2015 The 5th International Workshop on Computer Science and Engineering
doi: 10.18178/wcse.2015.04.116

The Mechanism and Realize Model of Extraction of the Network Security Situation Elements

Guang Kou[1,2,a], Guangming Tang[1,b], Shuo Wang[1,c], Shaoge Yan[1,d]

[1]Zhengzhou Information Science and Technology Institute, Zhengzhou, 450001, China

[2]Science and Technology on Information Assurance Laboratory, Beijing, 100072, China

[a]kg5188@163.com; [b]44287145@qq.com; [c]kg5188@sina.com; [d]kg5188@126.com

Keywords: Network Security, Situational Awareness, element.

Abstract. According to the model of Tim Bass Network Security Situational Awareness, select the situational awareness as the point of study, make full use of the ways of current network security situation element extraction, establishes an index system of multi-level and multi angle to achieve the extraction of the network security situation elements. Studying the network security situation method that based on the index System, put forward the new method to determine the weight of index based on the improved degree of center. Finally, established the system to realize the network security index system configuration, the system would combine with the index weight set, safety index calculation and situation evaluation flexibility and been modified according to the specific needs.

Introduction

Facing the future, information technology has become one of the important symbols to measure a country's comprehensive national strength. Countries compete to occupy the high point of the information technology. Cyberspace war has already start, virus attack, Trojan horse attack, DOS attack, security threats as a sharp sword equally inserted to cyber space [1], threatening the normal development of the society and people's happiness life. Now that the Network Information Security has been risen to the national strategic level, so it is imperative to create a spatial network security shield belonging to our own country .At present, the main space network safety protection technology is IDS (Intrusion Detection System), firewall and virus detection. In a way, it can curb the network attacks effectively. However, because of the different points of focus, these monomers safety equipment is lack of effective cooperation .Therefore, there is great limitations and the final effect is not very ideal [2].

In this context, it attracts many information security experts to research the Network security situation awareness, which used in the space network safety protection.

And it becomes a hot topic in network security field. Network security situational awareness refers to extraction, understand the network security elements which would cause the change of the network and predict the future trend of the NSSA in the large-scale computing network environment.

In the study of network security situation awareness, Tim Bass put forward the concept of network security situation awareness in 1999 firstly, and in 2000 put forward the data collection based on the distributed multi-sensor IDS and get the result of calculation and evaluation of the network security situation. Through the methods of data mining and data fusion, analysis and processing the IDS data, it can evaluate the safety of the target Network [3]. Jason Shifflet added the ontology and the related theory into the research of network security situation awareness; then put forward the structure of the network security situation awareness based on the modular framework [4].

Network security situational awareness asks for detection of the large-scale network security situation from the overall and comprehensive view. Its core idea is to extract the network security situation elements, calculate the current network situation value based on the reasonable situation evaluation method, finally get the current situation value of the target network through the original data such as network security data, flow information, system log, which obtained from network security equipment.

Therefore, extraction of the security situation of the network is a key step and lower base to realize the network security situational awareness. However, the current extraction of the network security situation elements just stays in the initial stage of theoretical research. There is no standard element system formed. So it is necessary to research the principle of situation element extraction

This paper is mainly about the research of the characteristics of network security events, which using historical data effectively to make full use of the current network security situation element extraction and establish an index system of multi-level and multi-angle. Based on above, we study the network security situation evaluation method based on the index system. Finally, we can establish configuration system of network security index hierarchy. It combines the system of safety index calculation and situation evaluation with the index weight set, which has certain flexibility.

Principle of situation element extraction

Tim Bass model. Tim Bass in 1999 applied the JDL model to the field of network security situation awareness for the first time. He put forward a Network security situation awareness framework, divided into five layers, including data refinement, attack object recognition, situation assessment, threat assessment and resource management. The five layers from bottom to top, show the whole process of "data --information -- knowledge". As shown in figure 1:

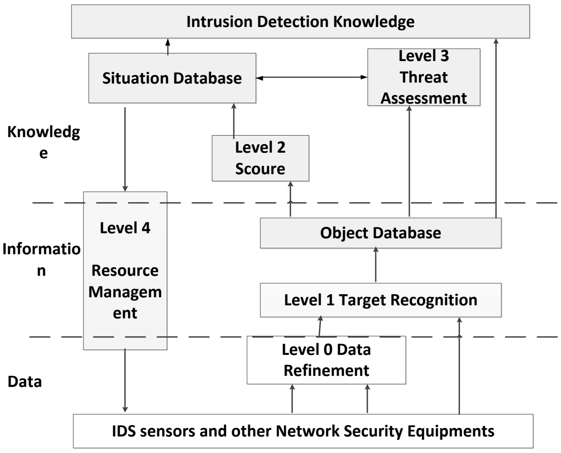
Intrusion Detection Knowledge
Situation Database
Level 3 Threat Assessment
Knowledge
Level 2 Scoure
Level 4 Resource Management
Information
Object Database
Level 1 Target Recognition
Level 0 Data Refinement
Data
IDS sensors and other Network Security Equipments

Fig 1. Tim Bass Intrusion Detection Data Fusion Framework

Among them, the zero level is responsible for obtaining, filtering and correcting the original data from all kinds of network security equipment ; the first level will be responsible for data standardization and parallel connection correlation and ultimately giving their weight value according to the relative importance of ; the second is responsible for the abstract and evaluation of the current security situation; the third is responsible for the assessment of the threats and possible effect based on the current situation.

The theoretical basis of network security situation element extraction. As a key step in Network security situation element extraction of situation awareness, it is an important technology of network security situational assessment. Considering the different types of the network security devices and the different emphasis of the equipment, the original data obtained from the equipment is various in formats. Therefore, it is significant to establish a network security situation element index system, which is comprehensive, full of extensive contents and scientific and reasonable.

The establishment of the index system should be closely based on the topological structure of network and the actual security needs. Besides, we should understand the relationship between these indexes and grasp the overall and individual on index system.

The factors that influence the network security situation are diverse. And the relationship between various elements is difficult to understand. Therefore, it is a hard work to establish a network security situation evaluation index system, which should follow the following four principles:

- The full and independent principle: Based on the comprehensive understanding of elements which will make the network security situation to change, we should analysis the relative independence of each index.
- Systematic and hierarchical principle: There are many factors of influence of network security situation and the index system of network security element is compared commonly big. We should consider the index system hierarchically to make clear the relationship between each target and to make sure that the whole index system is scientific and reasonable.
- The scientific principle: We should select a representative and specific indicators tightly on the basis of network security incidents and system requirements. In addition, the index calculation method, data acquisition processing method, the determination of index weight value and so on should have scientific basis.
- The feasibility principle: The establishment of index system should fully consider the data collection process, fully considering the characteristics of various security tools, convenient in data acquisition, format conversion and redundant processing have a choice on the basis of selection of appropriate indicators.

The extraction method in levels of situational factors

This article describes the three relatively independent of the network security situation in aspects of characteristics referring to the achievements in the field of network security situation, which comprehensive reasonably reflect the security situation of the target network. Characteristics of the three aspects respectively: network survivability index, the network vulnerability index and network threat index. As a result, the three aspects of the corresponding security index for network survivability index, the index of network vulnerability index and threatening. The composite index of the network security situation can be described by a triple:

$$S=<C, V, T>$$

Among them, S is the network security situational composite index;

- C is the network survivability index, calculated by the network survivability index, mainly focus on the description in the target network protection and network security events may withstand the attack ability.
- V is the network vulnerability index, calculated by the network vulnerability index focus on the description of security loophole in the network itself, mainly through the holes from the safety equipment information, in accordance with the standard method
- for evaluating the network vulnerability index. It is concluded that the network vulnerability index.

- T is the network threat index, calculated by the network threat index, focusing on the description of network security incident has threated to network caused or may cause, mainly through the alarm logs provide known attacks, malicious code and the number of frequency or unknown attacks related mathematical model is established to calculate.

The extraction and quantitative of network survivability indicators. Network survivability index mainly reflects the running state of the network, we can get it by calculating various nodes host survivability index based on the importance of the host node in the network. Therefore, the network survivability index is mainly composed of survivability index nodes host and network topology structure decision [5].

Host survivability index is mainly composed of host index in two aspects of the decision. Among them, the index is mainly composed of nodes host assets value, operating system type and version, with service status information by decision; Average traffic flow index is mainly composed of nodes of the host, peak flow rate and bandwidth utilization network traffic information decision. Therefore, the network survivability index mainly composed of the following:

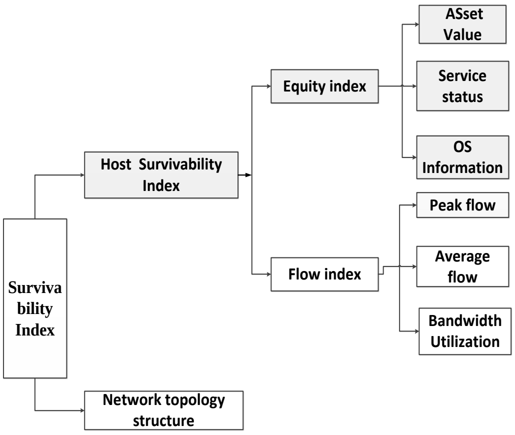

Fig 2. Network Survivability Index of Figure

The extraction and quantitative of network vulnerability indicators. This article mainly refers to the vulnerability index loophole harm each node of the host. And host node loophole harm mainly decided by safety measures jointly with the host vulnerability. Network vulnerability index, therefore, mainly through calculating various nodes host vulnerability index, and considering the weights of each node in the network host, the network vulnerability index.

The extraction and quantitative of network threat indicators. Network threat index is based on a certain cycle target network on the various security incidents to quantify the network threat level assessment, it mainly reflects the various network events on the degree of threat target network. Network threat index data mainly is from open source network security tools Snort that is able to collect all kinds of security incidents. As the typical network attack classification is known as the basic principle, research analyzes the characteristics of the common network security attacks, network security events can be divided into nine categories followed by a Trojan, botnets, viruses, worms, denial of service, tamper with the web page, hang horse, domain name hijacking and other security events. Network threat index system was established.

A model based on calculating index value

Set the index weight method based on entropy weight method. In multi-level index fusion process, the index weight set in each layer of network security situation directly affects the result, finally decides the whole network security situation index. Setting the index weight is mainly composed of subjective values. The method is too dependent on the expert's subjective judgment without using the original data in the network, so it is not very scientific. Objective methods, such as variation coefficient method and the entropy weight method can be calculated in the network situation occurs with the actual situation. Therefore, this article combine subjective and objective weight determination method, on the basis of the entropy weight method, through expert in combination with the specific situation of network to carry on the certain weighting adjustment, make full use of the advantages of two methods, accurate and reasonable to determine the index weight of various levels.

To determine the number of network vulnerability loopholes, difficulty of attack, attack methods and protection expense of five indicators weight, for example, the index weight determining process as follows:

- Step1: Take network vulnerability in the table in the database before the k line, structural vulnerability sample matrix

$$X = \begin{pmatrix} A_{11} & A_{12} & \cdots & A_{15} \\ A_{21} & A_{22} & \cdots & A_{25} \\ \cdots & \cdots & \cdots & \cdots \\ A_{k1} & A_{k2} & \cdots & A_{k5} \end{pmatrix}$$

- Step2: Numerical normalization processing various indicators. Normalization method is as follows:

$$a_{ij} = A_{ij} / \sum_{i=1}^{k} A_{ij}, i = 1, 2, ..., k, j = 1, 2, ...5$$

- Step3: Each index of the entropy value is calculated by the following formula.

$$H_j = -\frac{1}{\ln k} \sum_{i=1}^{k} a_{ij} \ln a_{ij}, j = 1, 2, ..., 5$$

- Step4: According to the following formula index reflect the differences between the entropy can be converted to a weight, get the final index weights.

$$w_j = \frac{1 - H_j}{k - \sum_{j=1}^{k} H_j}, j = 1, 2, ..., 5$$

- Step5: By experts through the subjective method (such as analytic hierarchy process), respectively, to determine the five indicators weight as follows:

$$w_1 '、w_2 '、w_3 '、w_4 '、w_5 ' .$$

- Step6: Calculate the final five indicators weight as follows:

$$w_j = \frac{w_j + w_j '}{2}, j = 1, 2...5$$

The improved host weight setting method Based on the degree of center node. This paper has established the "index - service - host - target network nodes" hierarchical network security situation index calculation model, on the basis of the target network topology structure, the weights for each node host is critical. We designed the topology of the target network, based on the improved degree of center node host weight setting method, a reasonable solution to determine the weighing values for the target network nodes in a host of problems [6].

Centricity principle: degrees centricity is to describe the size of a node control index and the higher the degree of central node, it node has the more ties in the network and it is more important in the target network, finally it has the greater corresponding weights. Below with a simple network topology based on the center of the degree of node host weight setting method. Target network topology chart abstraction as shown in figure 3:

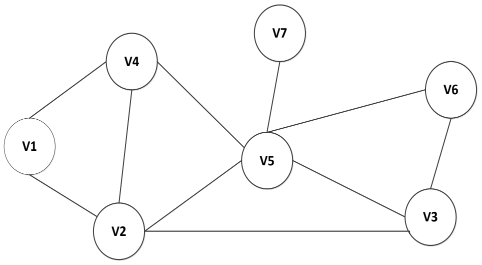

Fig 3.   Simple Network Topology Structure

Degree of center shows that the host which gets a direct link between hosts the more, the status of the node in the target host network is more important. Degree of centricity is a simple and effective method of determining the host network node weights. However, degree of center only considered the direct link between a node and other nodes, did not consider the node from the perspective of the overall host and the indirect contact of the whole network. Such as a node and other nodes host has directly related, but is the isolated nodes, the nodes in this case, the degree of centricity there are unreasonable places. In order to avoid this situation, in this paper, on the basis of the degree of centricity, we consider the experience from the experts about the node weight, make it more accurate and reasonable. To improve the degree of central host weight method for determining the following process:

- Step1: According to the figure 3 the network topology structure, we construct the adjacency matrix.

$$A = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

- Step2: Calculate degree of each node.

$$cD(i) = \sum_{j=1}^{j=7} A_{ij}, i = 1, 2...7$$

- Step3: Standardization degree of centricity, degree of centricity are within the scope of the [0, 1].

$$CD(i) = \frac{cD(i)}{7}, i = 1, 2...7$$

- Step4: The expert classification method based on three kinds of key nodes of the host, through the subjective method (such as analytic hierarchy process), respectively, to determine the seven node weights of host, respectively.

$$CD(1)'、CD(2)'、CD(3)'、CD(4)'、CD(5)'、CD(6)'、CD(7)'$$

- Step5: Calculate the final seven node weights of host are:

$$W_j = \frac{CD(j) + CD(J)'}{2}, j = 1, 2...7$$

The three layer network security situation assessment model based on the fusion of the indexs. The establishment of the index system of network security situational factors laid a foundation for network security situation assessment [7]. Through a variety of network security equipment to obtain the raw data and information, according to the requirements of multi-level index system of network security situation, establish a standardized network security situation index database, combined with the weight of each nodes, really achieve the goal from the node to the whole network of situation assessment [8]. The hierarchical assessment diagram is shown as figure 4.

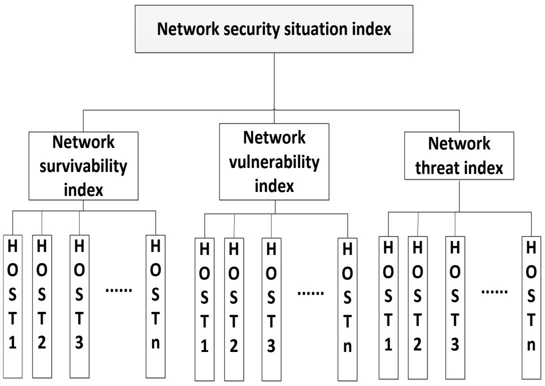
Network security situation index
Network survivability index
Network vulnerability index
Network threat index
HOST1
HOST2
HOST3
......
HOSTn

Fig 4. Hierarchical Network Security Situation Assessment Structure

In the hierarchical situation assessment index system, this paper adopts weighted average method to the next layer together become a layer index. The following type:

$$f(w_1 * x_1, ... w_n * x_n) = \sum_{i=1}^{n} w_i * x_i, \sum_{i=1}^{n} w_i = 1$$

Situational factor extraction system design and implementation

Extraction of multi-layer network security situational factors on the basis of the above mechanism, this paper designed the index system of network security situation assessment system [9]. The system is mainly divided into data parameters configuration module, index module and situational result display module. Among them, the data parameters configuration module is mainly responsible for the raw data unified classification and configuration of index weight; Index calculation module is mainly to the aggregation of each index; Situational results display module is mainly to the current network situation status display, to the network administrator to intuitive display. The whole network security situation assessment system structure diagram as shown in figure 5

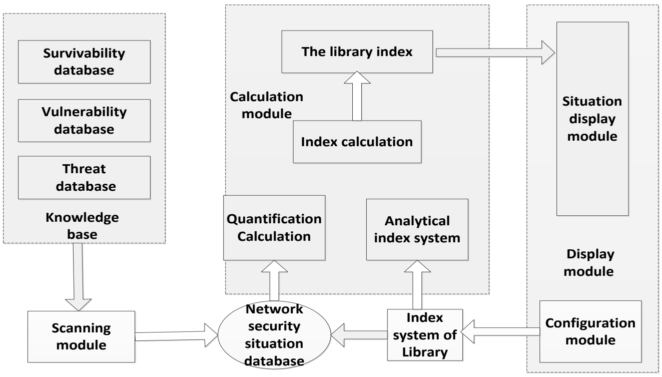

Fig 5. Network Security Situation Assessment System Structure

The conclusion

With situational awareness as the breakthrough point, this paper mainly studied the extraction methods of situational factors, fully referring to the methods currently used to extract the situational factors, establishes a set of multi-angle multi-level index system of network security, which realizes extraction of the network security situational factors. Finally, we set up an index system of network security configuration system, which is set up to work with the index weight, safety index calculation and combination of situation assessment with the certain flexibility. Overall, the paper work basically has the following several aspects:

- The relevant technology of the further study of the network security situational awareness and theoretical connotation, overall understanding of the research methods and ideas.
- The establishment of a multi-level index system of network security situation, the implementation of the extraction of situational factors [10].
- To study the situation assessment method based on the index system, puts forward the index weight and node hosts a new method for determining weights.
- To establish the network security situation assessment system, and completed the part of work

References

[1] ZHOU Changjian, SI Zhenyu, XING Jinge, LIU Haibo, “Study on cyberspace situation awareness modeling method based on Deep Learning”, Journal of Northeast Agricultural University, 44(5), pp. 144-149, 2013.5

[2] Antoniou J, Koukoutsidis I, Jaho E, et al. Access network synthesis game in next generation networks. Computer Networks, 2009, 53(15): 2716-2726P

[3] Tim Bass. Intrusion Detection Systems and Multi-sensor Data Fusion:Creating Cyberspace Situational Awareness[J]. Communications of the ACM， 2000，43(4): 99-105.

[4] Yegneswaran V, Barford P， Paxson V. Using honeynets for internet situational awareness[C]. Maryland: Proceedings of the 4th Workshop on Hot Topics in Networks，2005:762.

[5] XI Rongrong, YUN Xiaohun, JIN Shuyuan, ZHANG Yongzheng, “Research survey of network security situation awareness”, Journal of Computer Applications, 2012,32(1), pp. 1-4,59, 2012-1-1kmc

[6] Nagios-Port and Service Detection[Z].http://www.nagios.org，2009

[7] CAO Kunlun, Liu Jianming, XU Ruzhi, WANG Yufei, LI Yikang, “A Hybrid Security Situation Prediction Model for Information Network Based on Support Vector Machine and Particle Swarm Optimization”, Power System Technology, Vol. 35 No. 4, 2011.4, pp. 176-182.

[8] Ying Z, Qiang Z, and Zhenghu G. Research and Implementation of Network Transmission Situation Awareness. Proceedings of 2009 WRI World Congress on Computer Science and Information Engineering, CSIE. Piscataway, NJ, USA: IEEE, 2009, 10-14.

[9] Peng L. Sushil J, and Vipin S. Cyber Situational Awareness. Springer, 2009,15-24.

[10] Lee C, Fapojuwo O. Analysis and modeling of a campus wireless network TCP/IP traffic. Computer Networks, 2009, 53(15): 2674-2687P