Performance Evaluation of IP Dedicated Network Information Security System

Xiaojun Zhang, Yong Sun, Li Han, Qian Zhang
Beijing Aerospace Control Center, Beijing 100094, China
zxjyn2006@126.com

Abstract: In the paper, effectiveness method and implementation process in the evaluation process are studied from the aspect of solving key problems in the evaluation process aiming at the problem that the performance of dedicated IP network information security system can not be evaluated easily. The evaluation method based on unascertained measurement is adopted to determine the index weight and obtain the performance measurement vector of the system finally, thereby evaluating the performance of the information security system scientifically, laying foundation for organizing and implementing performance evaluation of information security system, and providing important basis for subsequent system improvement.

Keywords: Performance evaluation, unascertained measurement, information security, unascertained information.

1. Introduction

Dedicated IP network has become an important support platform of data transmission, real-time monitoring and organization command for many units. It becomes an important mode to obtain information and interact data, which provides the user with a convenient mode of information processing. Therefore, the network reliability and network security situation have become problems that are concerned by network administrators. Currently, many dedicated IP networks are equipped with some information security inspection equipment. The traditional security products constitute the basic protection, analysis and forensics system. However, since equipment interconnection, business services, etc. are changed constantly, the application scenario is more and more complex, and the system shows defects and hidden dangers during use. The risks faced by the system can be evaluated intelligently in network security risk evaluation. Main problems and contradictions of the system in the aspect of security can be discovered through scientifically analyzing the threat of the system in the aspects of confidentiality, integrity, availability, etc. The information security system is used for ensuring the security of the information system, lowering or eliminating information security threat, and it is an continuous process. The performance exerted by the information security system during the process can not be evaluated simply. A comprehensive index system should be established. Scientific evaluation and quantitative method is selected for evaluating the performance of the information security system, thereby increasing reliability of the system, pushing forward system construction, and searching an effective solution for healthy operation of the system, and improving the guarantee ability of the system.

At present, various software can not check the traceability and the influence scope comprehensively aiming at one security event, such as traffic monitoring system, anti-virus system, host control system, security management platform, etc. Figure 1 shows the traffic condition at some directions monitored by the traffic monitoring system. It is obvious that each kind of software can provide extremely limited data.

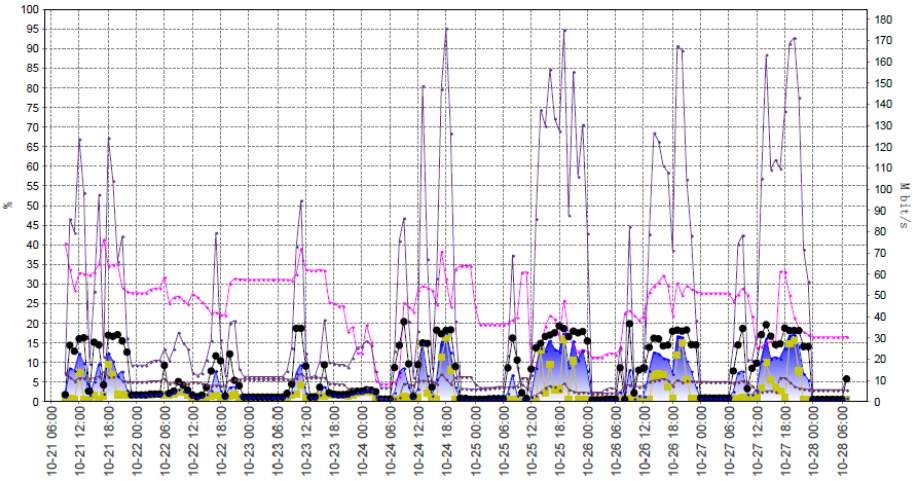

Fig.1 Traffic monitoring schematic diagram

2. Selection of evaluation methods

UnasCertained Information belongs to new uncertainty information which was presented by Professor Wang Guangyuan -Academician of Chinese Academy of Engineering, and is different from fuzzy information, random information and grey information [1]. Unascertained information refers to information that objective information is incomplete due to the limitation of objective conditions, the evidence mastered by decision-makers is imperfect, the subjective knowledge is imperfect, which is insufficient to determine the true state and quantity relationship of things, thereby leading to unclear subjective recognition. The subjective or cognitive uncertainty caused by unascertained information is called unascertainty [2].

2.1 Selection of evaluation method

The rationality of performance evaluation method indirectly affects the decision-making scientificity based on evaluation results. The availability, reliability, support ability and other factors of the information security system are comprehensively considered in order to guarantee the accuracy of the evaluation results in the aspect of selecting the evaluation methods for the purpose of searching the weak link influencing the system safeguard ability. A method based on unknown measure is selected for quantitative analysis on the system performance. Unascertained measurement evaluation method is compared with other evaluation methods [3], the unascertained measure satisfies ' normalization conditions' and ' additivity law'. The ' order' of the evaluation space can be guaranteed. Reasonable confidence identification criterion is given. Therefore, unascertained measurement evaluation method has good reliability and rationality.

The obtained evaluation data can not completely support the actual state of the evaluated objects mastered by the evaluation performance due to restrictions of various test conditions, test time, index specialty, etc. in the process of information security system performance evaluation, thereby producing evaluation unascertainty. Treatment of unascertained information by a mathematical method related to unascertained measure can provide result credibility and accuracy to certain extent.

2.2 Evaluation model algorithm based on unascertained theory

In the performance evaluation model, X is set as a performance evaluation plan. It is evaluated that X has m indexes I_1, I_2, $I_3\cdots\cdots I_m$. They are recorded as $I=\{I_1, I_2, I_3\cdots\cdots I_m\}$. x_j is used for indicating the observation value of plan X under the index I_j. $C=\{C_1, C_2, C_3\cdots\cdots C_m\}$=(excellent, good, intermediate, worse and bad) is set as the evaluation space. $C_K(1\leq k\leq 5)$ is set as the kth comment rate. Table 1 refers to the performance evaluation index system which is established based on above influence factors.

Table 1 Ability evaluation index system

Performance evaluation index system	Management foundation I_1	Management level I_{11}
		Informational base index I_{12}
		Management system feasibility I_{13}
		Management standardization I_{14}
	System/plan guarantee ability I_2	System completeness I_{21}
		System rationality I_{22}
		Effectiveness of information security event handling plan I_{23}
		Integrity of technical data I_{24}
	Personnel foundation I_3	Knowledge and demand matching rate I_{31}
		Business capability I_{32}
		Personnel stability I_{33}
		Employee collaboration level I_{34}
		Transformation and innovation degree of employees I_{35}
	Hardware equipment guarantee ability I_4	Business scope covered by products I_{41}
		Hardware integration and extensibility I_{42}
		Information security equipment troubleshooting capability/stability I_{43}
	Software equipment guarantee ability I_5	Virus reservoir /rule base updating cycle I_{51}
		Completeness/effectiveness of information security strategy I_{52}
		Real-time performance of information security event detection I_{53}

2.2.1 Single index unascertained measure of performance evaluation

The observed values x_j of object x about index I_j are different. x is located in different comment rates due to the index. It is set that x_j makes x in the kth comment rate c_k at degree μ_{jk}. Wherein, $\mu_{jk}=\mu(x_j \epsilon c_k)$. μ_{jk} is a measurement result on the degree. It must meet the measurement principle as a measure: nonnegative criticality, additivity and normality [4]. The μ_{jk} meets the follows:

(1)$0 \leq \mu_{jk} \leq 1$

(2) $\mu(x_j \in \cup_{K=1}^{K} C_K) = \sum_{K=1}^{K} \mu(x_j \in C_K)$

(3) $\mu(x_j \epsilon c)=1$

Wherein, j=1, 2, 3, …m; k=1, 2, 3, 4, 5, μ_{jk} meeting the above-three measurement criteria are unascertained measures, and they are hereinafter referred to as measures.

$$(\mu_{jk})_{m\times 5} = \begin{bmatrix} \mu_{11} & \cdots & \mu_{15} \\ \vdots & \ddots & \vdots \\ \mu_{m1} & \cdots & \mu_{m5} \end{bmatrix} \quad (1)$$

Matrix (2.1) is a single-index measurement evaluation matrix of object x, wherein μ_j(j=1,2, 3, …m) indicates that xj makes x in the unascertained measure of different comment rates.

2.2.2 Determination of weighed value of performance evaluation index

The observed value x_j of the object x about the index x_j makes the object in c_1, c_2, …c_5. The unascertained measure of each comment rate is $\mu_j=(\mu_{j1}, \mu_{j2}, \mu_{j3}, \mu_{j4}, \mu_{j5})$. The contribution of the index I_j on the object x classification is known. Five component values of μ_i are more scattered, w_j is smaller, the value is more concentrated, w_j is larger, and the information entropy determined by the measure μ_{jk} is set as follows:

$$H(j) = -\sum_{K=1}^{5} \mu_{jk} \bullet \log \mu_{jk} \quad (2)$$

$$\mu_j = 1 - \frac{1}{log5} H(j) = 1 + \frac{1}{log5} \sum_{K=1}^{5} \mu_{jk} \bullet \log \mu_{jk} \quad (3)$$

$$w_j = V_j / \sum_{j=1}^{m} V_j \quad (4)$$

The nature of the information entropy that μ_{jk} value is more concentrated, maximum can be obtained, namely 1. On the contrary, μ_{jk} value is more scattered, V_j value is closer to 0. w_j defined by formula (4) refers to the classification weight of indicator I_j about x.

$$W=(W_1, W_2, W_3, W_4, \cdots W_m) \quad (5)$$

It is called classification weight vector of the index I_1, I_2, I_3…I_m about x. The index weight vector is very important in the unascertained comprehensive evaluation system.

If the single index measure about x is evaluated as the matrix (2 .1), all index classification weight about x is formula (5). $\mu\mu = W \bullet \left(\mu_{jk}\right)_{m\times 5}$ is set.

$$\mu=(\mu_1,\ \mu_2,\ \mu_3,\ \mu_4,\ \mu_5) \tag{6}$$

Therefore, μ is the evaluation vector of x.

2.2.3. Evaluation criteria of implementation ability

It is ordered to classify by comment rates. The kth comment rate c_k 'is better than' k+1th comment rate $c_{k+1.}$ Therefore, the maximum measure recognition criteria are not applicable. Confidence recognition criteria are applied. Confidence recognition criteria: the confidence level is set as λ, (λ>0.5) is usually 0.6 or 0.7.

$$k_0 = \min_k[(\sum_{t=1}^{k} \mu_t) \geq \lambda, k = 1,2,3,4,5] \tag{7}$$

It is judged that x belongs to the k_0th com rate c_{k_0}. The above established performance evaluation model based on the unascertained measure avoids the randomness due to subjective factor evaluation. Information entropy and confidence recognition criteria are respectively adopted in the aspect of determining the weight and recognition criteria of different evaluation indexes, therefore the evaluation results are more objective. The evaluation method is simple, which can be realized easily, and it is highly operable.

2.3 Assessment process of performance evaluation

Firstly, the opinion of workers is solicited through self-assessment and questionnaire as basic reference data. Then, 20 experts are organized for on-site investigation. Each index is respectively scored, and data is collected. The data is distributed on five evaluation grades. Details are shown in table 2.

Table 2 Index score table

Index	Excellent	Good	Intermediate	Worse	Bad	Index	Excellent	Good	Intermediate	Worse	Bad
I_{11}	0.1	0.6	0.2	0.1	0	I_{33}	0.2	0.3	0.35	0.15	0
I_{12}	0.05	0.4	0.3	0.25	0	I_{34}	0.2	0.5	0.2	0.1	0
I_{13}	0.1	0.4	0.3	0.2	0	I_{35}	0.3	0.5	0.1	0.1	0
I_{14}	0.3	0.6	0.1	0	0	I_{41}	0.3	0.45	0.2	0.05	0
I_{21}	0.45	0.35	0.15	0.05	0	I_{42}	0.2	0.6	0.2	0	0
I_{22}	0.15	0.35	0.15	0.25	0.1	I_{43}	0.25	0.4	0.15	0.15	0.05
I_{23}	0.1	0.4	0.1	0.4	0	I_{51}	0.2	0.35	0.35	0.1	0
I_{24}	0.1	0.3	0.1	0.4	0	I_{52}	0.25	0.3	0.25	0.1	0.1
I_{31}	0.25	0.2	0.5	0.05	0	I_{53}	0.2	0.25	0.3	0.15	0.1
I_{32}	0.15	0.25	0.45	0.1	0.05						

The following single index measure matrix is obtained according to the above charge statistic data:

$\mu_{jk} = \begin{pmatrix} u_{jk}^1 \\ u_{jk}^2 \end{pmatrix}$, wherein,

$$u_{jk}^1 = \begin{pmatrix} 0.1 & 0.6 & 0.2 & 0.1 & 0 \\ 0.05 & 0.4 & 0.3 & 0.25 & 0 \\ 0.1 & 0.4 & 0.3 & 0.2 & 0 \\ 0.3 & 0.6 & 0.1 & 0 & 0 \\ 0.45 & 0.35 & 0.15 & 0.05 & 0 \\ 0.15 & 0.35 & 0.15 & 0.25 & 0 \\ 0.1 & 0.4 & 0.1 & 0.4 & 0 \\ 0.1 & 0.3 & 0.1 & 0.4 & 0 \\ 0.25 & 0.2 & 0.5 & 0.05 & 0 \end{pmatrix} \quad u_{jk}^2 = \begin{pmatrix} 0.2 & 0.3 & 0.35 & 0.15 & 0 \\ 0.2 & 0.5 & 0.2 & 0.1 & 0 \\ 0.3 & 0.5 & 0.1 & 0.1 & 0 \\ 0.3 & 0.45 & 0.2 & 0.05 & 0 \\ 0.2 & 0.6 & 0.2 & 0 & 0 \\ 0.25 & 0.4 & 0.15 & 0.15 & 0.05 \\ 0.2 & 0.35 & 0.35 & 0.1 & 0 \\ 0.25 & 0.3 & 0.25 & 0.1 & 0.1 \\ 0.2 & 0.25 & 0.3 & 0.15 & 0.1 \end{pmatrix}$$

$$V_j = 1 - \frac{1}{log5} H(j) = 1 + \frac{1}{log5} \sum_{K=1}^{5} \mu_{jk} \bullet log\mu_{jk}$$

and formula (4)

$$w_j = V_j / \sum_{j=1}^{m} V_j$$

The classification weight vector W of all indexes in system performance valuation model is obtained as follows:

W=(0.10221,0.05662,0.09004,0.05674,0.06324,0.0843,0.07338,0.05627,0.02336,0.04027,0.04044,0.003872,0.05281,0.06164,0.02245,0.02326,0.01914,0.05618)

The evaluation vector of the system performance model can be obtained as a result: $\mu = w \cdot (\mu_{jk})_{19X5}$=(0.234,0.417,0.212,0.084,0.053). λ=0.6 is obtained. It is concluded according to formula (2.7) that 0.234+0.417=0.651>0.6 when k_0=2. The above results show that the system performance is good. The evaluation results and all index scores in the matrix are combined. It is obvious that the system rationality should be improved in the aspect of system/plan guarantee. The strategy completeness and effectiveness in the aspect of system software equipment guarantee ability as well as real-time performance of the information security event detection are slightly weak, which are consistent with practical situation, and should be emphasized. Related measures are adopted for improving the level in these aspects, thereby guaranteeing that the system can be more effective.

3. Conclusion

In the paper, a performance index system of the IP network information security system is established. Comprehensive performance is evaluated for the system through the evaluation method based on unascertained measure. Risks faced by IP network should be comprehensively analyzed subsequently. Rules and systems should be further perfected, and handling means of information security events should be enriched. The technical data should be enriched continuously , and the ability of related personnel to handle information security events should be improved, thereby exerting the maximum performance of the system.

References

[1]J. van der Geer, J.A.J. Hanraads, R.A. Lupton, The art of writing a scientific article, J. Sci. Commun. 163 (2000) 51-59.
[2] W. Strunk Jr., E.B. White, The Elements of Style, third ed., Macmillan, New York, 1979.
Reference to a chapter in an edited book:
[3] G.R. Mettam, How to prepare an electronic version of your article, in: B.S. Jones, R.Z. Smith (Eds.), Introduction to the Electronic Age, E-Publishing Inc., New York, 1999, pp. 281-304.
[4] R.J. Ong, J.T. Dawley and P.G. Clem: submitted to Journal of Materials Research (2003)
[5] P.G. Clem, M. Rodriguez, J.A. Voigt and C.S. Ashley, U.S. Patent 6,231,666. (2001)
[6] Information on http://www.weld.labs.gov.cn