Chapter 104
Using Network Security Index System to Evaluate Network Security

Jian-feng Zhang, Fei Liu, Li-ming Zheng, Yan Jia and Peng Zou

Abstract Fast Internet growth and increase in number of network attack make network security essential in recent years. This paper proposes a novel approach to evaluate the network security situation using Network Security Index System (NSIS). The NSIS is composed of Foundational Index, Vulnerable Index, Risk Index and Comprehensive Index. Each index focuses on some specific aspect of network security, and the detailed methods of how to calculate the index are given. Experimental results show that the NSIS can assess the network security situation objectively and comprehensively.

Keywords Network security index system · Network security · Situation evaluation · Multi-criteria decision making

104.1 Introduction

With the development of human society, the network has been integrated into all aspects of people's lives. Along with the convenience, network also brings many security problems, the global Internet attack happens frequently, and makes a highly severe impact on the global network. At the same time, in our county a variety of network security incidents have become inevitable, such as network economic crimes, large-scale network attacks, network stolen and so on. All these have became a constraint to our economic development, especially became the key

J. Zhang (✉) · F. Liu · L. Zheng · Y. Jia
College of Computer, National University of Defense Technology,
Changsha, Hunan, China
e-mail: jfzhang@nudt.edu.cn

P. Zou
Academy of Equipment Command and Technology,
Beijing, China

E. Qi et al. (eds.), *The 19th International Conference on Industrial Engineering and Engineering Management*, DOI: 10.1007/978-3-642-38433-2_104,

factors that threaten social stability and national security. So that how to evaluate the situation of network security comprehensively and objectively has became a challenging issue. In this paper we use Network Security Index System (NSIS) to solve this problem perfectly. NSIS choose the objective and subjective attributions to quantify and compute network security situation, and it is designed to assist managers to discover the main elements that influence network security. So the managers can focus on the primary to defense the attack and protect the network.

NSIS is implemented in our system named YHSAS, this system is to analyze and predict the larger-scale network security situation. In this system, sensors like IDS, firewall, et al. are distributed deployed to detect and monitor the abnormal events in the network, all the threaten events generated by these sensors are send to server to be analyzed. Base on these information NSIS is used to evaluate the network situation in our system.

The rest of this paper is organized as follows. In Sect. 104.2, related theories of network security index system are explained. Section 104.3 explains the design of this system. Section 104.4 presents an experimental evaluation. Finally, the conclusion is given in sect. 104.5.

104.2 Related Works

Tim Bass (2000) proposes a distributed intrusion detection system using multi-sensor data to assess computer network security through data fusion and data mining methods. Meanwhile, Han et al. (2004) use qualitative analysis methods to assess network vulnerability. Kamara et al. (2003) propose Internet firewall vulnerability assessment, Hariri et al. (2003) propose a large-scale network attack assessment using quantitative analysis, The OCTAVE (Alberts et al. 2003) and ISO 13335 (2001) standards combined qualitative and quantitative methods to evaluate network security.

Shi and Zhuang (2007) propose a model of network security risk assessment system both with quantitative evaluation theory, and risk is defined as the product of asset, threat and vulnerability. Chen Xiuzhen et al. (2004) develop a quantitative hierarchical threat evaluation model to evaluate security threat status of a computer network system, the computational method in this model is based on the structure of the network and it focus on the threat situation. The threat indexes of services, hosts and local networks are calculated by weighting the importance of services and hosts. Yong and Yifeng (2009) proposes a network security situational awareness model based on log audit and performance correlation algorithm. The value of network security situation is computed using service information.

The existing researches on evaluate network security situation are mainly focus on a single security attribute such as threat, vulnerability and so on, lack of the evaluation on integrated network security situation. This paper prose a novel approach that use NSIS to evaluate the network security situation objectively and comprehensively.

104.3 Design of Network Security Index System

In order to reasonably assess the situation of network security, the index of network security must satisfy the following properties:

1) *Objectivity:* The indexes choose from network information should be representative and authentic. Meanwhile, these indexes can also indicate the network security comprehensively.
2) *Computability:* As can be applied to practice, the raw data used for Network Security Index System could be convenient to quantify and calculate, and the method of quantification and calculation must be reasonable.
3) *Sensitivity:* The values of each index in Network Security Index System should be changed sensitively when network security changes. And the trend of this change must be consistent with the network situation.

Based on the above characteristics, this paper designs our own Network Security Index System. As shown in Fig. 104.1, the NSIS is composed of Foundational Index, Vulnerable Index, Risk index and Comprehensive Index. All these indexes are introduced in following sections, the sections is organized by three parts: firstly, the attributes are selected to each index; Then the methods of quantify these attributes are given; and finally based on the qualified values, we use the aggregation algorithms to calculate the indexes. The functions in this paper are implemented in our YHSAS, and can also be replaced by others in different situation.

In order to indicate the relationship between the situation and the values that calculated by NSIS, we provide a rating from 1 to 5 using the scale in Table 104.1. Values in this table are the upper bound of each situation.

104.3.1 Foundational Index

Foundational Index is mainly focus on the capability of the hardware and the situation of the services, and is used to reflect whether the devices and the services work well. The resources of hardware and software are consumed when the network is under attacking. In this situation the utilization rate of CPU and Memory of these equipments will be high away from the normal level, and the network flow will increase seriously. So the Foundational Index is assessed by the properties as follows:

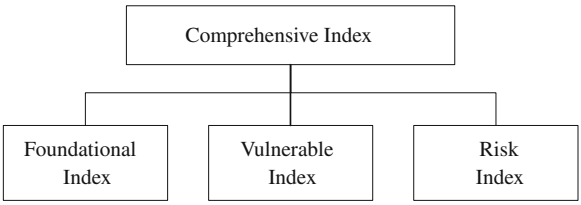

Fig. 104.1 Structure of network security index system

Table 104.1 Relationship between security situation and index values

Value	Situation
1	The situation of the network is very good. All the network devices are performing very well, almost no vulnerabilities and attacks are existed in the network
2	The situation of the netwok is good. All the network devices are working well, few vulnerabilities and attacks are existed in the network. The impact of all these vulnerabilities and attacks can be ignored
3	The situation of the network is medium. Some network devices are working near its threshold, some vulnerabilities and attacks are existed in the network. These vulnerabilities and attacks impact the security of the network
4	The situation of the network is dangerous. Some network devices are overloading. A few vulnerabilities and attacks are existed in the network. These vulnerabilities are serious, and the existed attacks used these vulnerabilities make an impact on the confidentially, integrity and availability of the network
5	The situation of the network is severe. Many network devices are severe overloading. Many vulnerabilities and attacks are existed in the network. These vulnerabilities are severe, and the existed attacks used these vulnerabilities make a severe impact on the confidentially, integrity and availability of the network

1) *Peak flow:* Peak flow is the max flow that received by a host and device in the fixed time period. Max flow can show the most threaten situation of the hosts and devices confronted.
2) *Bandwidth utilization:* High bandwidth utilization by one or more computers or network devices, either transient or sustained, which degrades network performance and effectively prevents or inhibits legitimate activities.
3) *CPU utilization:* CPU utilization is important to measure the performance of a host or device, and the higher the percentage of the CPU used, the less power the CPU can devote to other tasks. Here CPU utilization is considered as average percentage of the CPU used in the fixed time period.
4) *Memory utilization:* As the CPU utilization, we consider the memory utilization to asses the real-time performance of the devices. Many denials of services attacks have the aim to exhaust the CPU and memory resources, so this property is as important as CPU utilization to assess the running performance of a host or device.

Based on the defined the properties, the Foundational Index is calculated by the following steps:

Firstly, we use the overload of each property to qualify the severe scale in every time period. Suppose that a network has N nodes, and the overload of the property is defined as in

$$o_{ji} = \begin{cases} \dfrac{l_{ji}}{L_{ji}}, if l_{ji} > L_{ji} \\ 1 \end{cases} \tag{104.1}$$

where $i = 1, 2, 3, 4$ respectively stands for peak flow, bandwidth utilization, CPU utilization and memory utilization, j is the node number from 1 to N, L_{ji} represents the threshold for property i at node j, and its values are meeting specific statistical laws in a certain time period, l_{ji} represents the actual value for property i at node j. o_{ji} is the overload of the property i at node j.

Secondly, the o is normalized to a severity rating from 1 to 5. Let s_{ji} be the normalized result of O_{ji}. S is assigned as follows: if $o = 1$ then $s = 1$, if $1 < o \leq 1.25$ then $s = 2$, if $1.25 < o \leq 2$ then $s = 3$, if $2 < o \leq 3$ then $s = 4$and if $o > 3$ then $s = 5$. We can also define the different transfer function to normalize the overload according to the real situation.

Thirdly, we calculate the Foundational Index for every node as in

$$I_j = f(o_{j1}, o_{j2}, o_{j3}, o_{j4}) = \underset{1 \leq i \leq 4}{Max}(o_{ji}) \tag{104.2}$$

Finally, based on the Foundational Index of each node, we get the Foundational Index as in

$$I_F = f(o_1, o_2, \cdots o_N) = \sum\nolimits_{j=1}^{N} u_j o_j \tag{104.3}$$

where u_j is the weight of the node in the network, and$\sum_{j=1}^{N} u_j = 1$. The function used to calculate the Foundational Index can be different in different situations.

104.3.2 Vulnerable Index

In computer security, vulnerability is a weakness which allows an attacker to reduce a system's information assurance. If a computer or system has much vulnerability, it may be easy to be exploited, and the asset on it may confront serious threat, so it is important to assess the harmful of the vulnerabilities exist in the network. In this paper we use Vulnerable Index to measure the self-security of equipment without any external attacks. We assess the vulnerabilities by three important attributes:

(1) *Asset:* In ISO/IEC (2001), anything that has value to the organization is defined as asset. In network system, we mainly defined asset as hardware, software, information. Vulnerabilities can be related to properties or attributes of the asset. The vulnerability of some import asset has higher threat, once this vulnerability is exploited, it may bring wide influence.

We use the definition of asset in international standards ISO/IEC 13335 (2001) to quantify the importance of network equipment, we assign 1 to "Negligible" level, 2 to "Low" level, 3 to "Medium" level, 4 to "High" level and 5 to "Critical" level. To complete this procedure, firstly we should identity the assets on each host and network device, then the values should be assigned to these assets

by owners or users, and finally the asset of each host or network device is given by all assets on it.

(2) *Inherent threaten:* This attribute is used to consider what you can obtain through the vulnerability. For example, the vulnerability to get root privileges may be greater threat than the vulnerability to misuse of resources.

The inherent threaten of vulnerability is defined as in Anderson (2004), "Hole", "Warning" and "Note" are used to describe the threaten of vulnerability, we assign 1 to "Note" level, 3 to "Warning" level and 5 to "Hole" level.

(3) *Usability:* Usability is used to show that how easily the vulnerability may be exploited. Some vulnerability can only be exploited by experts, but some can be implemented by script kiddies (Rubin 2002).

The usability of vulnerability is defined as follows: "Easy" give a description of the vulnerability that can be exploited by script kiddies, and value 5 is assigned to this level; "Possible" means that the vulnerability may be exploited by some skillful persons, value 3 is assigned to this level; Vulnerability with "Difficult" level shows that the vulnerability can only be exploited by experts.

The Vulnerable Index is calculated by two steps:

Firstly we evaluate the vulnerabilities on every host or network device. Vulnerability on a host or device may be exploited by each other. For example, by some weak vulnerability attackers can only obtain remote access privilege, but based on this remote privilege, attackers may get root privileges by other vulnerability. So we consider each host and device as a whole to be evaluated. Suppose that there are N vulnerabilities on a host, let M_i be the Vulnerable Index of this host, and M_i can be expressed as in

$$\mathrm{M}_i = f(T_j, U_j) = T_j * U_j/5 \tag{104.4}$$

where i is used to identity different host or network device in the network, T_j is the inherent threaten value of specific vulnerability j and U_j is the usability value of specific vulnerability j.

After getting all values of Vulnerability Index for each host and network device, we use aggressive algorithm to get the Vulnerable Index for this network as:

$$\mathrm{I}_V = f(M_i, A_i) = Max(u_1 M_i + u_2 A_i) \tag{104.5}$$

where i is used to identity different host in specific network, A_i is the asset value of the host, u_1, u_2 are the weight of M_i andA_i, the max value of all the host is specified to Vulnerable Index of the network.

104.3.3 Risk Index

Risk is defined as a function of the values of the assets, the likelihood of threats, the ease of exploitation of the vulnerabilities by the identified threats, and any existing or planned safe guards (ISO/IEC 2001).

In this paper, we use Risk Index to evaluate the impact of the network attacks. Here the network attacks exist as alarms, and the alarms are generated from the threaten events collected by IDS and other security tools using correlate algorithm. In order to evaluate the situation of network attack, we cluster the alarms by the attack category, destination IP and the using vulnerability. After that we consider the attributes of these clusters as follows:

1) *Reliability:* Reliability is used to assess the likelihood of threats and the ease of exploitation of vulnerabilities by the identified threats. An alarm may have a high reliability if the vulnerability used by the threat exists truly at the target host, otherwise the reliability may be low.

The value of reliability is initialized according to the performance of each security tools, and then the value is modified in our YHSAS by correlation rules. In this paper we quantify the reliability as the number from 1 to 5, the bigger the more reliable.

2) *Scale:* We use scale to express the size of cluster. This attribute is very important to evaluate the impact of attack, for example, DDOS attack with high packet sending rate is more threat than the one with low packet sending rate. The scale is normalized as in

$$S = \begin{cases} 1, & x > MaxValue \\ \frac{x - MinValue}{MaxValue - MinValue}, & MinValue \le x \le MaxValue \\ 0, & x < MaxValue \end{cases} \tag{104.6}$$

Where x is the number of alarms in each cluster, *MaxValue* and *MinValue* are the biggest and smallest values in history, of course these two values can also specific by users.

3) *Asset:* Asset here is the same meaning as the asset in Vulnerable Index.
4) *Threatening:* Threatening is the self-attribute of an attack, some attacks such as DDOS is threaten to the availability of host or service, some attacks such as worms may be destructed to system. So we define the threatening as four levels: “Disclosure”, “Modification”, “Non-availability”, and “Destruction”. “Disclosure” is used to describe the attacks that have the aim to steal users’ information, such as port scans. “Modification” describes the attacks that destroy data integrity, such as some virus. “Non-availability” means that the attacks ruin the availability of the data like DDOS. The severe threaten is

expressed as "Destruction", meaning that the system is ruined by this attack, such as CIH (Ren 2001).

The level of all the attacks should be defined by experts, and the definition may be different in different application scene. In this paper we assign 2 to "Disclosure", 3 to "Modification", 4 to "Non-availability", and 5 to "Destruction".

After discussing the risk attributions, we use these attributions to assess the risk of the network situation. Let I_R be the Risk Index, I_R can be expressed as in

$$I_R = f(S_i, A_i, R_i, T_i) = u_1 S_i + u_2 A_i + u_3 R_i + u_4 T_i \tag{104.7}$$

Where we suppose that C is the number of clusters, $i = 1, 2, \cdots C$, To cluster i, N_i is the scale of this cluster, A_i is the asset of destination IP, R_i is the reliability of the alarm, T_i is the inherent risk about this alarm, u is the weight of the attributes, and $\sum u = 1$.

104.3.4 Comprehensive Index

The Comprehensive Index is decided by Foundational Index, Vulnerable Index and Risk index. It is used to reflect the whole situation of the network. The Comprehensive Index is calculated as

$$I_c = u_F * I_F + u_V * I_V + u_R * I_R \tag{104.8}$$

where u is the weight for each index, and $\sum u = 1$, Its value can be assigned according to the role of corresponding index in the whole network.

104.4 Experimental Results

104.4.1 Introduce the Experimental Environment

We evaluate the effectiveness of the NSIS in the real environment. Before the experiment, a brief introduction about the environment is statement. The NSIS is deployed in an enterprise network as shown in Fig. 104.2. This enterprise network contains fifty PCs, twenty servers and a core switch, Snort (Roesch and Green 2003) is used as an IDS tool, Ntop (Pras 2000) is used to monitor the network flow and vulnerabilities are collected by Anderson (2004). Our NSIS is implemented in YHSAS server, and the web server is used to show the results of NSIS to users. All the values in NSIS are calculated every six seconds in our system.

The statement of YHSAS is initialized as follows: we sign 2 as the asset to all PCs, 3 to the servers and 5 to the switch. The optimal parameters of all equations in this paper are determined by training. Suppose all the devices have no severe vulnerabilities, and not be under attacking.

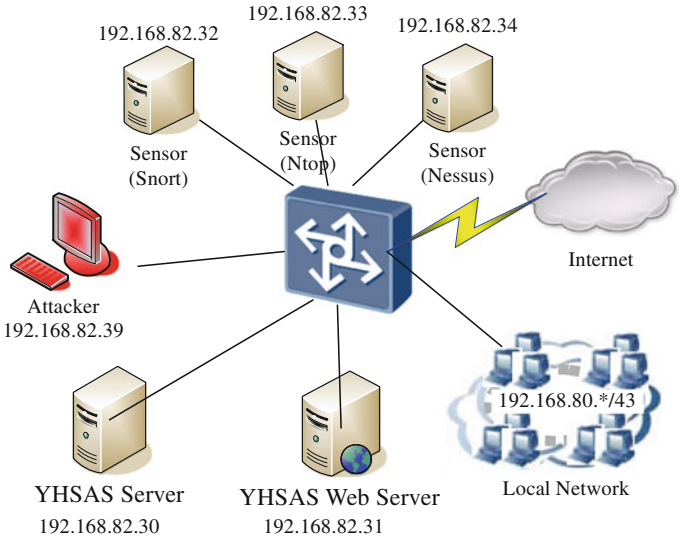

Fig. 104.2 Experiment environment

104.4.2 Validate the NSIS by Simulation

In this experiment, we simulate a DDOS attack to validate whether the values of index can reflect the situation of the network when the network is under attacking. In this scene, we launch the DDOS attack using TFN2K (Center 1999) to attack the server in our environment. The TFN2K daemons are capable of a larger variety of attacks, including ICMP flooding, SYN flooding, and smurf attacks. In our typical scenario, we use ICMP flooding to consume the resource at the target server. This attack last for twenty minutes. In the first 10 min, we increase the attack intensity from 10 per min to 300 per min, and in next 10 min, we decrease the attack intensity until to stop the attack.

Figure 104.3 shows all the index values in NSIS from the beginning of attack to the end, and the values are calculated every 6 s. We can find that the value of Foundational Index increases suddenly after 8 min which illustrates that the performance of the victim may meet its bottleneck when the attack intensity achieves 250 per min. When the intensity of DDOS decreases to 150 per min, the Foundational Index decreases suddenly. The values of Risk Index increase and decrease along with the attack intensity. Because of unchanged vulnerabilities in network, Vulnerable Index is also unchanged during the times.

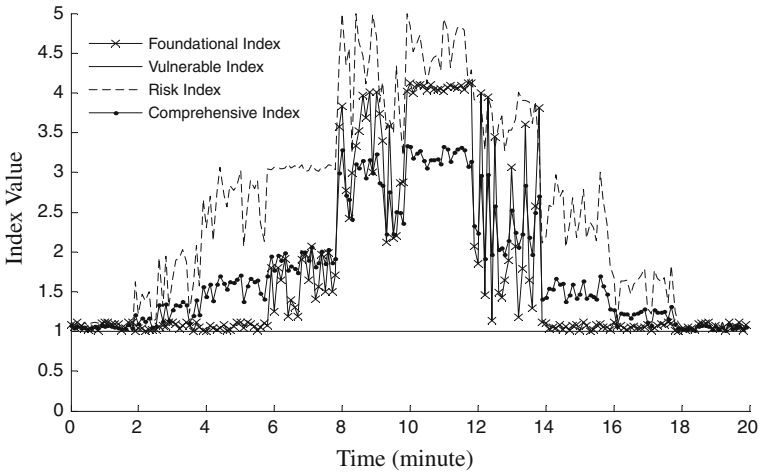

Fig. 104.3 The index curve under simulated attack

104.4.3 Monitor the Situation by NSIS

This experiment is to illuminate the usability of our NSIS. According the curve of NSIS we can get the security situation of the monitored network. Our system is deployed at enterprise network and running all the times. On April 6 we find that the curve of Risk Index is ascending rapidly as shown in Fig. 104.4.

Figure 104.4 shows that the situation of this network becomes severely, the network may be under attacking. After anglicizing the alarm data, we find that a

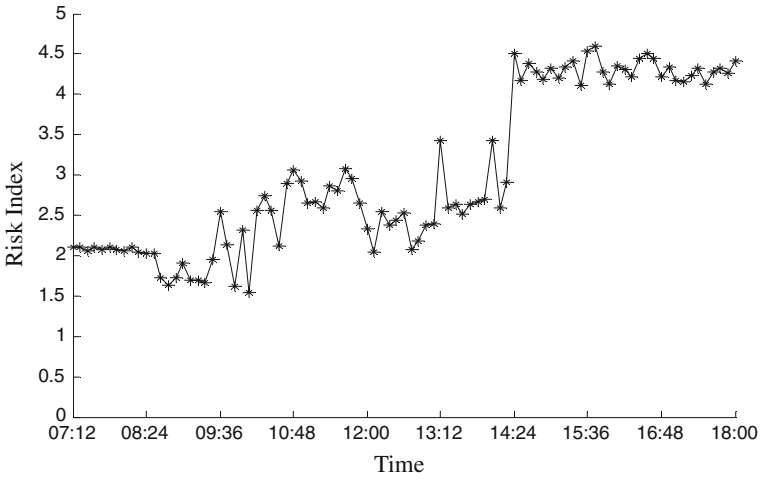

Fig. 104.4 The Risk Index on April 6

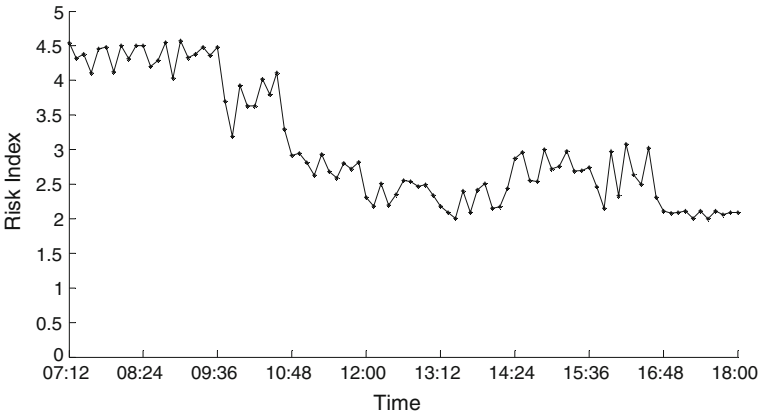

Fig. 104.5 The risk index on April 10

host in this enterprise is exploited, and it uses vulnerability named CVE-2001-0876 (http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2001-0876) to infect other computers. These abnormal behaviors are detected by IDS and some other tools in our system. This type of attack is named as "MISC UPnP malformed advertisement" by snort. After taking some security measures, the Risk Index returns to normal level as shown in Fig. 104.5.

104.5 Conclusion

In this paper, Network Security Index System is proposed to assess the network security situation. The NSIS is composed of Foundational Index, Vulnerable Index, Risk Index and Comprehensive Index, and used to evaluate the network security situation comprehensively and objectively. Then the detailed methods of how to calculate the indexes are given. The experiments illuminate that the NSIS can reflect the situation of the network security reasonability.

Acknowledgments This paper is supported by the National 863 Program of China (2010AA012505, 2011AA010702, 2012AA01A401, and 2012AA01A402), National Natural Science Foundation of China (60933005), National Science Technology Support Plan Program of China (2012BAH38B04) and National 242 Information Security plan of China (2011A010). We gratefully acknowledge the efforts of all team members in our project. Finally we would like to thank the reviewers for their insightful comments which significantly improved this paper.

References

Alberts C, Dorofee A, Stevens J, Woody C (2003) Introduction to the OCTAVE(R) approach. Carnegie Mellon University, Pittsburgh

Anderson H (2004) Nessus, part 3: analysing reports. Book Nessus, part 3: analysing reports. Series Nessus, part 3: Analysing reports

Bass T (2000) Intrusion detection systems and multisensor data fusion. Commun ACM 43(4):99–105

Center C (1999) CERT Advisory CA-1999-17 Denial-Of-Service Tools. Book CERT Advisory CA-1999-17 Denial-Of-Service Tools, Series CERT Advisory CA-1999-17 Denial-Of-Service Tools,, 1999

Han Y, Yang J, Chang B, Na J, Chung T (2004) The vulnerability assessment for active networks; model, policy, procedures, and performance evaluations. Comput Sci Appl–ICCS: 191–198

Hariri S, Qu G, Dharmagadda T, Ramkishore M, Raghavendra C (2003) Impact analysis of faults and attacks in large-scale networks. Secur Priv IEEE 1(5):49–54

ISO/IEC TR 13335 (2001) Information technology-Guidelines for the management of IT Security

Kamara S, Fahmy S, Schultz E, Kerschbaum F, Frantzen M (2003) Analysis of vulnerabilities in internet firewalls. Comput Secur 22(3):214–232

Pras A (2000) NTOP–Network TOP. An overview. University of Twente, The Netherlands

Ren T (2001) Computational model of computer virus. Chin J Comput: 02

Roesch M, Green C (2003) Snort Users Manual Snort Release: 2.0. 0. Apr 8 2003, vol 25

Rubin A (2002) Security considerations for remote electronic voting. Commun ACM 45(12):44

Shi L, Zhuang Y (2007) Quantitative risk assessment model for network security. Comput Eng Appl 43(018):146–149

Xiuzhen C, Qinghua Z, Xiaohong G, Chenguang L (2004) Study on Evaluation for Security Situation of Networked Systems. J Xi'an Jiaotong Univ 38(004):404–408

Yong W, Yifeng L (2009) A network security situational awareness model based on log audit and performance correction. Chin J Comput 32(4):763–772