

Network security equipment evaluation based on attack tree with risk fusion

CHENG Ran, LU Yue-ming

(School of Information and Communication Engineering, Beijing University of Posts and Communications, Beijing 100876, China)

Abstract: Network security equipment is crucial to information systems, and a proper evaluation model can ensure the quality of network security equipment. However, there is only a few models of comprehensive models nowadays. An index system for network security equipment was established and a model based on attack tree with risk fusion was proposed to obtain the score of qualitative indices. The proposed model implements attack tree model and controlled interval and memory (CIM) model to solve the problem of quantifying qualitative indices, and thus improves the accuracy of the evaluation.

Key words: attack tree, evaluation, network security equipment, risk fusion

doi: 10.11959/j.issn.2096-109x.2017.00183

1 Introduction

Various network security equipment such as firewalls, intrusion detection systems(IDS), and virtual private networks(VPN) have been deployed in information systems, to resist different levels and forms of network security threats. To ensure the quality of network security equipment, a measure of its security level must be put forward. However, there is only a few models of comprehensive evaluation models for network security equipment. The main reason is that there exist unsolved problems, including the differences between manufacturers and types, in the process of evaluation.

In 1998, the Lincoln Laboratory of MIT established the Lincoln Adaptive Real-time Information Assurance Testbed. In the experiment, they generated attack data and obtained the detection rate and false alarm ratio of the IDS. They drew the receiver operating characteristic(ROC) curve according to the result to evaluate the performance of network

security equipment^[1].

In 1999, the US and Canadian government and the European Community co-authored the Common Criteria of Information Technical Security Evaluation(CC), CC provided a detailed information security product metrics that helped developers eliminate security issues throughout the development process^[2].

A complete evaluation process requires a comprehensive index system, and some efforts have been made to build index systems of certain types of network security equipment. In those index systems, the score of quantitative indices can be obtained directly through the experiment, but for the score of qualitative indices, evaluation methods are diverse. The traditional methods, such as fuzzy comprehensive evaluation(FCE)^[3], are subjective and leads to the deviation of evaluation results. This paper proposed an evaluation model to measure qualitative indices based on attack tree with risk fusion. The model is shown in Fig. 1.

Received Date: 2017-06-10, **Revised Date:** 2017-07-03. **Corresponding Author:** CHENG Ran, hscrws@bupt.edu.cn

Foundation Item: The Research of Key Technology and Application of Information Security Certification Project (No. 2016YFF0204001)

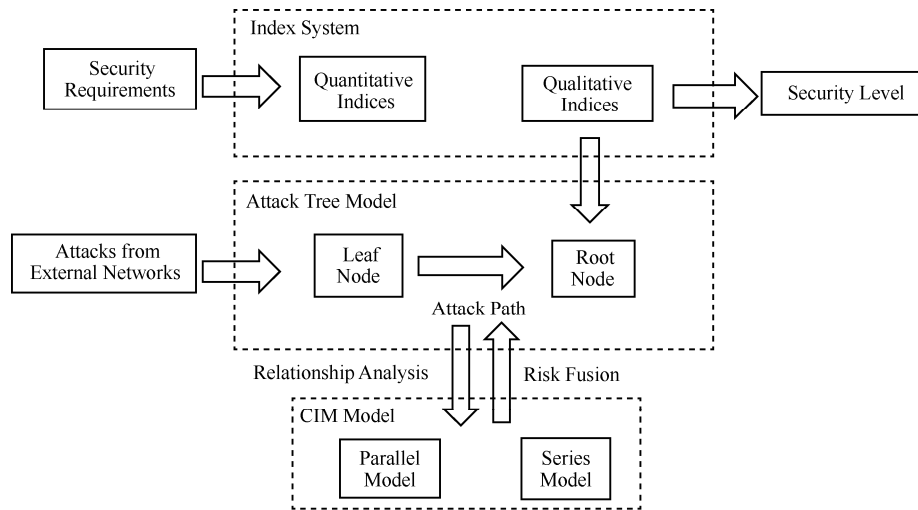


Fig. 1 Network security equipment evaluation model based on attack tree with risk fusion

Due to the complexity of security equipment, its evaluation index system has a multi-level structure. The model establishes the evaluation index system by analyzing the external network attacks and the security requirements for the equipment. The data for quantitative indices are obtained directly from experiments. As for the qualitative indices, an attack tree is set up for each index^[4], the risk of each security event is calculated with CIM model^[5], and the score of the index is obtained from the risk of the root node. After calculating the score of each index, we use analytic hierarchy process (AHP) to obtain the weight of them, and we can get the safety level of the equipment with linear weighted sum method^[6]. This model transforms qualitative indices into measurable indices by building attack trees, uses CIM model to implement the risk fusion and thus reaches a more comprehensive and objective evaluation of network security equipment.

The model aims to solve the problem of quantifying qualitative indices of network security equipment and reach a precise evaluation result. Based on this model, the paper established an evaluation index system of network security equipment, introduced attack tree model and CIM model, and

implemented the model by taking a specific qualitative index as an example.

2 The index system of network security equipment

A complete index system is the foundation for a comprehensive evaluation. According to international standard technical requirements for firewall, IDS, and VPN, this paper considers five quality properties including reliability, security, usability, function and performance^[7]. Based on these five properties, the paper proposed an evaluation index system for network security equipment.

To achieve comprehensive evaluation, we employed the following rules when choosing indices considering the complexity of network security equipment.

1) Every index should be important in its higher level property. The indices should reflect the quality of systems and have a significant impact on it.

2) According to the indices' measurability, the score of indices should be able to differ from different security levels, and can be directly measured. According to the two above-mentioned rules, we built an evaluation index system as shown in Fig. 2.

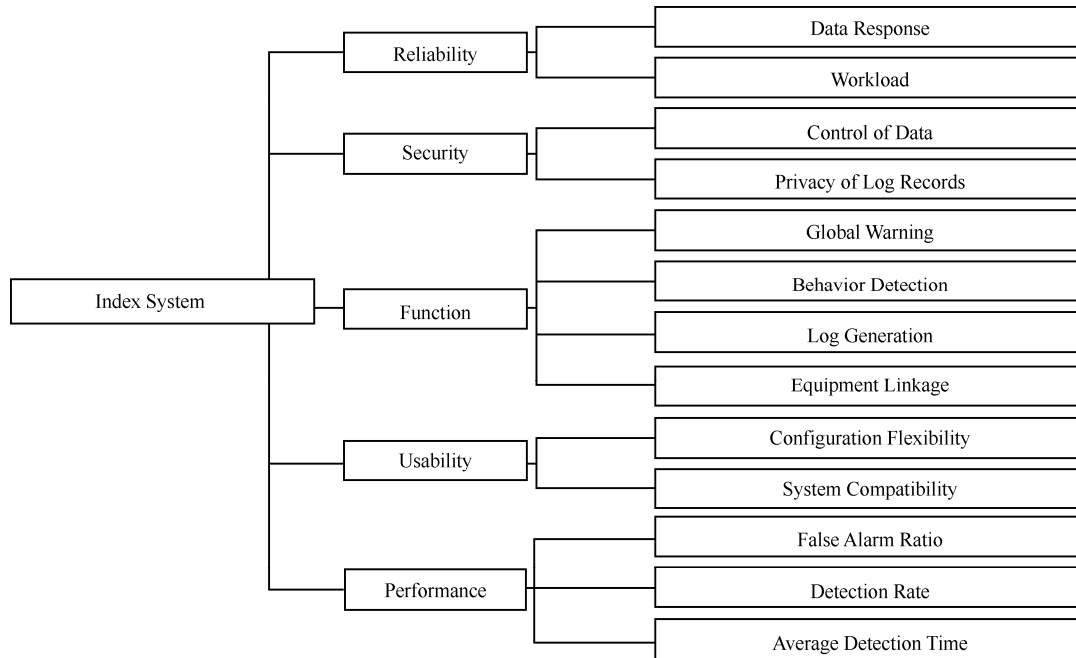


Fig. 2 The index system of network security equipment

Some of the indices in the index system are explained in detail in the following subsections.

2.1 Reliability indices

Reliability indices focus on the ability of the equipment to complete the function under specific conditions.

1) Data response. The equipment should have the ability to respond in the case of abnormal data.

2) Workload. This index measures the maximum capacity of resources an equipment can handle, while maintaining detection, alarm, and other main functions.

2.2 Security indices

Security indices focus on the ability to protect the equipment itself from accidents.

1) Privacy of log records. The equipment should only allow authorized users to perform operations on log records.

2) Control of data. When the equipment is under attack, it should be able to preserve the saved data.

2.3 Function indices

Function indices focus on the specific behavior

the network security equipment implement in the maintenance of security.

1) Global warning. All equipment should work together so that once an abnormal event is detected, the whole network will receive the signal and block the attack event.

2) Equipment linkage. The system should be able to cooperate with other equipment, to adjust their configuration automatically.

2.4 Usability indices

Usability indices focus on the difficulty of the network security equipment to be operated by users.

Flexible configuration. The equipment should be configured flexibly under different security conditions.

2.5 Performance indices

Performance indices focus on the performance of network security equipment.

1) False alarm ratio. This index indicates the ratio of non-attack operations among all the operations marked abnormal by equipment.

2) Detection rate. This index represents the fraction of intrusion operations that are detected by

equipment.

3) Average detection time. This index measures the average time from the detection to the response of attacks.

3 The attack tree model of network security

The network security equipment evaluation index system mentioned in section 2 has both quantitative indices and qualitative indices. To implement the measurement of qualitative indices, we need to use uniform evaluation algorithms to process the indices. Network security equipment serves to defend against attacks. Therefore, we can analyze network security equipment's security level from the attackers' perspective^[8]. Accordingly, this section introduces the attack tree model to facilitate the evaluation of qualitative indices and achieve an objective and comprehensive evaluation.

3.1 The attack tree model

The attack tree model uses a tree-like structure to describe the attacks against a system, and every complete attack generally includes a series of single attack behaviors. The states of attack can form an attack path and multiple attack paths can form an attack tree. The attack tree provides a formal and methodical approach to describe the security threats faced by the system and the possible attacks on the system. The root node of the tree indicates the ultimate goal of the attackers, namely the security requirements of network security equipment. The sub-goals are represented by child nodes and the leaf nodes represent the specific attack methods. The attack tree decomposes some possible security problems into several specific ones. As a result, each security problem's contribution value is decomposed into the computation of several specific security problems' contribution values.

3.2 Establishment of network security equipment's attack tree

For network security equipment, we first need to determine a security function requirement that

can be a possible ultimate goal of the external attack and use it as the root node of the attack tree. Next, possible attack events that are able to achieve the goal are analyzed and used as the child nodes of the attack tree. The relationship between these child nodes are also determined.

There are two types of child nodes. For nodes of type "OR", any event in its next level occurs will make itself occur. On the other hand, to make the node of type "AND" to occur, all the events of its next level should occur. We use the same approach to analyze all the child nodes until all the leaf nodes are events raised by attackers. A simple attack tree is shown in Fig. 3.

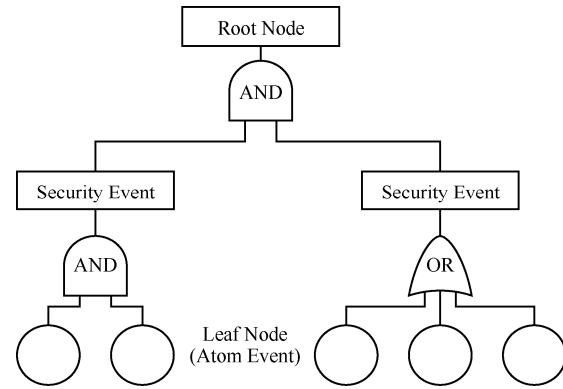


Fig. 3 A simple attack tree

3.3 Risk contribution value of atom events

The risk value of each security event in the attack tree depends on its sub-events' risk contribution value. Experts are given questionnaires to evaluate every leaf node's atom event's risk contribution value. The probability distribution of each atom event's risk contribution value can be computed by equation (1).

$$P_i = \frac{N_i}{N} \quad (1)$$

where N is the number of experts and N_i is the number of experts who rank the event's risk contribution value as level i .

3.4 The attack tree model and the information security index system

The root node of the attack tree corresponds to

a qualitative index in the information security index system. The attack tree model is used to quantify the index's risk contribution value and obtain the score of the qualitative index. We define the information security score using equation (2).

$$S_i = 1 - r_i \quad (2)$$

Where r_i is the risk contribution value of the event in the root node.

4 The CIM model of network security events

In attack tree model, every security event's risk value is determined by its sub-events' risk values. The computation approaches are different for different kinds of nodes. This section introduced CIM models to help calculate the fused risk value.

4.1 The CIM model

The CIM model was proposed by Chapman and Cooper in 1983. It is an effective approach to calculating fused probability distribution. Histograms having intervals with the same width are used in the CIM model to represent the probability distribution of a variable. The CIM model selects different response model to fuse risk probability according to the relationship between events and thus achieve the information security evaluation of the whole system.

The understanding of the CIM model can be carried out from two aspects: "control interval" and "memory".

4.1.1 Control interval

The CIM model utilizes small intervals with the same width in place of risk distribution curves. To increase precision, the interval can be shrunk to make the description more accurate. It simplifies the calculation of risk fusion.

4.1.2 Memory

After the risk interval distribution of each security event is determined, the risk probability should be fused according to different response models. The series model is used in the situation where an event will only occur when the two events

in its next level both occur. The parallel model is used in the situation where an event will occur when either event occurs in its next level. Whatever model is used, when fusing multiple events, the first two events are fused and the result is fused with the third, etc^[9].

4.2 The CIM series model

In the series model, the events of a higher level will be at risk only when all events of the next level are at risk. This scenario corresponds to the nodes of type "AND" in an attack tree. If series model is used when fusing risk probability of event D_1 and D_2 , the result can be computed using equation (3).

$$P(D_i = d_i) = \sum_{i=1}^n P(D_1 = d_{1i})P(D_2 = d_i - d_{1i}) \quad (3)$$

Where $d_i = d_{1i} + d_{2j}$, $i=1, 2, \dots, n$; $j=i=1, 2, \dots, n$, d_i is the median of risk interval and n is the number of groups.

4.3 The CIM parallel model

In the parallel model, the probability of each event is independent of each other and any event being at risk leads to the events of the higher level at risk. The nodes of type "OR" in an attack tree corresponds to this scenario. The formula used to fuse risk probability of event D_1 and D_2 is equation (4).

$$P(D_i = d_i) = \sum_{i=1}^n P(D_1 = d_i, D_2 \leq d_i) + \sum_{i=1}^n P(D_1 < d_i, D_2 = d_i) \quad (4)$$

Where d_i is the risk interval's median and n is the number of groups.

5 The measurement of qualitative index using attack tree with risk fusion

5.1 The establishment of attack tree

We take reliability index data response as an example to show how the IDS's data response index is evaluated. Intrusion detection can be categorized into anomaly intrusion detection and misuse intrusion detection and they use anomaly detection and feature detection respectively^[10]. After analyzing the security threats, IDSs' weakness and the service

failure issue caused by them, we establish the attack tree as shown in Fig. 4.

5.2 Computation of the security events' risk contribution values

To introduce the approach to computing risk distribution, we choose B3 as an example.

5.2.1 Results of C1~C4

Each event's risk contribution value was divided into 9 intervals from 0.05 to 0.95. According to the experts' evaluations of 4 atom events C1~C4, we calculated the risk distribution P_{ij} of atom event C_i . The risk distributions of atom events was shown in Table 1.

Since C1~C4 are connected to a node of type "OR", their probabilities of occurring are independent of each other and the occurrence of any event

will result in the occurrence of B3. Therefore, we used the parallel model to calculate B3's risk contribution value.

5.2.2 Result of B3

B3 has four sub-events that are connected by "OR" relationship. We first used the parallel model to calculate C1 and C2's fusion result and it is shown in Table 2.

Similarly, we fused C3 and C4 with the result in turn and event B3's risk distribution is shown in Table 3.

Instead of the naive sum of all the probability of the same interval, CIM's parallel model's computation of security events' risk contribution value is a fusion with memory. The risk distribution of B3 and C1~C4 is shown in Fig. 5.

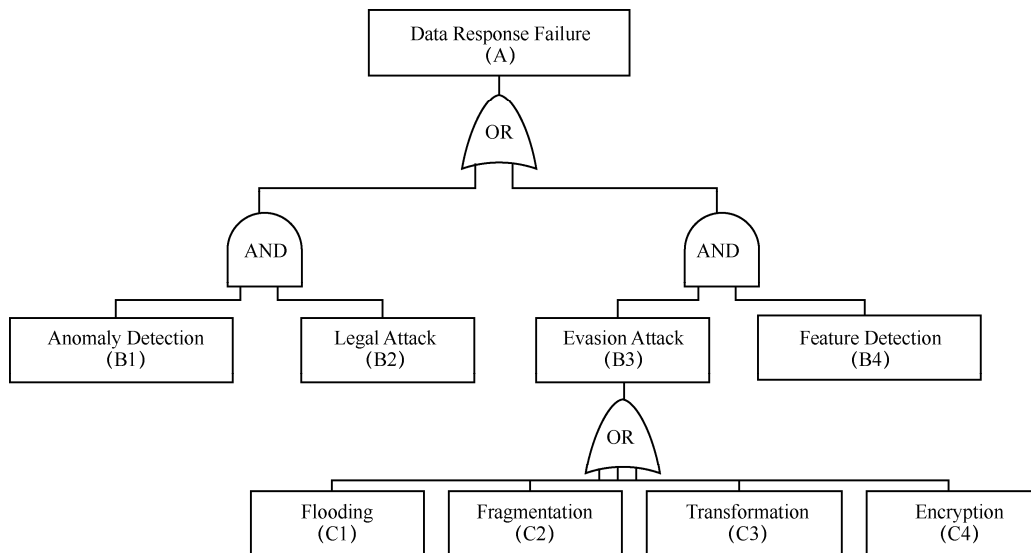


Fig. 4 The attack tree corresponding to data response index

Table 1

The risk distributions of atom events

Event	Risk interval				
	0.05~0.15	0.15~0.25	0.25~0.35	0.35~0.45	0.45~0.55
C1	$\frac{1}{10}$	$\frac{2}{10}$	$\frac{4}{10}$	$\frac{2}{10}$	$\frac{1}{10}$
C2	$\frac{1}{10}$	$\frac{1}{10}$	$\frac{2}{10}$	$\frac{3}{10}$	$\frac{3}{10}$
C3	$\frac{3}{10}$	$\frac{4}{10}$	$\frac{2}{10}$	$\frac{1}{10}$	0
C4	$\frac{1}{10}$	$\frac{1}{10}$	$\frac{5}{10}$	$\frac{3}{10}$	0

Table 2 Fusion of the risk of C1 and C2 using parallel model

Risk Interval	Risk Distribution
0.05~0.15	$\frac{1}{10} \times \frac{1}{10} = 0.01$
0.15~0.25	$\frac{2}{10} \times \left(\frac{1}{10} + \frac{1}{10} \right) + \frac{1}{10} \times \frac{1}{10} = 0.05$
0.25~0.35	$\frac{4}{10} \times \left(\frac{1}{10} + \frac{1}{10} + \frac{2}{10} \right) + \frac{2}{10} \times \left(\frac{1}{10} + \frac{2}{10} \right) = 0.22$
0.35~0.45	$\frac{2}{10} \times \left(\frac{1}{10} + \frac{1}{10} + \frac{2}{10} + \frac{3}{10} \right) + \frac{3}{10} \times \left(\frac{1}{10} + \frac{2}{10} + \frac{4}{10} \right) = 0.35$
0.45~0.55	$\frac{1}{10} \times \left(\frac{1}{10} + \frac{1}{10} + \frac{2}{10} + \frac{4}{10} + \frac{3}{10} \right) + \frac{3}{10} \times \left(\frac{1}{10} + \frac{2}{10} + \frac{4}{10} + \frac{2}{10} \right) = 0.37$

Table 3 The risk distribution of event B3

Risk Interval	Risk distribution
0.05~0.15	0.000 3
0.15~0.25	0.008 1
0.25~0.35	0.168
0.35~0.45	0.453 6
0.45~0.55	0.37

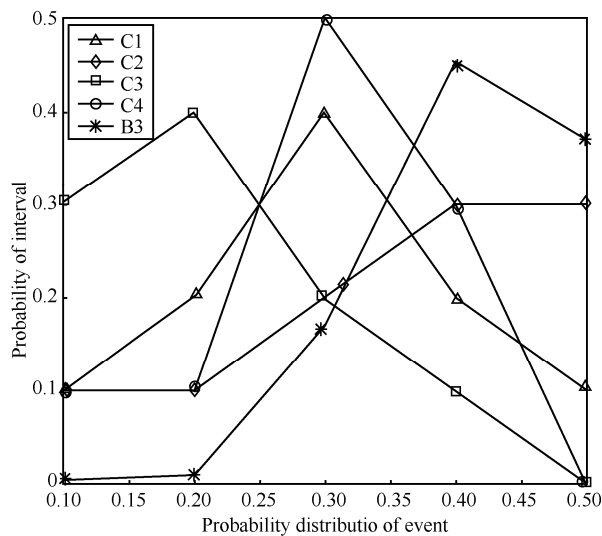


Fig. 5 Accumulation of atom events using parallel model

Calculated using the midpoint of each risk interval, C3's expected risk contribution value is 0.436 07.

5.2.3 The risk distribution of root node

Similarly, we obtained the risk distribution of event A and the result is shown in Table 4.

Event A's expected risk contribution value is

0.708 8. We then got the score of network security equipment's data response index according to equation (2).

Table 4 The risk distribution of event A

Interval's midpoint	Interval's probability
0.1	0
0.2	0
0.3	0.001
0.4	0.012
0.5	0.089
0.6	0.247
0.7	0.255
0.8	0.239
0.9	0.157

6 Conclusion and future work

At present, there is only a few evaluation models for the quality of network security equipment. This paper established the index system of quality of security from the aspects of function, performance, reliability, usability and security. In addition, having noticed the shortage in subjective evaluation method, we improved the evaluation model by evaluating the qualitative index with the help of risk contribution value. This model reduces the subjective factors and makes the results more reliable.

After the computation of the score of each index, methods like AHP can be used to obtain the

weight of each index, and linear weighted sum method can be employed to get the security level of network security equipment. In the future, we will carry out research on the calculation of index weight.

References:

- [1] LIPPMANN R P, FRIED D J, GRAF I, et al. Evaluating intrusion detection systems: the 1998 DARPA off-line intrusion detection evaluation[C]//DARPA Information Survivability Conference and Exposition(DISCEx'00). 2000:12-26.
- [2] HERRMANN D S. Using the common criteria for IT security evaluation[M]. Florida: CRC Press, 2002.
- [3] HAN L M Q. Analysis and study on AHP-fuzzy comprehensive evaluation[J]. China Safety Science Journal, 2004.
- [4] FUNG C, CHEN Y L, WANG X, et al. Survivability analysis of distributed systems using attack tree methodology[C]//Military Communications Conference. 2005:583-589.
- [5] CHAPMAN C B, COOPER D F. Risk engineering: basic controlled interval and memory models[J]. Journal of the Operational Research Society, 1983, 34(1):51-60.
- [6] SAATY L. How to make a decision: the analytic hierarchy process[J]. European Journal of Operational Research, 1990,48(1): 9-26.
- [7] PETTERSSON J. A study on software management approaches: proposing a project support tool[J]. University West Library, 2003.
- [8] VAN-HOLSTEIJN F A. The motivation of attackers in attack tree analysis[J]. TU Delft Library, 2015.
- [9] ZHANG X, BAI Y, LV L. Application of the controlled interval and memory model in the risk assessment of city gas transmission and distribution networks[C]//The International Conference on Pipelines and Trenchless Technology. 2012.
- [10] GONG Y, MABU S, CHEN C, et al. Intrusion detection system combining misuse detection and anomaly detection using genetic network programming[C]//Iccas-Sice. 2009:3463-3467.

About the authors:



CHENG Ran (1994-), born in Anhui. She is working on her master degree at Beijing University of Posts and Telecommunications. Her research interests include distributed computation and information security.



LU Yueming (1969-), born in Jiangsu. He received his Ph.D degree of computer architecture from Xi'an Jiaotong University in 2000. He is a professor in Beijing University of Posts and Telecommunications. His research interests include network simulation, network security and distributed computing.