = \begin{pmatrix} N_j & c_1 & \langle a_{1j}, b_{1j} \rangle \\ & c_2 & \langle a_{2j}, b_{2j} \rangle \\ & \cdots & \cdots \\ & c_n & \langle a_{nj}, b_{nj} \rangle \end{pmatrix} \quad (1)$$

Extension association analysis

Extension association analysis is the key step of extension evaluation. Need to determine the final assessment level by index on the degree of association and index weight

(1) Index on the degree of relevance

$$K_j(v_i) = \left\{ \frac{-p(v_i, V_{ij})}{|V_{ij}|} \quad \frac{p(v_i, V_{ij})}{p(v_i, V_{ip}) - p(v_i, V_{ij})} \right\} \quad (2)$$

(2) the determination of the weight of the index

$$r_{ij}(v_i, V_{ij}) = \left\{ \frac{2(v_i - a_{ij})}{b_{ij} - a_{ij}} \cdots\cdots v_i \le \frac{b_{ij} + a_{ij}}{2} \quad \frac{2(b_{ij} - v_i)}{b_{ij} - a_{ij}} \cdots\cdots v_i \ge \frac{b_{ij} + a_{ij}}{2} \right\} \quad (3)$$

Based on the simple correlation function fixed weight can have an intuitive interpretation: numerical indicator into one level and is located at the center of interval correspondence, the weight of the index can be larger, indicating that the expert judgment is clear; if the values in the interval of the edge that expert judgments are more obscure, the weight of the index is smaller [7].

The correlation degree of the level of J in the level of P:

$$K_j(P) = \sum_{i=1}^{n} r_i \, K_j(v_i) \quad (4)$$

Comprehensive Evaluation System of Network Security Management Based on Multi Dimensional Extension Fuzzy Technology

The application of fuzzy comprehensive evaluation of multiple dimensions can be extended by an example. By the expert to the information system of an organization to carry on the evaluation, the score results see Table 2.

Table 2. Fuzzy Evaluation Results of Experts

Index	System measures	Human input	Technical effect
Policy strategy	3.8	3.0	3.0
Environmental security	8.5	7.0	8.2
Hardware security	5.5	6.5	7.5
Software security	5.8	7.0	7.5
Communication security	6.5	7.0	7.8
Data security	5.5	5.0	5.7

For the dimension of the system measure, the correlation matrix of each evaluation index is obtained by the formula (1):

$$\begin{bmatrix} 0.067 & -0.067 & -0.440 & -0.600 \\ -0.900 & -0.833 & -0.500 & 0.500 \\ -0.300 & 0.250 & -0.125 & -0.417 \\ -0.360 & 0.100 & -0.589 & -0.407 \end{bmatrix}$$

The simple correlation function matrix of the index weight is obtained by the formula (2):

$$\begin{bmatrix} 0.133 & -0.200 & -2.200 & -8.400 \\ -3.000 & -2.500 & -0.500 & 1.000 \\ -1.000 & 0.500 & -0.500 & -0.500 \\ -1.200 & 0.200 & -0.200 & -4.400 \end{bmatrix}$$

The weight vector of the index is obtained by the formula (3) - (5):

$$\begin{bmatrix} 0.128 & 0.226 & 0.170 & 0.136 & 0.170 & 0.170 \end{bmatrix}$$

By the formula (6), the degree of relevance of the evaluation grade is obtained.

$$\begin{bmatrix} -0.431 & -0.128 & -0.178 & -0.224 \end{bmatrix}$$

The weight vector of the index of the dimension is defined by the formula (7) - (8):

$$\begin{bmatrix} 0.195 & 0.163 & 0.175 & 0.140 & 0.152 \end{bmatrix}$$

The correlation degree vector of the evaluation grade of the evaluation object is:

$$\begin{bmatrix} -0.476 & -0.421 & 0.061 & -0.276 \end{bmatrix}$$

The evaluation level of the dimension is high, the comprehensive evaluation result is 3.2, the level of network security management of the organization is located in the point of B, and there is a lot of room for improvement.

Extension fuzzy comprehensive evaluation made matter-element tend to another level, this is the fuzzy evaluation and grey relational evaluation cant’ do the (in this case, the use of the two methods of evaluation results will simply think the level of each dimension of grade 2 or 3). Can be seen that the extension of fuzzy comprehensive evaluation can get more information, the effect is better [8].

Application examples show that the multi-dimensional extension fuzzy comprehensive evaluation, from the management, human resources, technology, etc. facing the quantitative evaluation of the level of network security management organization, is conducive to tissue measurement network security management level and make continuous improvement, so as to establish and improve the information security management system. The organization should implement the network security management system measure, ensure the effective human input, to receive the ideal technical effect. In the evaluation of the expert's score, we should lead the expert to the technology effect and pay attention to the effectiveness of the human investment [9]. For example, the minimization of the operating system installed, open network service is minimized, multi verification system of measures to reduce network security risk is often underestimated.

Based on the multi dimension can be extension fuzzy technology of network security management comprehensive application examples: "and or" logical rules, and utilization of meta divergence inference rules, can obtain the required range or meet certain conditions of the network interface or host set [10].

Establish a network security technology involving various network security model and its model base element representation, which makes all kinds of network security knowledge with the unified form of expression [11], for the application of extension method to solve various problems in the network security and the basis of all kinds of network security technology foundation. The extension method is applied to the field of network security, can provide a strong theoretical support for solving all kinds of problems in the field of network security, there is conducive to all kinds of network security technology of standardization, unified development, the ultimate realization of the various technical collaboration and network security of overall control and management.

CONCLUSION

In this paper, a comprehensive evaluation model of multi dimension extension fuzzy technology in network security management is put forward. The application shows that the model is feasible and effective [12]. Through simple correlation function of extension theory to determine the index weight, through extensive correlation analysis of various dimensions of evaluation value, reflecting the extension evaluation based on data mining the useful information ability, to ensure the objectivity and accuracy of evaluation. Obtained by simple correlation function of index weight with different metadata to be assessed and change, will not be conducive to network safety management level in different tissues were compared, that is no guarantee that the evaluation can be compared, this through further research to solve. In general, the multi dimension extension fuzzy comprehensive evaluation method is an effective method to evaluate the network security management level [13].

In short, the dimensions of extension of fuzzy technology in network security management can on some performance of the traditional network security management related technology improved is a supplement to the traditional technology, and extension method to solve all kinds of problems in the field of network security provides a strong theory support, help to manage all kinds of network security technology standardization, unified development, finally realize all kinds of security technology coordination and overall control and management of network security, and network security management technology development goal is consistent [14].

Further the model is applied to the actual environment, in-depth understanding of the performance evaluation model of the influence degree of various factors, such as determination of the evaluation factors selection, classical field, correlation function parameters and decision rule threshold selection, and ultimately be able to get on these factors is more objective and standard of the determination and selection of the scheme [15].

Acknowledgement

If you follow the “checklist” your paper will conform to the requirements of the publisher and facilitate a problem-free publication process.

References

[1] ISO. ISO/IEC27004-2006 Information Security Management Measurement. 2006.

[2] Wolfgang B. Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001[C]//Proc. of the 2nd Int’l Conf. on Emerging Security Inf., Systems and Technologies. Cap Esterel, France: [s.n.], 2008: 224-231.

[3] Q Kumar, Classification and detection of computer intrusions [Ph.D. Thesis], Purdue University, 1995.

[4] L. Liand Gy Ungho Lee, DDoS Attack Detection and Wavelets, Telecommunication Systems, 2005, 28(3): 435-451.

[5] W. W. Cohen, Fast effective rule induction, Proceedings of the 12th International Conference on Machine Learning, CA, 1995: 115-123.

[6] S. A. Hofineyr, S. A. Somayaji, Intrusion detection using sequences of system calls, Journal of Computer Security, 1998, (6): 151-180.

[7] X. Liand N. Ye, Decision tree classifiers for computer intrusion detection, Real-time system security [M], Nova Science Publishers, 2003.

[8] D. Y. Yeung and Y. Ding, Host-based intrusion detection using dynamic and static behavioral models, Pattern Recognition, 2003, (36): 229-243.

[9] N. Ye and Y.Z.C.M. Borror, Robustness of the Markov-chain model for cyber-attack detection, IEEE Transactions on Reliability, 2004, (53): 116-123.

[10] W-HChen, S-Hsu and H-P Shen, Application of SVM and ANN for intrusion detection, Computers & Operations Research, 2005, (32): 2617-2634.

[11] Y. Li, K. Chen, X. Liao and W. Zhang, A genetic clustering method for intrusion detection, pattern Recognition, 2004, (37): 927-942.

[12] A. Patcha and J-M. Park, Network anomaly detection with incomplete audit data, Computer Network, 2007, doi: 10. 1016. 2007. (04). 017.

[13] S.H.OH and W.S. Lee, An anomaly intrusion detection method by clustering normal user behavior, Computers & Security, 2003, 122(7): 596-612.

[14] H. Debar and A. Wespi, Aggregation and correlation of intrusion-detection alerts, Proc.of in Recent Advances in Intrusion Detection. RAID, 2001.

[15] A.P. Moore, R.J. Ellison, R.C. Linger, Attack Modeling for Information Security and Survivability, Technical Note, CMU, 2001.