Construction of information security evaluation index system

Cheng Cheng[1], Jingpeng Wu[2], Shuo You[3], Yanhui Zhou[*]

[1]Institute of Computer and Information Science, Southwest University, ChongQing 400715, China

[2]HaiNan Medical University, HaiNan 571199, China

[3]ChongQing Rail Transit Co. Ltd., ChongQing 400042, China

Keywords: information security; level protection; evaluation index

Abstract. As we all known, information security has become an important affecting factor about the development of information technology. Toefficiently ensure the information security, it is necessary to take regular evaluation for the security situation of information system. However, the basis work of evaluation index system is less scientific and measurable. According to the essential demand of information system security level protection (ISSLP) and the present information security status of the company system, in this paper, firstly, the evaluation index system of ISSLP is systematically constructed andindividual evaluation indexes are objectivelyclarified. Then, by analytic hierarchy process and subjective estimate method, the weight of these indexes is determined. Finally, the calculation method, which is able to reflect information security situation and the weakest security link of system, is expounded to quantify individual evaluation and comprehensive evaluation. What is more, the experimental result on real data shows that our method is performance more nice, which can provide a new thought in the aspect of information security evaluation work.

1. Introduction

The information security products which are the core part of an information system can influence the security of entire system. Especially after 2013, a lot of scandal on information security is exposed by media. People begin to pay more attention on the information security of a product, particularly information system over level three [1]. As informational level of our country increased, the evaluation of information system becomes the foundation and method to protect the security of technique and management [2]. The evaluation result can reflect the security level of the information system. But the evaluation result now are usually provide by manual method and are easily affected by artificial factors. Quantitative analysis for evaluation [3] has gained great attentions for several decades. Thus there is necessary of quantifying evaluation system of information security. In this article we will introduce our work on the development of evaluation system. First, based on baseline for classified protection of information system security [4] we build up evaluation index for information system, to make it convenient for people who do the evaluation work to consider the security level based on comprehensive indexes and release their work on the relationship of each level. Second, based on the system, we used analytic hierarchy process and make sure weight of each index. At last, we separate the index into details, and quantify each index detail, decrease the influence of artificial factors, thus set a solid foundation for the future work.

2 Information security evaluation index system

According to the baseline for classified protection of information system security [4] and the AHP method [5,6], we build up the frame of the information security evaluation index system from two aspects: technology requirements and management requirements. For example, the system is divided into five levels from the top to the bottom as Figure 1 shows. By using the five different levels, we can gather all the analyzing results of each level into a whole to measure the entire level

© 2016. The authors - Published by Atlantis Press

of security of this system [7]. Also we can measure the entire system to find out each weakness of the system we are analyzing and get the suggestion of improving the security of this system.

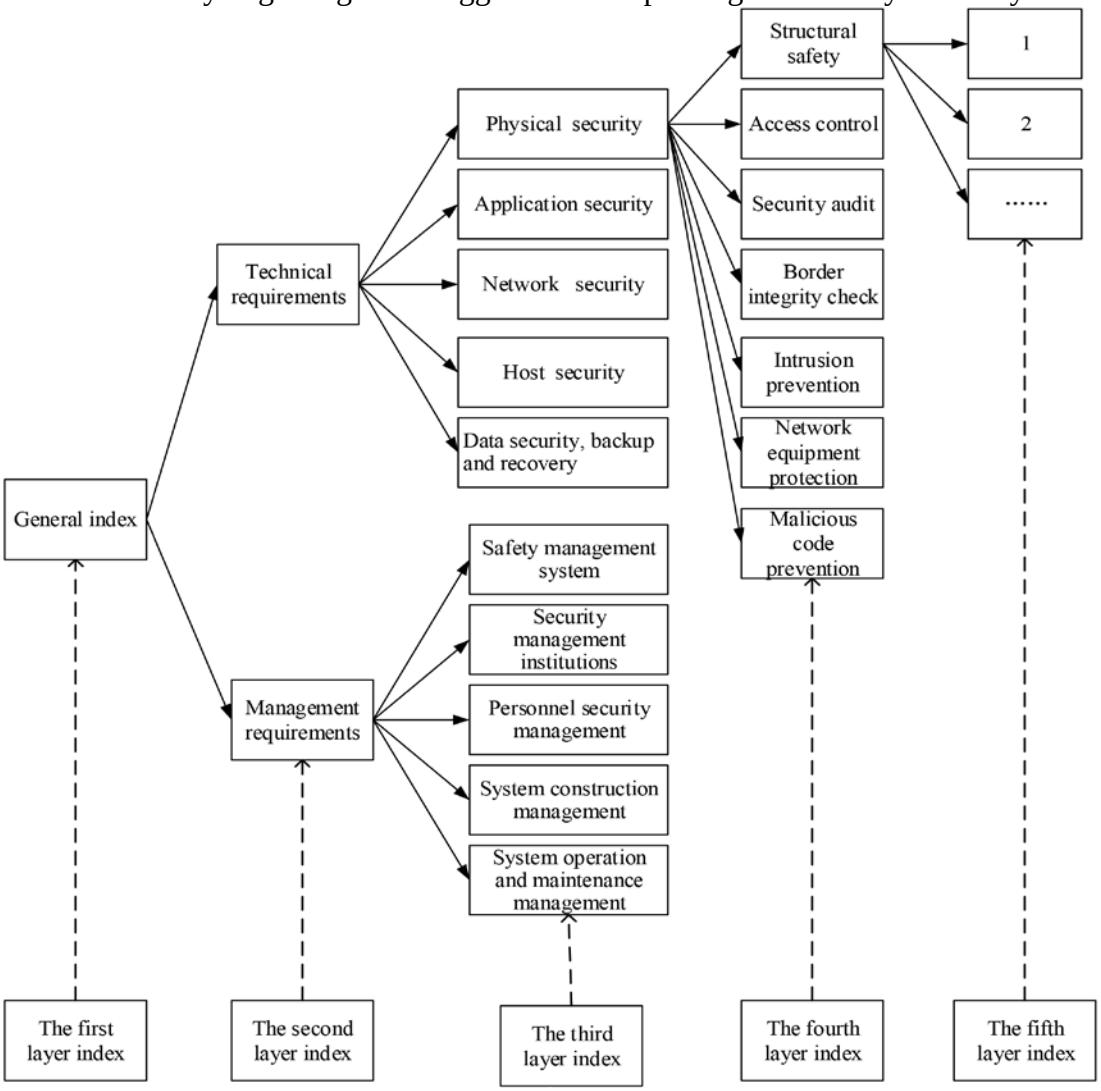

Fig1Information Security quantitative evaluation index system modal

3 Information security testing evaluation and calculation process

Finding the evaluation indexes is the core of building up the evaluation system. To support the comparability and comparability, each index contains 2 properties: index weight and standard compliance [8,9].

3.1 Information security evaluation index weight

Index weight reflects the importance of each index in the entire evaluation system. For the convenience of provide references to the evaluation system, we use hierarchical analyzing method to confirm the weight of each index. We get the Table1.The index used in this system will adjust as the development of theory and technology of information security.

Tab.1Information Security Evaluationquantitative evaluation indicator weight

The second layerIndex	Weight	The third layerIndex	Weight	The fourth layerIndex	Weight W_r	Standard compliance η_r
Technical requirements	0.48	Physical security	0.09	Physical location of choice	0.0051	87
				……	……	……
		Network security	0.14	Structural safety	0.0217	58
				……	……	……
		Host security	0.13	Identification	0.0224	79
				……	……	……
		Application security	0.11	Identification	0.0206	60
				……	……	……
		Data security and backup and recovery	0.04	Data integrity	0.0123	73
				……	……	……
Management requirements	0.52	Safety management system	0.09	Management system	0.0157	78
				……	……	……
		Security management institutions	0.05	Post setting	0.0266	68
				……	……	……
		Personnel security management	0.06	Hiring	0.0303	70
				……	……	……
		System construction management	0.12	Grading system	0.0053	93
				……	……	……
		System operation and maintenance management	0.18	Environmental management	0.0045	84
				……	……	……

In the table1,the fourth layer index which are as follows is just the one of the fourth layer index under the third layer index .We did not enumerate all of the fourth layer index because of the article length.

3.2 Calculation for information security evaluation measurements

3.2.1 Calculation of standard compliance.

1 Quantitative calculation method of standard compliance

Standard compliance [10] aims at explaining the specific evaluation requirements of each indexes, and it is also uses to describe the specific magnitude which is extracted from information security in the quantitative index. In other words, Standard compliance is a measurement of system implementation, When calculating the standard index degree of a the fourth layer, if all of the fifth layer index are satisfying the standard requirements, then the fourth layer index standard compliance should be 100%.

In calculation of the standard compliance[10], we can simply make an assumption that the index A of the fourth layer are composed of $\theta_i(i=1,2,\cdots,\kappa)$, where κ denotes the number of index in the fifth layer, then we get that the standards compliance value of θ_i is λ_j,and the largest value of its standards compliance is $\frac{1}{\kappa}$(that is to say the largest standards compliance value of A is

$\kappa \times \frac{1}{\kappa} = 1$), based on this objective basis, it is reasonable to suppose the value of formula (1):

$$\lambda_j = \begin{cases} \frac{1}{\kappa}, & \text{satisify the standard requirements} \\ \frac{1}{2 \times \kappa}, & \text{partily satisify the standard requirements} \\ 0, & \text{otherwise} \end{cases} \quad (1)$$

Therefore, the standard composition degree of the indicator A in line with the formula (2):

$$\eta_r = 100 \times \sum_{i=1}^{\kappa} \lambda_j \quad (2)$$

According to practical experience and the requirement of evaluation, this paper will calculate the fifth layer standard compliance data, which is obtained in accordance with the degree of compliance with the "information system security level of protection of basic requirements" into " meet ", "basic meet ", "generally meet", "basically does not meet "," does not meet ", according to practical experience, the degree of discrimination on the basis of its assignment as shown in Table 2.

2 The graphic representation of Standards Compliance

According to the method of the degree of standard compliance which are the formula (1) and the formula (2), we simply use an entire circle represents the overall system, or some level of safety standards in line with the overall circular area of 1, that is, the circle is complete when the cover represents a standard part of the analysis of 100% compliance, therefore, the radius of the circle is $r = \frac{1}{\sqrt{\pi}}$, If the index A of the fourth layer are composed of $\theta_i (i = 1, 2, \cdots, \kappa)$, where k denotes the number of index in the fifth layer, then in graphics the whole circle is divided into κ sectors of equal area, and the value of sector radius which the standard compliance of θ_i contributes to the standard compliance of A is r_{ϕ_i}.Then according to the formula (1),we get the formula (3) as follow.

Table 2 the degree of discrimination on the basis of its assignment

The Fifth floor index on the basis of its assignment	The degree	λ_j
It does not exist non-conformance term, or non-conformance term faces very low risk in this system;	meet	$\frac{1}{\kappa}$
It exists non-conformance term, and non-conformance term faces lower risk in this system;	basically meet	$\frac{1}{1.5 \times \kappa} \le \lambda_j < \frac{1}{\kappa}$
It exists non-conformance term, and non-conformance term faces low risk in this system;	Generally meet	$\frac{1}{2 \times \kappa} \le \lambda_j < \frac{1}{1.5 \times \kappa}$
It exists non-conformance term, and non-conformance term faces high risk in this system;	Basically does not meet	$\frac{1}{2.5 \times \kappa} \le \lambda_j < \frac{1}{2 \times \kappa}$
It exists non-conformance term, and non-conformance term faces very high risk in this system;	Does not meet	0

$$r_{\phi_i} = \begin{cases} \frac{1}{\kappa \times \sqrt{\pi}}, & \text{satisify the standard requirements} \\ \frac{1}{2 \times \kappa \times \sqrt{\pi}}, & \text{partily satisify the standard requirements} \\ 0, & \text{otherwise} \end{cases} \quad (3)$$

Therefore, according to formula (3), you can use the specific standard compliance assessment

control point, draw standard compliance degree of sector standards θ_i directly. The area of the fan-shaped can reflect the safety standards in line with the situation of θ_i .And we use totally κ standard compliance θ_i combined into a sector that is reflected in the status of compliance with safety standard of A , the sum of area of all sectors is the standard compliance θ_i , then we can find out the worst part of the degree of compliance of all the standard components A from the drawing.

3.2.2 Approach of Comprehensive index calculation

Comprehensive evaluation is to describe and evaluate the information system which is a comprehensive evaluation index information security overall situation during the evaluation, It can reflect the current information system safety. We can use the formula (1) which will give a comprehensive evaluation method to calculate the evaluation information security evaluation level index. And the index is the objective reflection on the current level of information security.

$$V = \sum_{r=1}^{\chi} \eta_r \times W_r \quad (4)$$

V denotes the information security level index, η_r describes the quantized value index of the fourth layer for item r , W_r denotes the valuation weight value index of the fourth layer for item r which is shown in table 2, χ denotes the number of index of the fourth layer. Correspondence between the level of information security and compliance level of the index are shown in table 3.

Tab.3Correspondence between thelevel of information security and compliance level of the index

V	The degree	Recognition results
$V \geq 90$	meet	The information security level of the information system which is measured is much high.
$80 \leq V < 90$	basically meet	The information security level of the information system which is measured is high.
$70 \leq V < 80$	Generally meet	The information security level of the information system which is measured is c.
$60 \leq V < 70$	Basically does not meet	The information security level of the information system which is measured is low.
$V < 60$	Does not meet	The information security level of the information system which is measured is much low.

4 Experiment

We take an assessment of the information system as an example, and analysis the assessment of structural safety which belongs to network security by experiment.

Using table 2 as the judgment basis of standards Compliance, We get the Table4.Then,according to the Table4,we get that the score of Structural safety is 58 by the formula (1) and the formula (2).And what's more, by the formula (3), we also get the figure 2 which directly understand that number 6 is the weakest security link of structural safety .

Using the analysis and calculating process of the standard compliance which belong to Structural safety as a case, we get the standard compliance of the fourth layer evaluation index by calculating the whole system index as shown in Table1.Then,According to table 1,we get η_r and W_r .Finally, applying the formula (4),we get the value of V :

$$V = 0.0051 \times 87 + 0.0217 \times 58 + 0.0224 \times 79 + \ldots\ldots + 0.0053 \times 93 + 0.0045 \times 84 = 78.3047$$

Table 4 Quantitative method of information security evaluation index weight

number	The third layer Index	The Fourth layer Index	The Fifth layer Index	λ_j
1	Network security	Structural safety	It should ensure that the business processing capabilities of major network equipment have so redundant space to meet the need of the business peak;	1/7
2	Network security	Structural safety	It should ensure that the various parts of the network bandwidth to meet the need of the business peak;	1/8
3	Network security	Structural safety	It should establish routing control and a secure access between the terminal and the service server of business;	1/10
4	Network security	Structural safety	It should draw the network topology which is consistent with the current operation.	1/12
5	Network security	Structural safety	Based on the factors ofvarious departments, for example,job functions,the importance,the import degree of information and soon. It should divide into different subnets or network segments, then, according to the principles to convenient management and control, it allocates the addresssection to various subnets andnetwork segment.	1/14
6	Network security	Structural safety	It should avoid that the important network segments are deployed at the network boundary and directly connected to an external information system. It should take reliable technical isolation means between important segments and other segments;	0
7	Network security	Structural safety	According to the order of importance of business services, it specifies bandwidth allocation priority toensure that firstly protect important host when congestion occurs on the network.	1/17

Fig2.the standard compliance of Structural safety

According to table 3, the value of V is between 70 and 80.It is so obvious that the information security level of the information system which is measured is medium, and the system basically

meet the requirements of essential demand of information system security level protection.

5 Conclusion

In this paper, according to the requirements of essential demand of information system security level protection and the present status of the company system of information security, we first construct the evaluation index system of information security level protection and clarify individual evaluation index. Then, the weight of index in the System is determined by analytic hierarchy process and subjective estimate method. Finally, the calculation method to quantify individual evaluation and comprehensive evaluation, which directly reflect the weakest security link of system, is expounded .The experimental result on real data shows that the integrated evaluation results are got more precise. It makes the evaluation staff more targeted to the information system testing, and provides a new thought for the information security evaluation work.

Acknowledgement

This work is supported by the National Key Technology Research and Development Program of the Ministry of Science and Technology of China (No. 2012BAH77F00 and No.2015BAK41B00). The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

* Supported by National Key Technology Research and Development Program of the Ministry of Science and Technology of China (No. 2012BAH77F00 and No.2015BAK41B00) .

*Corresponding author .

Email address: xiaohui@swu.edu.cn(Yanhui Zhou).

References

[1] Zhang Junbin, Lu Lei, Yu You. The classification and evaluation of Information security product system under level protection [J].Information Security and Communications Privacy, 2014(8):019.

[2] Yao Honglei, Yang Wen. Evaluation index system of information security level protection for third-class system, [J].Rallway Computer Application. 2015(215):59-61.

[3] Yang N, Yu H, Sun H, et al. Quantifying software security based on stochastic Petri nets. [J]. Journal of Computational Information Systems, 2010, 6(9): 3049-3056.

[4] General Administration of Quality Supervision, Inspection and Quarantine of the People's Republic of China.GB/T 22239-2008, Information security technology—Baseline for classified protection of information system security [s].Standards Press of China, 2008.

[5] Shubai X. AHP theory [J]. Tianjin University Press, China, 1988, 63: 252-257.

[6]Chong Xiaolei, Zhuang Zimin, Lu Chao, Chen Xin. Information Security Analysis based on AHP and Fuzzy Comprehensive Evaluation,[J]. Information Security and Communications Privacy, 2014(11):137-139.

[7]Xiao Guoyu.Information Systems Classified Security Protection Customer Evaluation, [J].Netinfo Security, 2011(7)

[8]Wang Wei, Xie Xuefu, Du Zhiliang.A Level Determination Technology for Classified Protection of Information System, [J] ,Information Security and Technology,2015(7)

[9]Zeng Ying. A System Design of Classified Protection System for Hospital Information System,[J] Microcomputer Applications,2014(3)

[10]Zhang Zhan, Qu Fang,YUwei Hu. Information security Testing and evaluation process based on the Analytic Hierarchy Process , [J]. Police Technology, 2014(6):102-107.

[11]Merkow M S, Breithaupt J. Information security: Principles and practices, [M]. Pearson Education, 2014.

[12]Fedorchenko A, Kotenko I, Chechulin A. Integrated repository of security information for network security evaluation [J]. JoWUA, 2015, 6(2): 41-57.

[13]Chen H, Chen X, Fan L, et al. Classified security protection evaluation for vehicle information system[C]//Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC), 2015 International Conference on. IEEE, 2015: 1-6.

[14]Rhee K, Jeon W, Won D. Security requirements of a mobile device management system [J]. International Journal of Security and Its Applications, 2012, 6(2): 353-358.

[15]Kazemi M, Khajouei H, Nasrabadi H. Evaluation of information security management system success factors: Case study of Municipal organization [J]. African Journal of Business Management, 2012, 6(14): 4982-4989.

[16] Tao L, Jiang X. The Building of Network Information Security Comprehensive Evaluation index System based on Analytical Hierarchy Process [J].International Journal of Advancements in Computing Technology, 2013, 5(3).

[17] Ramesh A, Suruliandi A. Performance analysis of encryption algorithms for Information Security[C]//Circuits, Power and Computing Technologies (ICCPCT), 2013 International Conference on. IEEE, 2013: 840-844.