International Journal of Security and Its Applications
Vol. 9, No. 3 (2015), pp. 49-62
http://dx.doi.org/10.14257/ijsia.2015.9.3.06

An Improved Evaluation Index System for the Host Information Security Evaluation System

Yuyi Ou, Jinbiao Xie and Jie Ling

Faculty of Computer
Guangdong University of Technology
Guangzhou, China
ouyuyi@163.com, biaobiao0607@126.com, jling@adut.end.cn

Abstract

This paper studies the principle of the host information security risk assessment and the method to determine the right of each index's weight. Because Liao Hui and others proposed network terminal security assessment index system exists index weights unreasonable distribution problem, using Delphi method and AHP calculate each index weight and the weights of total ranking of lowest level indexes relative to the highest lever indexes, identified the indicators which have greatest impact to the assessment objectives and apply it to a host of information security evaluation system. Uses the fuzzy comprehensive evaluation method and combined with examples to prove the index system after improving its weight distribution can be more scientifically reflect the importance of the indexes in the evaluation system and the result of the host information security evaluation is reasonable and comprehensive.

Keywords*: Host information security; Index weight distribution; AHP; Delphi; Terminal Security Assessment*

1. Introduction

With the rapid development of information technology, information technology has promoted the development of the world also has brought a lot of convenience to people's life, but at the same time information in a different way to control and influence our life, industries are increasingly dependent on information systems, and attendant information security issues have become increasingly prominent. International conflict of information access, control and use is becoming more and more fierce, all countries on the understanding of information and information systems security has risen to the height of maintaining social stability and national security [1]. According to statistics, within the scope of the global, a computer virus invasion happens in every 20seconds; about 25% of the Internet firewall is compromised; Steal business information event with 260% of the average monthly rate of increase; about 70% of the network executives report suffered losses because disclosure of confidential information [2], the 2006 year China network security analysis report pointed out that [3] : network attacks occur in the same period in 2006 is more than one times in the same period in 2005; Baidu in 2010 was hacked again, the offline for up to five hours; The end of 2011, CSDN, End of the World, and many other Internet companies' information is publicly available for download. So it can be imagined that the resulting loss to the country and to the people, pure technically impossible fundamentally to solve the security problems of information system, instead of from the Internet virus, hacker attack is becoming more and

ISSN: 1738-9976 IJSIA

more and more serious threat, the risk assessment is the premise and foundation of information system security, therefore the risk of security of the host of a comprehensive assessment is of great importance.

Due to the factors involved in the risk assessment to be very diverse, but also between the various factors that influence each other [4], currently in the evaluation process has not yet formed a unified index. Liao Hui [5] had taken the information security risk assessment which based on the norms for assessing basis, proposed a network terminal security evaluation system. To some extent, the scope and the extent of the assessment are more comprehensive, and reduce the difficulty of implementing network terminal security assessment. However, there is insufficient in determining the weight of each index in the process.

Taking into account the weight distribution of the index system of rationality and science as well as the actual operation of the host information security evaluation index system is not possible to assess all the indicators are put into the system for evaluation and other reasons. In this paper, using the analytic hierarchy process [6] and Delphi method [7] to get each layer index weighting coefficient sets, and calculate the total weight sorting of the bottom index relative to the assessment objectives, to determine several indexes which have the greatest impact on the assessment of the target, and take them as host information security evaluation index.

2. Host Information Security Risk Assessment Related Concepts and Principles

A. Host Information Security Risk Assessment Related Concepts

1) Information Security Risk Assessment

Information Security Risk Assessment [8] is standing on risk management perspective, using scientific methods to analyze the threats and vulnerabilities which the information system faced. By evaluating information security incidents hazards and possible impacts, propose effective countermeasures and protective measures to guard and resolve against the risk of information security, and thus the risk control within an acceptable range.

2) Assets

Risk assessment begins with the identification of information assets, the assets of the organization are valuable information or resources, Confidentiality, integrity and availability are the three attributes of information assets evaluation [9].

3) Information Asset Assessment

Evaluation of information assets consist of two parts: identifying information assets and estimating the value of the asset. Identifying information is confirmed by evaluating the organization's information assets and giving the assets list. Estimating of the value of the asset is to estimate the value of information assets, there are more mainly consider the importance of the assets, the carrying value of the asset is secondary.

4) Vulnerability

Weak points that can be used by the threat and have impact on assets.

5) Vulnerability Assessment

Vulnerability assessment is to get the weaknesses and shortcomings of the information assets through a variety of testing methods. The existence of these weaknesses and defects may cause leaks information assets from unauthorized access, assets useless or uncontrolled.

6) Threat

Threat is potential damage factors or events to the organization and its assets, is one of the important elements that constitute information security risks.

7) Threat Assessment

Threat assessment information assets are to assess the potential harm that information asset will face. Threats may come from deliberate or accidental events, May also be derived from the system either directly or indirectly attack. Generally speaking, the threat uses the system, service or application weaknesses to cause asset damage.

The relationship between them is: the threat use the vulnerability to damage or affect the assets.

B. Host Information Security Risk Assessment and Principles

The host information security risk assessment is the assessment of the computer system, the value of assets on the network, potential threats, existing vulnerabilities and the possibility of vulnerability caused by the threat of security incidents utilization system, according to certain criteria, and combined value of the assets involved in security incidents to determine the impact when security incidents happen. The basic principles of risk assessment [10] as shown in Figure 1:

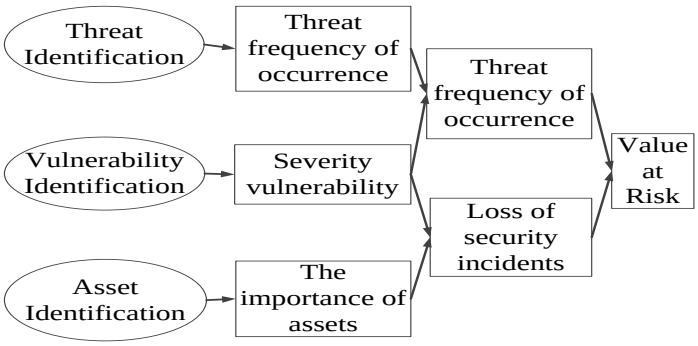

Figure 1. The Basic Principles of Risk Assessment

It can be seen from Figure 1 host information security risk assessment is mainly related to the 3 elements of asset, threat and vulnerability. Every valuable asset will face a lot of kinds of threats, the value of assets, the higher value of the assets, the more threat it will face, but only when threatened use assets vulnerability itself may affect assets or damage. However, indicators of threats and vulnerabilities related to a host of information security faced with multi-level, multi-factor, uncertainty and complexity, therefore reasonably determine index weight became an objective, scientific assessment of the premise. Combined evaluation model and methods based on such a premise, comprehensive analysis of the host asset value, threat, vulnerability and impact on the value of the probability and the impact after the risk happened, such risk assessments can obtain conviction.

3. Related Work

In recent years, around the multiple indicators of host security risk assessment, relevant knowledge in other areas continues to penetrate, making the host security risk assessment methods continue to enrich. About how to determine the indexes weight of the host security risk assessment, both at home and abroad have proposed dozens of kinds of empowerment method. In general, that can be classified into three categories: Subjective weighting evaluation (like Fuzzy comprehensive evaluation method, Delphi), Objective weighting evaluation method (like analytic hierarchy process) and Integrated weighting method (like Fuzzy analytic hierarchy process). Subjective weighting method adopted

qualitative method, experts according to their experience to make a subjective judgment and get the weight. Objective weighting method based on the correlation between indicators or indicators of variation to determine weights. Integrated weighting method will be both subjective and objective weighting method for gathering reflects the subjective color and reflects the objective facts.

Reference [11] presents fuzzy analytic hierarchy process, and uses fuzzy consistent matrix to express the multiple comparison value of biding evaluation indexes. Through matrix calculation, the biding evaluation indexes weights can be determined in a scientific way. Reference [12] introduces the main content of weight coefficient computing method based on AHP, and the step of root and sum of two judgment matrix disposal methods. Reference [13] using the modified Delphi index weight method to study the teachers' ability of Distance Higher Education, confirm 20 important ability of teachers, and analyze each one of the teacher abilities, in order to provide some guidance for distance higher education practice.

4 Lack of Terminal Secutity Evaluation Index System

The index of threatening and vulnerability that the host information security face has features such as multi-level, multi-factor, uncertainty and complexity, therefore reasonably determine index weight became a premise of an objective and scientific assessment. Combined assessment models and methods in such a premise, based on a comprehensive analysis of the host asset value, threat, vulnerability and likelihood of occurrence and the impact of the risk caused by, so can obtain an objective and scientific risk assessment values. However, the literature [5] used expert consultation and principal component analysis methods to determine the weight of each index which can cause some problems. Expert consultation in accordance with the knowledge and experience of experts to determine the weight of each indicator may cause deviation of the evaluation results due to the formation of the subjective factors; Principal component analysis method solves an objective assessment to determine the weight problem, but it will lead to loss of information, more important point is that in the literature [5], there is no scientific way to verify the index weight distribution is reasonable.

5. Improved Evaluation Index System

C. Improved principle

Analytic Hierarchy Process (AHP) is a system analysis method that can combine the qualitative analysis and quantitative analysis together. It can break down complex problems into a hierarchical structure and has clear ideas, simple method, widely applicable, systematic, and other characteristics. Person's subjective judgment can be used to express and deal with the number of forms; also AHP can handle both quantitative and uneasy quantitative factors, prompt people through conformance testing to determine whether the problem is consistent subjective [10]. Using this method to determine the effectiveness and practicability of the index weight had been verified in multiple areas [14-17].

Evaluation indicators reflect different aspects of the security situation in the host information system and the impact of each indicator on the system are not the same, for a more reasonable distribution of these weights. This paper uses AHP to calculate weights distribution as follows: (1) Hierarchical sequence of evaluation index system to form a hierarchical, orderly hierarchy model. (2) Each index on the same floor pairwise comparison to find out the importance relative to the upper level of a common index and construct judgment matrix. (3) Calculation on constructing judgment matrix of indicators for the

relative weight of an upper layer of common indicators. (4) One-level weighting and consistency verification. (5) Calculating and sorting the synthesis weight of the indicators at the bottom relative to the tops. (6) Total weight sorting consistency verification.

D. Improvement of the indicators of relative weight

1) Index system of finishing

Literature [5] had put forward four-level evaluation system which after finishing as shown in Table 1.

Table 1. Four Level Evaluation Index System

Target Layer	A Layer	B Layer	C Layer
Information assets	A1	B1	C1, C2, C3, C4, C5, C6
		B2	C7, C8
		B3	C9, C10
		B4	C11, C12
	A2	B5	C13, C14
		B6	C15, C16, C17, C18
	A3	B7 B8 B9 B10	/
	A4	B11 B12	/
Threatening	A1	B1	C1, C2, C3, C4, C5, C6
		B2	C7, C8, C9
	A2	B3	C10, C11, C12, C13
		B4	C14, C15
		B5	C16, C17, C18, C19, C20, C21
Vulnerability	A1	B1	C1, C2, C3, C4, C5, C6
		B2	C7, C8, C9, C10
		B3	C11, C12, C13, C14
		B4	C15, C16, C17
	A2	B5	C18, C19

Indicators are divided into target layer and layer A, B, C, D layers. Target layer contains 3 goals: information assets, threatening and vulnerability. Corresponding index system of literature [5], for information assets target, A1 on behalf of the hardware, A3 represent data, B6 representative application software; for threatening targets, A1 on behalf of environmental threats, B2 represent technical failure, B5 represent intentional behavior.

2) Construct judgment matrix

Based on Table 1, the method of constructing judgment matrix is as follows: For index O, we can use the proportion of 1 ~ 9 scaling method [18] to assign O's lower indexes mi and mj which is more important to O, as shown in Table 2.

Table 2. 1 ~ 9 Degrees Judgment Matrix Standard

The importance of scale	Meaning
1	Compared to the representation of 2 elements, is of the same importance
3	Compared to the representation of 2 elements, the former was slightly more important than the latter
5	Compared to the representation of 2 elements, the former was more important than the latter
7	Compared to the representation of 2 elements, the former is more important than the latter strongly
9	Compared to the representation of 2 elements, the former is extremely important than the latter
2,4,6,8	Represents the middle value of the judgments
Reciprocal	If the ratio of the importance of the element i and element j is aij, then the ratio of the importance of the element with the element i j is aji=1/aij

Judgment matrix constructed to satisfy the following characteristics: $a_{ij}>0$； when i=j, $a_{ij}=1$ ； $a_{ji}=1/a_{ij}$; Where a_{ij} as the index i compared the importance of the index j. It can be seen that the judgment matrix is a mutually inverse matrix.

Take C16-C20 of Threat target for example, its judgment matrix is shown as Table 3.

Table 3. Judgment Matrix of Threat's C16-C20

/	B1	B2	B3	B4	B5	B6
B1	1	1	2	1/3	1/3	2
B2	1	1	1/3	1/3	1/3	1/2
B3	1/2	3	1	1/2	1/2	3
B4	3	3	2	1	2	3
B5	3	3	2	1/2	1	3
B6	2	2	1/3	1/3	1/3	1

3) Single-level weight calculation and consistency verification

In order to calculate the relative weight and consistency inspection need to find the judgment matrix corresponding to the largest eigenvalue and eigenvector, if they can pass the conformance tests, the normalized eigenvectors after processing is the relative weight. Since the judgment matrix itself has considerable margin of error, so when calculating the maximum eigenvalue and corresponding eigenvectors do not need to pursue higher accuracy. Therefore, the specific steps of single-level weight calculation are as follows: (1) Calculate the product M_i of each line of n-order judgment matrix A: $M_i = \prod_{j=1}^{n} a_{ij}$, i=1, 2…n; (2) Calculated the n-square of Mi: $w_i' = \sqrt[n]{M_i}$, i=1, 2…n; (3) Normalized the Vector $w' = (w_1', w_2', \ldots, w_n')^T$ like :$W_i = \frac{w_i'}{\sum_{j=1}^{n} w_j'}$,i=1,2…n; then W=（W_1,W_2,…， W_n）is the eigenvector we want. (4) Calculate the maximum of judgment matrix eigenvalue λ_{max} ： $\lambda_{max} = \sum_{i=1}^{n} \frac{(AW)_i}{nW_i}$, Where $(AW)_i$ represent the i-th element of the vector (AW). (5) Consistency verification. When the random consistency ratio $CR = \frac{CI}{RI} < 0.1$, considered judgment matrix has satisfactory consistency, indicates that you can use the eigenvector as weight vector and the weight distribution is reasonable, otherwise need to follow the proportion of 1 ~ 9 scaling method to reconstruct the judgment matrix and then recalculate according to the above steps until pass consistency verification. CI is the consistency index of judgment matrix and $CI = \frac{\lambda_{max} - n}{n - 1}$. RI is the mean random consistency index. In accordance with the RI algorithm, RI value of 1~10 order judgment matrix can be obtained using by MATLAB and shown in Table 4.

Table 4. Average Random Consistency Index

n	1	2	3	4	5
RI	/	0	0.58	0.90	1.12
n	6	7	8	9	10

RI	1.24	1.32	1.41	1.45	1.49

As can be seen from Table 4, it can be considered that it always pass the conformance tests when the judgment matrix is constructed by 2-order, then RI=0.00. At this time, use the steps above to get weight distribution will be meaningless, so in this case using Delphi method not only take into account the Validity of results but also consider realistic operation. Vulnerability targets, for example, the judgment matrix and relative weight of C layer relative to the B1 (physical environment) are shown in Table 5.

Table 5. The Judgment Matrix and Relative Weight of C Layer Relative to the B1

/	C1	C2	C3	C4	C5	C6	W
C1	1	5	4	7	7	7	0.4968
C2	1/5	1	1	2	2	2	0.1233
C3	1/4	1	1	5	6	6	0.2149
C4	1/7	1/2	1/5	1	1	1	0.0561
C5	1/7	1/2	1/6	1	1	1	0.0545
C6	1/7	1/2	1/6	1	1	1	0.0545

From Table 5, in conjunction with single-level weight calculation steps and formulas can get largest eigenvalue λ_{max} and CI of this judgment matrix, λ_{max} =6.2211， CI=0.04422. Check for 6 order of judgment matrix in Table 1, we can get RI=1.24, and CR=CI/RI=0.0357<0.1,therefore, this judgment matrix pass consistency tests. This computed weight distribution w= $(0.4968, 0.1233, 0.2149, 0.0561, 0.0545, 0.0545)^T$ can be accepted.

4) Total weight sorting and consistency verification

Total weight sorting is calculated the weight sorting from top to bottom indicators calculation one by one in the same layer relative to the target in the highest level, thus it is concluded that the relative weight of the underlying index relative to the objectives of assessment and at the meantime to determine its importance in the evaluation process. As shown in Table 1 evaluation index system is divided into four layers: the target layer, A layer, B layer and C layer, assuming that relative to a target O in the target layer, the index number of A, B, C layer is m, n and p. The steps of total weight sorting are as follows: (1) the relative weight of m indexes in A layer relative to target O is a1，a2…am; (2) the relative weight of n indexes in B layer relative to an index i in A layer is b_{1i}， b_{2i}…b_{ni}, where i=1,2,…m, if B_j and A_i no link, then b_{ji}=0（$1\le j\le n$）； (3) calculate the weight of the j-th index in B layer relative to target O, $q_j = \sum_{i=1}^{m} a_i b_{ji}$,$1\le j\le n$； (4) calculate and sort the total weight of B layer relative to target O, q_j（$1\le j\le n$）; (5) calculate Random consistency rate CR' of B layer relative to target O, if the consistency index of index in B layer relative to index A_i is CI_i and the corresponding average random consistency index is RI_i, when $CR' = \frac{\sum_{i=1}^{m} a_i CI_i}{\sum_{i=1}^{m} a_i RI_i}$ <0.1, the total weight sorting of B layer is acceptable. (6) the relative weight of p indexes in C layer relative to an index k in B layer is c_{1k}, c_{2k}…c_{nk}, where k=1, 2,…p, if Cr and B_k no link, then c_{rk}=0($1\le r\le p$); (7) calculate the weight of the r-th index in C layer relative to target O, $w_r = \sum_{k=1}^{n} q_k c_{rk}$,$1\le r\le p$; (8) calculate and sort the total weight of C layer relative to target O, w_r($1\le r\le p$); (9) calculate Random

consistency rate CR of C layer relative to target O, if the consistency index of index in C layer relative to index B_k is CI_k and the corresponding average random consistency index is RI_k, when $CR = \frac{\sum_{k=1}^{n} q_k CI_k}{\sum_{k=1}^{n} q_k RI_k} < 0.1$, the total weight sorting of C layer is acceptable. Vulnerability target, for example, the result of total weight sorting of B layer relative to vulnerability target is shown in Table 6, and the result of total weight sorting of C layer relative to vulnerability target is shown in Table 7.

Table 6. The Total Weight Sorting of B Layer Relative to Vulnerability

A Layer / B Layer	A1(Technical vulnerability)	A2(Management Vulnerability)	The total size of the index weight q_j（1≤j≤5）	Sort
Weight a / Weight b	0.3	0.7		
B1(Physical Environment)	0.1220	0	0.03660	5
B2(System Software)	0.5584	0	0.16752	3
B3(Application System)	0.3196	0	0.09588	4
B4(Technology Management)	0	0.3	0.21	2
B5(Organizational management)	0	0.7	0.49	1
λmax	3.0181	2	/	/
CI	0.00905	0	/	/
RI	0.58	0	/	/

Consistency test of B layer relative to Vulnerability: CR’ =（0.3*0.00905+0.7*0）/（0.3*0.58+0.7*0）=0.0156<0.1, Validated.

Table 7. The Total Weight Sorting of C Layer Relative to Vulnerability

B / C	B1	B2	B3	B4	B5	Wr(1≤r≤19)	Sort
q / c	0.0366	0.1675	0.0959	0.21	0.49		
C1	0.4068	0	0	0	0	0.0149	11
C2	0.1233	0	0	0	0	0.0045	16
C3	0.2149	0	0	0	0	0.0079	14
C4	0.0561	0	0	0	0	0.0021	17
C5	0.0545	0	0	0	0	0.0020	18
C6	0.0545	0	0	0	0	0.0020	19
C7	0	0.6109	0	0	0	0.1023	4
C8	0	0.2173	0	0	0	0.0364	7
C9	0	0.1055	0	0	0	0.0177	10
C10	0	0.0663	0	0	0	0.0111	13
C11	0	0	0.3570	0	0	0.0342	8
C12	0	0	0.1283	0	0	0.0123	12
C13	0	0	0.0658	0	0	0.0063	15
C14	0	0	0.4489	0	0	0.0430	6
C15	0	0	0	0.6370	0	0.1338	3

C16	0	0	0	0.2583	0	0.0542	5
C17	0	0	0	0.1047	0	0.0220	9
C18	0	0	0	0	0.5	0.2450	1
C19	0	0	0	0	0.5	0.2450	2
Λmax	6.2211	4.1962	4.1221	3.0387	2	/	/
CI	0.0442	0.0654	0.0407	0.0194	0	/	/
RI	1.24	0.9	0.9	0.58	0	/	/

Consistency test of C layer relative to Vulnerability:

CR=(0.0366*0.04422+0.16752*0.0654+0.09588*0.0407+0.21*0.01935+0)/ (0.0366*1.24+0.16752*0.9+0.09588*0.9+0.21*0.58+0)= 0.0508<0.1，Validated.

5) Total weight sorting of bottom indexes relative to the top target

The information assets of host information safety evaluation system designed in this paper contains three properties: information confidentiality, information integrity, and information availability, so we do not calculate the weight distribution of information assets of this index system. We can get the influence of evaluation results sorting as well as the distribution of the weight that the indexes in C layer of vulnerability and threatening relative to assessment results according to the above steps and method. The result is shown in Table 8.

Table 8. C Level Indicators Total Ranking

Sort	Threatening of total weight sorting		Vulnerability of total weight sorting	
/	The bottom index	Weight distribution	The bottom index	Weight distribution
1	C19	0.1518	C18	0.2458
2	C20	0.1205	C19	0.2458
3	C14	0.096	C15	0.1342
4	C10	0.0869	C7	0.1026
5	C8	0.0766	C16	0.0544
6	C18	0.0709	C14	0.0431
7	C15	0.064	C8	0.0365
8	C16	0.0608	C11	0.0343
9	C9	0.0482	C17	0.0221
10	C12	0.0479	C9	0.0178
11	C21	0.0402	C1	0.0149
12	C17	0.0358	C12	0.0123
13	C5	0.0236	C10	0.0111
14	C3	0.017	C3	0.0079
15	C7	0.0152	C13	0.0063
16	C11	0.015	C2	0.0045
17	C13	0.0101	C4	0.0021
18	C4	0.0073	C5	0.002
19	C1	0.0048	C6	0.002
20	C2	0.0038	/	/
21	C6	0.0035	/	/

6. The Fuzzy Comprehensive Evaluation Method

Fuzzy Comprehensive Evaluation method comes from the theory of fuzzy sets [19] of the cybernetics expert Zadeh L.A who comes from United States. It uses the fuzzy relationship synthetic principle to give the things which have a variety of attributes and the attribute boundary is not clear a reasonably comprehensive and overall evaluation.

To express the relationship of a particular element and fuzzy sets, fuzzy comprehensive evaluation method is introduced to the concept of membership. Membership is represented by a number in the closed interval [0, 1], membership values closer to 1, said the current element is higher on the membership degree of fuzzy sets and vice versa.

The basic steps of fuzzy comprehensive evaluation are as follows:

E.Establish the factors set

The criterion layer based on the hierarchical analysis of host information security evaluation method recognition set as the factor set U= {Information assets, Threatening, Vulnerability}, wherein each subset single factor is:

Information assets={C1,C2⋯,C18};

Threatening={ C1,C2⋯,C21};

Vulnerability={ C1,C2⋯,C19};

F.Establish the evaluation set

Judge gives an evaluation result set of evaluation object. General according to the actual situation the evaluation level can be divided into 4 ~ 5 degree, and the evaluation result set is V={V1,V2,⋯,Vk}.Take the median interval as the level parameter, and the corresponding evaluation parameter column vector is V':

$$V'=(v_1,v_2,\cdots,v_n)$$

G. Criteria evaluation and establish fuzzy relationship matrix

Different experts give an evaluation of each indicator according to the field of professional knowledge, and quantify the qualitative index, then count the frequency of different level comments of each index that the experts give. So we can get the single factor evaluation matrix R_i of each subset.

H. Single factor evaluation

Take weighting coefficient vector w_i of each single factor that used AHP method and the single factor evaluation matrix R_i synthesis operation:

$$B= w_{i*} R_i$$

I. Multi-factor comprehensive evaluation

Based on Step D, we can obtain comprehensive evaluation matrix of each subset in the factor set U:

$$R=(B_1,B_2,\cdots,B_m)^T$$

So, up layer by layer, until determine the fuzzy comprehensive evaluation results of criteria layer C relative to the final target, and the formula of the fuzzy comprehensive evaluation result is :

$$E=W_c*R_c=(e_1,e_2,\cdots,e_n)$$

E is a membership resulting vector of factor set U, final results of the evaluation is an algebra value that E multiplied by Evaluation parameter column vector V':

$Z=E*V'=(e_1,e_2,\cdots,e_n)*(v_1,v_2,\cdots,v_n)$

Z is a security assessment results throughout the evaluation process.

7. Assessment Process and Implementation

Network terminal security assessment is to identify and analyze the main value of the assets, threats and vulnerabilities. Information assets integrated its confidentiality, integrity, availability three attributes in assignment. According to the assets in the confidentiality, integrity and availability of different degree could be divided into five grades, to different level give different values, the higher the level the greater the value. The final assignment of assets: Assets = f (C, I, A), where f is the function of C, I, A of the information assets mapped to the information assets:

$$Assets = Round\left(\sqrt[3]{C * I * A}\right)$$

The assets are divided into five levels, the higher the level the greater the value, the more important assets. Network terminal security assessment based on the final assignment of assets to determine whether it is an important asset, primarily evaluated for critical assets.

According frequency threats (T) appears to threaten assignment and divided into five grades, vulnerability (V) recognition is for each asset, identify vulnerabilities could be exploited by the threats, and the assignment of vulnerability severity. Vulnerability scanning tools can find a host loophole. Correspond to the same weaknesses in different environments, and its degree of vulnerability is different. From the standpoint of the organization's security policy to determine the degree of vulnerability, the same vulnerability is divided into five levels of threat and vulnerability given different values in different grades, the higher the level the greater the value, the assignment ranges between 1 to 5 numbers. Use the fuzzy comprehensive evaluation method to calculate the ultimate threat, vulnerability assessments. Based on three basic elements of the network terminal security assessment, that is, assets, threats, vulnerabilities final assignment, combined with network terminal security situation assessment model to analyze the results to assess the security situation in the network terminal value, then a comprehensive qualitative analysis, the main assessment algorithms and calculations are as follows:

J. $P=T+V;$

P, T and V represent the Possibility of security events, the threat and vulnerability.

K. $L=P*A$

L, P and A represent the Extent of the loss, Security Event possibility and Assets

L. $S=L*R$

S, L and R represent the Terminal security value, Loss of terminal security incidents and the probability of risk occurrence.

8. Experiments and Results Analysis

This experiment uses the host information security evaluation system designed in this paper to assess a windows xp host which doesn't install anti-virus software and has system vulnerabilities and software applications vulnerabilities. To highlight the comparability of test, combining quantitative assessment models make the following assessment:

Plan 1: According to reference [20], select the 10 top indexes of threatening : C5, C3, C7, C8, C9, C12, C14, C16, C20, C13 and 10 top indexes of vulnerability: C1, C7, C9, C10, C11, C8, C15, C17, C18 and C19 of the original assessment system. Specific indexes weights consult reference [20].

Plan 2: select and normalize the top 10 indexes in table 8, and use them to assess in the original evaluation system. "Threatening" and the corresponding weights are selected is C19,C20,C14,C10,C8, C18, C15 , C16, C9, C12; "Vulnerability" and the corresponding weights are selected isC18, C19,C15,C7,C16,C14,C8,C11,C17,C9, all these shown in Table 9;Assessment result is shown in Table 10.

Table 9. Assessment Index and Weight

Threatening		Vulnerability	
Index	Weight	Index	Weight
C19	0.1843	C18	0.2624
C20	0.1463	C19	0.2624
C14	0.1166	C15	0.1433
C10	0.1055	C7	0.1095
C8	0.0930	C16	0.0581
C18	0.0861	C14	0.0460
C15	0.0777	C8	0.0390
C16	0.0738	C11	0.0366
C9	0.0585	C17	0.0236
C12	0.0582	C9	0.0190

Table 10. Assessment Result

Plan	Asset value	Threatening value	Vulnerability value	Assessment results
Plan 1	3	0.52	0.60	good
Plan 2	3	0.89	0.82	bad

Greater the threatening value and the vulnerability value of the assessment, reflecting the larger threats to the host and the greater chance of vulnerabilities being exploited. Assessment is divided into: "very good", "good", "medium", "bad" and "very bad" five grades. From Table 10, in the same experimental conditions, the assessment result of Plan 1 to the host which doesn't install anti-virus software and has system vulnerabilities and software applications vulnerabilities is obviously unreasonable; the threatening value and vulnerability value in Plan 2 are all bigger than that in Plan 1, also assessment result in Plan 2 is "bad", combined with the actual, Plan 2 more can reflect the actual circumstances of the host. By comparing these two plans we can find that use the improved index system in the host information security assessment system to assess, the assessment result will be more rational, scientific, and more realistic.

9. CONCLUSION

In this paper, we assign index weights scientifically and reasonably by using Delphi and AHP method, although host information security evaluation involves complicated and diversified index, to some extent, making assessments more objective, accurate, and easy to operate. But there are still insufficient, there is some uncertainty in construction of judgment matrix, when random consistency ratio $CR \geq 0.1$, you will need to reconstruct the judgment matrix and the calculation steps will be tedious. So when the judgment matrix can't pass the consistency check how to automatically correct judgment matrix will further discuss.

Acknowledgment

This work is supported by the project supported by the natural science foundation of the education department of Guangdong province: "Cloud services independent building and coordination of research"(2013KJCX0064),and the Key project of natural science foundation of Guangdong province(S2012020011071),and the Ministry of Education and research cooperation projects of Guangdong Province(2012B091000037, 2012B091000041),and the project supported by the natural science foundation of the education department of Guangdong province and science and technology plan projects of Guangzhou(2013J4300058).

References

[1] R. David and G. G. Risk, "A Practical Guide for Deciding what's Really Safe and What's Dangerous in the World around You", Houghton Mifflin Company, New York, **(2002)**.
[2] X. Guo-Ai, C. Xiu-Bo and G. Yan-Hui, "Information Security Management", Beijing: Beijing University of Posts and Telecommunications Press, **(2011)**, pp. 2.
[3] "The 2006 annual Chinese network safety analysis report", http://www.51tiger.com/xxlrl. 2007.4.26.
[4] L. De-Yi, L. Chang-Yi and D. Yi, "Artificial Intelligence with Uncertainty", Journal of Software, vol. 15, no. 11, **(2004)**, pp. 1583-1594.
[5] L. Hui and L. Jie, "Research on network terminal security assessment index system", Computer Engineering and Design, vol. 31, no. 05, **(2010)**, pp. 961-964.
[6] F. Deng-Guo, Z. Yang and Z. Yu-Qing, "Survey of information security risk assessment", Journal of China Institute of Communications, vol. 25, no. 7, **(2004)**, pp. 10-18.
[7] T. Jun, Z. P. Zhu and W. Kanliang, "The Integrating Model of Expert's Opinion Based on Delphi Method", Systems Engineering-Theory & Practice, vol. 24, no. 1, **(2004)**, pp. 57-62.

[8] W. Da-shun, "Information Security Risk Assessment Summary", China Science and Technology Information, no. 14, **(2013)**.
[9] W. Tao and C. Jin-shi, "Research on strategy of information security risk assessment", Modern Electronics Technique, vol. 35, no. 9, **(2012)**.
[10] "GBT20984-2007, Information Security techniques - Information security risk assessment specification", State Administration of Quality Supervision, Inspection and Quarantine, **(2007)**.
[11] L. Hai-hua, Z. Hong-ze and L. Hai-qiang, "Based on Fuzzy Analytic Hierarchy Process in coal mine engineering bid evaluation index weight determination", Coal Technology, vol. 32, no. 02, **(2013)**, pp. 54-56.
[12] L. Hong-Qiang, Q. Yong, Y. Xia, W. Xing-Gang and G. Ren-Wei, "A Study of Weight Coefficient Computing Method Based on AHP", Mechanical Engineer, vol. 06, **(2012)**, pp. 22-25.
[13] W. Xue-Mei, "A Modified Delphi Study on Teacher Competencies for Distance Education in Higher Education", University Education Science, no. 1, **(2012)**.
[14] Z. Dong-Mei, M. Jian-Feng and W. Yue-Sheng, "Model of fuzzy risk assessment of the information system", Journal on Communications, vol. 28, no. 4, **(2007)**, pp. 51-56, 64.
[15] L. Hai-Hua, Z. Hong-Ze and L. Hai-Qiang, "Based on Fuzzy Analytic Hierarchy Process in coal mine engineering bid evaluation index weight determination", Coal Technology, vol. 32, no. 2, pp. 54-56.
[16] W. Shao-Kun, L. Shu-juan and L. Yan, "Confirming weight of voice of the customer in QFD using the method of AHP", Machinery Design & Manufacture, no. 6, **(2005)**, pp. 170-172.
[17] C. Jian-e and J. Tai-Li, "Research on the Weight of Coefficient through Analytic Hierarchy Process", Journal of WUT (Information & Management engineering), vol. 29, no. 1, **(2007)**, pp. 153-156.
[18] X. Long, Q. Yong and L. Qian-mu, "Information security risk assessment based on AHP and fuzzy comprehensive evaluation", Computer Engineering and Applications, vol. 45, no. 22, **(2009)**, pp. 82-85.
[19] H.-J. Zimmermann, "Fuzzy Set Theory and its Applications", Springer, **(1996)**, pp. 47-91.
[20] L. Hui, "Research and Implementation of Network Terminal Security Assessment Technology", Guangzhou: Guangdong University of Technology, **(2010)**.

