Network Security Risk Assessment Based on Enterprise Environment Characteristics

Yunxue Yang[1], Zhenqi Yang[2], Qin Yang[1], Guohua Ji[1], and Shengjun Xue[1]
(Corresponding author: Yunxue Yang)

Department of Computer Science and Technology, Silicon Lake College[1]
168 Greenland Avenue, Huaqiao International Business Zone, Kunshan, Jiangsu, China
Binjiang College of Nanjing University of Information Science & Technology, China[2]
333 Xishan Avenue, Wuxi, Jiangsu, China
Email: brightyyx@qq.com

(Received Jan. 15, 2021; Revised and Accepted June 6, 2021; First Online Nov. 13, 2021)

Abstract

The authors studied the issue of network security risk assessment and proposed a method for the network security risk assessment based on enterprise environment. First of all, the authors proposed a vulnerability severity risk assessment method based on economic losses of an enterprise to evaluate the vulnerability severity for the enterprise. Next, the authors proposed a dynamic security risk assessment method by using the Bayesian attack graph model and combining the changes of network environment. Last, the case study interpreted the detailed calculation processes of the dynamic security risk assessment method, and the simulation experiment showed that the proposed method conforms to the real threat level of the network or information system evaluated, therefore, the evaluation results are more accurate and objective.

Keywords: Bayesian Attack Graph; Bayesian Inference; Dynamic Risk Assessment; Network Security

1 Introduction

With the rapid development of computer technology and network technology, the application of computers and networks has penetrated into all aspects of social life. However, due to security vulnerabilities in network systems, the number and variety of network attacks have multiplied, making network security problems more and more serious [8]. Typical cases include: In June 2019, Canada's largest credit cooperative, Desjardins, encountered security breaches and 2.9 million customer information was leaked. In 2020, many websites such as China's JD.com could not be accessed normally due to man-in-the-middle attacks, resulting in large-scale network hijacking incidents. The attack is likely to be based on the DNS system or at the operator level. Currently, users in some areas are mainly affected by all operators. For example, China Mobile, China Unicom, China Telecom and Education Network can reproduce the hijacking problem [12, 18].

Network security incidents have caused huge economic losses to enterprises. According to Allianz Risk Barometer Top Business Risks 2020 issued by Allianz Global Corporate & Specialty Risk (AGCS) [1], cybercrime caused a global economic loss of \$1.5 trillion, of which about 50% occurred in the top 10 economies of the world and this loss is expected to hit \$2.5 trillion this year with an increase of 60%.

In order to solve network security problems and conduct security management and control, network security risk assessment has become a research hotspot in the field of information security. The results of the security risk assessment not only reflect the security status of the network or information system, but also predict the possibility of future attacks on the network and risks brought by these possible attacks. This is the main basis for security administrators to take further security risk control measures. The current cybersecurity risk assessment methods mainly use the models such as attack tree, attack graph and Petri net to model network attacks and analyze various possible attacks and the relationship between them [14]. These models mainly quantitatively evaluate the attack probabilities of network nodes from the perspective of the vulnerabilities existing in the network and the associated utilization of the vulnerabilities.

An important aspect of cybersecurity risk assessment is the assessment of security vulnerabilities that exist in the network. An effective assessment of security vulnerabilities can improve the effectiveness of patches and system security hardening and the typical example of this aspect is the Common Vulnerability Scoring System (CVSS) [4]. CVSS is a vulnerability assessment standard jointly issued by the US Information Security Response and Security Group and the General Security Vulnerability Scoring System Expert Group in 2007. The current common standard of CVSS is version 3.1 published in 2019 [5].

CVSS uses quantitative score to determine the risk level of vulnerability from a technical perspective. In some publicly available vulnerability databases and scanning tools, CVSS method is commonly used. CVSS evaluates the risk of a vulnerability through three measure groups: The base measure group, the time measure group, and the environment measure group. However, in the actual situation, usually only the basic metric group is used, and the time metric group and the environmental metric group are not universally applicable [21].

Since the environmental characteristics of the enterprise affected by the vulnerability are not considered, the same vulnerability risk score is often calculated by using CVSS in the different enterprise environments. However, the impact of vulnerabilities on various corporate organizations is very different in the real world. Some previous research work has also raised this issue and it is recommended to use the CVSS method carefully to determine the risk of vulnerabilities [6]. Moreover, technically dangerous vulnerabilities do not necessarily have a large economic impact on corporate institutions, which is not uncommon [11]. Current cybersecurity risk assessment methods, such as the attack tree and attack graph models are based on a risk assessment of security vulnerabilities that exist in the network. However, the shortcoming of the current work is that when calculating the risk of a node (the probability of an attacker reaching the node), it only uses the CVSS base score of the vulnerability ignoring the characteristics of the vulnerability in a specific enterprise environment, such as the confidentiality, integrity and availability requirements of the enterprise, as well as the economic losses caused by the vulnerability. Because the risk assessment of the vulnerability is inaccurate, it is impossible to obtain an accurate cybersecurity risk assessment result that is consistent with the actual situation of the enterprise [9].

In summary, in order to develop a reliable cybersecurity risk assessment method that is consistent with the actual situation of the enterprise, it is necessary to fully consider the environmental background information of a specific enterprise. First, the risk of the vulnerability should be assessed based on the characteristics of the enterprise environment, and then the network security risk assessment should be conducted within the enterprise. Based on the above observations, the main contributions of this paper are:

1) In order to assess the risk of security vulnerabilities, this paper proposes a set of metrics based on the economic loss of enterprises.

2) In order to assess the risk of security vulnerabilities quantitatively, this paper proposes a quantitative method to integrate CVSS metrics, enterprise's economic loss metrics and enterprise's security requirements metrics.

3) Based on the above two points, this paper proposes a dynamic security risk assessment method (NSRAEE), which can be combined with the environmental changes of enterprises to assess the enterprises' risks dynamically.

2 Related Work

2.1 Security Vulnerability Assessment

In order to assess the seriousness of system vulnerabilities, Karie *et al.* [9] proposed a quantitative evaluation model based on grey evaluation method and analytic hierarchy process. Mahdavifar *et al.* [11] selected the access route, and used the complexity and degree of influence as the three elements to evaluate the threat of the vulnerability. The users used the analytic hierarchy process to establish the evaluation model and the vulnerability level of the vulnerability was classified as super-risk, high-risk, medium-risk and low risk. Atapattu *et al.* [2] used a medical "case-control study" approach to compare the severity and availability of vulnerabilities. Xiao *et al.* [20] used fuzzy analytic hierarchy approach to evaluate the security level of software vulnerabilities, and further considered human subjectivity in reality, emphasized the relationship between different factors affecting information security, improved the traditional fuzzy comprehensive decision model, and proposed fuzzy integral decision model.

Zhu *et al.* [23] proposed a new vulnerability rating and scoring system (VRSS) based on the existing vulnerability level system. VRSS combines the advantages of the existing vulnerability level system and can qualitatively determine vulnerability threat levels and rate vulnerabilities quantitatively. In order to further improve the quality of vulnerability scores, Rosli *et al.* [7,13] used the analytic hierarchy process to classify vulnerabilities through vulnerability types and quantitatively describe the characteristics of vulnerability types on the basis of VRSS, thus improving the quality of vulnerability scores.

2.2 Cybersecurity Risk Assessment

The traditional cybersecurity risk assessment methods mainly use the models of attack tree, attack graph and Petri net to model network attacks and analyze various possible attacks and the relationship between them. These models mainly quantitatively evaluate the attack probability of network nodes from the point of view of vulnerabilities existing in the network and the correlation of vulnerabilities.

In order to further study the uncertainties in cyberattacks, some probabilistic models are proposed to study the quantitative assessment of cybersecurity risks, including Markov decision process models, Bayesian networks, Bayesian attack graphs and other models. These approaches model the uncertainties in the existence of cyber attacks. For example, Wang *et al.* [3] proposed a probabilistic model for assessing cybersecurity risks, using attack graphs to model network vulnerabilities, and applying Bayesian networks to perform cybersecurity risk analysis. Sun *et al.* [19] used Bayesian networks to model the potential attack paths in the system and proposed an attack path optimization algorithm based on attacker's knowledge and attack patterns in the attack graph, thus conducting security risk assessment. In this work, the node is given a probability value to describe the probability of an attack occurring at the node and the probability value of the system is destroyed by the Bayesian network.

The above work can only deal with the simpler situation in the network system and is the static security risk assessment. Although the results of the static security risk assessment are accurate, due to the uncertainty and suddenness of the network security incidents, the evaluation results are relatively lagging and it is difficult to meet the actual needs [17]. In response to this problem, Li *et al.* [15] introduced a Bayesian attack graph model and based on this, the authors proposed a dynamic security risk assessment method. The fundamental difference between their work and our work is that they do not fully consider the environmental characteristics of the enterprise when assessing cybersecurity risks.

3 Security Vulnerability Assessment

Security Vulnerability assessment is the basis for cybersecurity risk assessment. To assess the risk of vulnerabilities associated with the environmental characteristics of an enterprise, we first introduce a set of security vulnerability assessment metrics that determined by the economic loss caused by exploits to the enterprise, and then introduce the integration of CVSS metrics, enterprise's economic loss metrics and quantitative metrics for enterprise security requirements to quantify the risk of security vulnerabilities.

3.1 Enterprise's Economic Loss Metrics

Corporate's economic loss metrics focus on the economic impact of exploits on businesses, with the goal of specifically quantifying the damage caused by cyber attacks into financial data. Before describing the metric set in detail, we first introduce several necessary conditions:

1) After the introduction of the new measurement standard, the comprehensive score of the security vulnerability should be diversified, that is, it should avoid the excessive concentration of vulnerability risk score;

2) The vulnerability risk scoring process should not be too complicated referring to the CVSS scoring principle;

3) For ease of understanding, the score should be consistent between different analysts in the company.

3.1.1 Enterprise's Economic Loss Classification

The quantitative scoring process is more objective than qualitative ratings. However, quantitative scoring does not give a relatively straightforward understanding of the risk of security vulnerability. Referring to the CVSS vulnerability risk classification principle, this paper divides the economic loss into four scales, namely low-level, intermediate-level, advanced-level and severe-level. There are two advantages to this: One is to facilitate the economic loss caused by different attack scenarios within the company; the other is to facilitate the understanding of non-technical personnel, such as business management personnel. Since it is impossible to compare the absolute value of property damage between enterprises of different scales, for example, the property loss of 100,000 US dollars may be a high-level loss for a small and medium-sized enterprise, but it may be a low-level loss for a large multinational company. Therefore, the proposed qualitative level of property loss is related to the specific financial system of a specific enterprise. The enterprise needs to define the currency interval threshold according to its own characteristics, as shown in Table 1, where the quantitative score is in decimal.

Table 1: Enterprise economic loss levels

low	$[0, C_{medium}]$	3.5
medium	$[C_{medium}, C_{high}]$	6.1
high	$[C_{high}, C_{critical}]$	7.1
serious	$[C_{critical}, \infty]$	10.0

3.1.2 Enterprise's Economic Loss Metrics

We define a set of vulnerability economic loss metrics based on the empirical work of Spagnuelo *et al.* [22]. Spagnuelo *et al.* defined economic cost units based on publicly known security incidents. This paper integrates the "potential economic loss" as shown in Figure 1. The definitions and calculation formulas for each type are described below.

Definition 1. *Revenue loss (RevL). Computer systems bring benefits to enterprises. Suppose c represents the number of customers in a business and r represents the average customer revenue for a transaction. There are two main reasons for the loss of corporate's revenue: One is that system services are not available; the other is customers' loss due to longer service response time. Suppose A indicates the availability of system services, $A = 1$ indicates that system services are available and $A = 0$ indicates that system services are unavailable. Then the loss of revenue due to the unavailability of system services is:*

$$RevL = c \times r \times (1 - A) \quad (1)$$

Definition 2. *Reputation loss (RL). The reputational damage caused by exploits is harder to measure. The usual*

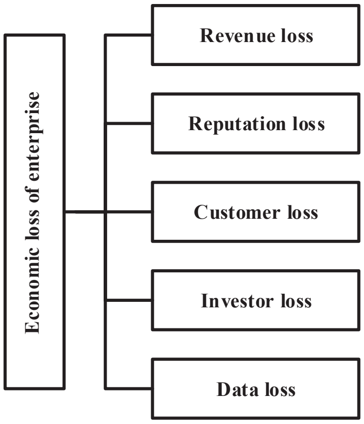

Figure 1: Economic loss of the enterprise

measure of reputational loss is by measuring the historical impact of exploits and security incidents on corporate stocks. Assuming that ise is the average historical impact of exploits on a company's stock price, then the reputation loss is calculated:

$$ise = \frac{1}{n}\sum_{t=0}^{n} P_t - P_{after} \quad (2)$$

Definition 3. *Customer loss (CL). After the enterprise's exploit event is announced, the security-sensitive customers will terminate the cooperation with the enterprise, which will lead to customer losses. The calculation formula is:*

$$CL = ssc \times arc_t \quad (3)$$

where ssc is the number of customers who are sensitive to security and arc is the average customer's revenue in each time period.

Definition 4. *Investor loss (IL). After the company's exploits are announced, security-sensitive investors will stop investing in the company. The formula for calculating investors' losses is:*

$$IL = ssi \times ai_t \quad (4)$$

where ssi is the number of security-sensitive investors and ai_t is the average investment amount of the investor in each time period.

Definition 5. *Data loss (DL). Data leakage will cause property damage to the company. The calculation formula for data loss due to data leakage is:*

$$DL = avr \times nlr \quad (5)$$

where avr is the average value of each data record and nlr is the number of lost data records. The avr value can be determined by using historical audit data within the enterprise.

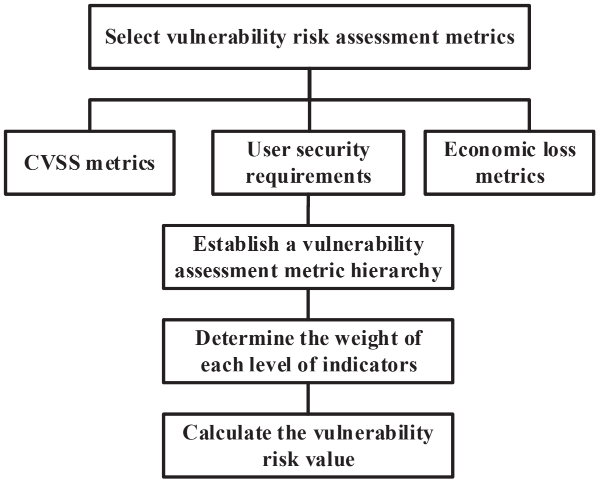
Select vulnerability risk assessment metrics
CVSS metrics
User security requirements
Economic loss metrics
Establish a vulnerability assessment metric hierarchy
Determine the weight of each level of indicators
Calculate the vulnerability risk value

Figure 2: Risk assessment method for security vulnerabilities

3.2 Quantitative Assessment Method for Risk of Security Vulnerabilities

This paper considers the risk of vulnerabilities from three aspects: Economic losses caused by vulnerabilities, enterprise security requirements and CVSS scores of vulnerabilities for the vulnerability risk assessment based on the economic losses caused by cyber attacks to enterprises. The metrics for assessing the vulnerability risk are:

1) Corporates' economic loss metrics.

2) Enterprises' security requirements metrics.

3) CVSS basic metrics.

Because these metrics do not affect the risk assessment of vulnerabilities on average, they need to be weighted by a user-centric approach that considers the security needs of specific users and the specificities of the enterprise environment. All three types of metrics use "cost" as the sole criterion, that is, in an ideal situation, how to minimize the cost loss caused by the vulnerability. Therefore, this is a typical multi-criteria decision-making analysis (MCDA) which sorts a certain number of objects according to established standards [10]. In this article, vulnerabilities are objects that need to be sorted according to standards. The analytic hierarchy process (AHP) is one of the most widely used and accurate MCDA methods [16]. The method is divided into three levels: Target layer, criterion layer and solution layer according to the overall goal and decision-making scheme of the problem, and then the method of pairwise comparison is used to determine the importance of the decision-making scheme, so as to make a satisfactory decision. AHP can be divided into the following four steps:

1) Identify problems and establish a hierarchy;

2) Construct a judgment matrix;

3) Hierarchical single sorting and consistency test;

4) Hierarchical total ordering and combination consistency test.

According to the four steps, the established risk vulnerability assessment method is shown in Figure 2.

4 Cybersecurity Risk Assessment

In this section, we introduce the cybersecurity risk assessment method which is based on the quantitative assessment of vulnerability risk. First, we introduce the relevant definitions, then introduce the assessment method that can be combined with the characteristics of the enterprise environment for dynamic security risk assessment.

4.1 Related Definitions

Definition 6. *Atomic attack. Suppose S is a set of network attributes, A is a conditional dependency between a pair of network attributes and A is represented as a form of mapping $S \times S \to [0,1]$. Then, given $S_{pre}, S_{post} \in S$, $a : S_{pre} \to S_{post}$ is called an atomic attack if:*

1) $S_{pre} \neq S_{post}$;

2) $A\left(S_{pre}, S_{post}\right) > 0$ when $S_{pre} = 1$ and $S_{post} = 1$;

3) There does not exist $S_1, S_2, ..., S_j \in S - \{S_{pre}, S_{post}\}$ making $A\left(S_{pre}, S_1\right) > 0$, $A\left(S_1, S_2\right) > 0$, ..., $A\left(S_j, S_{post}\right) > 0$.

An atomic attack indicates that the attacker successfully reached attribute S_{post} from attribute S_{pre} with a non-zero probability. Among them, the condition 3 indicates that the attacker directly reaches the attribute S_{post} from the attribute S_{pre}, and does not pass other network attributes in the middle. In addition, an atomic attack is usually associated with an exploit which exploits an attacker from one network property to another. We use e_i for vulnerability utilization and $t(e_i)$ for the danger of exploiting the vulnerability.

Definition 7. *Bayesian attack graph (BAG). Suppose S is a set of network attributes and A the set of atomic attacks defined on S. A Bayesian attack graph is a quad of $BAG = (S, \tau, \varepsilon, P)$, where:*

1) $S = N_{internal} \cup N_{external} \cup N_{terminal}$. $N_{external}$ is a set of attributes S_i, for the set of S_i, there does not exist $a \in A | S_i = post\left(a\right)$. $N_{internal}$ is a set of attributes S_j and there does not exist $a_1, a_2 \in A | S_j = pre\left(a_1\right) \wedge post\left(a_2\right)$. $N_{terminal}$ is a set of attributes S_k and there does not exist $a \in A | S_k = pre\left(a\right)$.

2) $\tau \subseteq S \times S$. If $S_{pre} \to S_{post} \in A$, then ordered pair $\left(S_{pre}, S_{post}\right) \in \tau$. In addition, for $S_i \in S$, the set $Pa\left[S_i\right] = \{S_j \in S | \left(S_j, S_i\right) \in \tau\}$ is called the parent node set of S_i.

3) ε is a set of elements of the form $\langle S_j, d_j \rangle$. For all $\forall S_j \in N_{internal} \cup N_{terminal}$ and $d_j \in \{AND, OR\}$, d_j is AND if $S_j = 1 \Rightarrow \forall S_i \in Pa\left[S_j\right]$, $S_i = 1$. d_j is OR if $S_j = 1 \Rightarrow \exists S_i \in Pa\left[S_j\right]$, $S_i = 1$.

4) P is a set of conditional probability distributions. Each attribute $S_j \in N_{internal} \cup N_{terminal}$ has a conditional probability distribution with a value of $Pr\left(S_j | Pa\left[S_j\right]\right)$.

Definition 8. *Condition probability distribution (CPD). Let $BAG = (S, \tau, \varepsilon, P)$ be a Bayesian attack graph, $S_j \in N_{internal} \cup N_{terminal}$. For $S_i \in Pa\left[S_j\right]$, e_i is an exploit related to the atomic attack $S_i \to S_j$. The conditional probability distribution of S_j is $Pr\left(S_j | Pa\left[S_j\right]\right)$ and the definition is:*

if $d_j = AND$,

$$Pr\left(S_j | Pa\left[S_j\right]\right) = \begin{cases} 0, \exists S_i \in Pa\left[S_j\right] | S_i = 0 \\ t\left(\bigcap\limits_{S_i=1} e_i\right), otherwise \end{cases} \quad (6)$$

if $d_j = OR$,

$$Pr\left(S_j | Pa\left[S_j\right]\right) = \begin{cases} 0, \forall S_i \in Pa\left[S_j\right] | S_i = 0 \\ t\left(\bigcup\limits_{S_i=1} e_i\right), otherwise \end{cases} \quad (7)$$

When multiple exploits are involved, in order to calculate the conditional probability distribution, we proceed as follows: For the case of "AND", each exploit is an independent event. The probability of destroying a target node depends on the probability of successfully exploiting a single exploit. Therefore, the law of independence of events is:

$$t\left(\bigcap\limits_{S_i=1} e_i\right) = \prod\nolimits_{S_i=1} t\left(e_i\right). \quad (8)$$

In the case of "OR", this relationship is actually a Noisy-OR relationship. There is:

$$t\left(\bigcup\limits_{S_i=1} e_i\right) = 1 - \prod\limits_{S_i=1} \left[1 - t\left(e_i\right)\right]. \quad (9)$$

4.2 Cybersecurity Risk Assessment Method

Cybersecurity risk assessment is the basis for network security risk management. Currently, cybersecurity risk assessment techniques can be divided into two categories: Static security risk assessment and dynamic security risk assessment.

The static security risk assessment is to evaluate the security risks of the network in a short period of time or at a certain point in time. Although the assessment results are accurate, they are relatively lagging, so it is difficult to meet the actual needs. Dynamic security risk assessment studies the evolution trend of network security risks

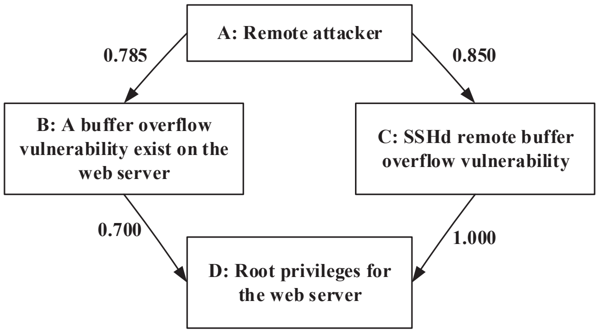
A: Remote attacker
0.785
0.850
B: A buffer overflow vulnerability exist on the web server
C: SSHd remote buffer overflow vulnerability
0.700
1.000
D: Root privileges for the web server

Figure 3: Risk assessment method for security vulnerabilities

and evaluates the network security in a period of time in combination with the changes of network environment, so as to grasp the changes of network security risks with the changes of network environment factors. The dynamic security risk assessment method we use is described below.

During the life cycle of a network system, the probability of occurrence of each network state changes. Emerging cybersecurity events can affect the likelihood of an attack. This paper evaluates network security risks from these emerging cybersecurity incidents by using the Bayesian attack graph model to calculate posterior probabilities.

Suppose $S = \{S_1, S_2, ..., S_n\}$ is a set of attributes in a Bayesian attack graph and $E = \left\{S_1^{'}, S_2^{'}, ..., S_m^{'}\right\} \subset S$ is a subset of S, the attributes in this set represent the attack events that have occurred. These attributes are called “evidence”, i.e. for all $S_i^{'} \in E$, there is $S_i^{'} = 1$. Existing S_j needs to determine the posterior probability of S_j. According to Bayes' theorem, there is:

$$\Pr(S_j|E) = \frac{\Pr(E|S_j) \times \Pr(S_j)}{\Pr(E)} \tag{10}$$

where $\Pr(E|S_j)$ is the conditional probability that $\left\{S_1^{'}, S_2^{'}, ..., S_m^{'}\right\}$ are combined in the state given S. $Pr(E)$ and $Pr(S_j)$ are priori unconditional probability values for the corresponding attributes. The evidence in E is independent of each other, so we have $\Pr(E|S_j) = \prod_i \Pr\left(S_i^{'}|S_j\right)$ and $\Pr(E) = \prod_i \Pr\left(S_i^{'}\right)$.

5 Case Study

5.1 Case Analysis

This paper takes a small bayesian attack graph shown in Figure 3. as an example to illustrate the calculation process of the network security risk assessment method in detail. In Figure 3. node A represents ”remote attacker”, node B represents ”a buffer overflow vulnerability exists on the web server (CVE-2019-9933)” and node C represents ”SSHd remote buffer overflow vulnerability”. Node D stands for ”root privileges for the web server.” The edges in Figure 3. indicate the corresponding exploits. For example, the edge between node A and node B indicates that ”the attacker exploited the buffer overflow vulnerability to launch an attack.” The value next to each edge is the result of dividing the vulnerability risk quantified value by 10, in order to make the score between 0 and 1. The attacker's goal is to gain root access to the Web server for damage. It is assumed that in this case, the availability of the Web server is high, and the security risk assessment of the network structure is performed for this feature. The specific calculation process is as follows.

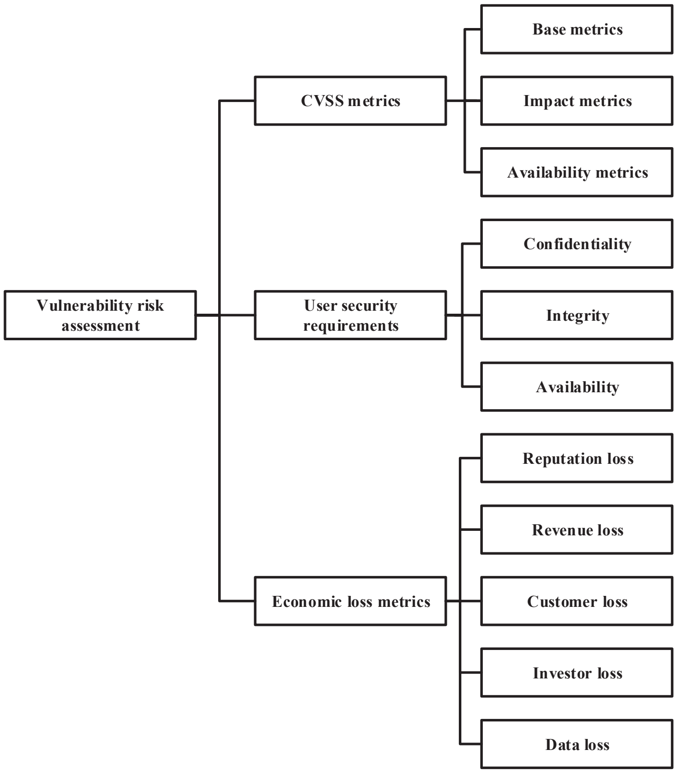

Figure 4: Hierarchical structure of vulnerability severity assessment

Step 1. Establish a hierarchy of vulnerability risk assessments.

The hierarchy of the risk assessment for vulnerability CVE-2019-9933 is shown in Figure 4.

Step 2. Construct a judgment matrix.

In this case, the availability of Web servers is high, so the CVSS metrics, user security requirements and economic loss metrics are constructed in a 1:3:1 ratio. The importance of the criteria layer for the target layer is $G = \begin{bmatrix} 1 & 1/3 & 1 \\ 3 & 1 & 3 \\ 1 & 1/3 & 1 \end{bmatrix}$.

Similarly, the importance matrices of the solution layer for the criterion layer are $C_1 = \begin{bmatrix} 1 & 4 & 4 \\ 1/4 & 1 & 1 \\ 1/4 & 1 & 1 \end{bmatrix}$, $C_2 = \begin{bmatrix} 1 & 1 & 1/3 \\ 1 & 1 & 1/3 \\ 3 & 3 & 1 \end{bmatrix}$, and $C_3 =$

$$\begin{bmatrix} 1 & 2 & 3 & 5 & 6 \\ 1/2 & 1 & 3 & 4 & 5 \\ 1/3 & 1/3 & 1 & 3 & 5 \\ 1/5 & 1/4 & 1/3 & 1 & 2 \\ 1/6 & 1/5 & 1/5 & 1/2 & 1 \end{bmatrix}$$

. Considering that the data loss accounts for the largest proportion of economic losses, the loss of revenue, reputation loss, customer loss, investor loss and data loss construct the matrix C_3 in a ratio of $1:2:3:5:6$.

Step 3. Hierarchical single sorting and consistency check. Taking the judgment matrix G as an example, we use Matlab to calculate the maximum eigenvalue, the corresponding eigenvector, the consistency index and the random consistency ratio of the matrix G are $\lambda_{\max} = 4$, $W = (0.15, 0.45, 0.1)^T$, $C = \frac{\lambda_{\max} - n}{n-1} = \frac{4-4}{4-1} = 0$ and $C_R = 0$ respectively. Therefore, the CVSS base metrics, user security requirements and economic loss metrics can be considered to have weights of vulnerability risk assessments of 0.1, 0.45, and 0.35 respectively.

Step 4. Hierarchical total ordering and its combination consistency test. Hierarchical total sorting combination consistency check $C = 0$, $C_R = 0 < 0.1$.

Step 5. Calculate the vulnerability value of vulnerability risk. According to the expert's scoring sample matrix of vulnerability CVE-2019-9933, the risk of the vulnerability is quantified as:

$$P_v = W \times S = 8.6428 \tag{11}$$

The risk of other vulnerabilities in Figure 3. can be quantified using the same method.

Step 6. Calculation of node risk value.

Suppose the network administrator detects a network attack on node D, that is, the attacker gains root access to the web server. The posterior probability of node B is calculated as follows:

$$\Pr(B|D) = \frac{\Pr(D|B)\Pr(B)}{\Pr(D)} \tag{12}$$

where,

$$\Pr(D|B) = \sum_{C \in \{T,F\}} [\Pr(D|C, B = T)\Pr(C)] \tag{13}$$

The posterior probability of the Node B is 0.6830. It is worth noting that the node's unconditional probability is 0.4810 without considering the web server being attacked. After considering the attack event occurring on node D, the posterior probability of node B becomes 0.6830. There is a significant improvement over the previous one. By taking into account the environmental information of the system, it is possible to make a more accurate and effective assessment of the security of the network.

5.2 Effect Evaluation

This section uses the network topology shown in Figure 5. as the evaluated network for simulation experiment. We suppose a small and medium-sized enterprise X specializes in providing online electronic trading services to users. The enterprise's network topology is shown in Figure 5. The network consists of three sub-networks, namely the external service area, the internal management area and the internal user area. The three areas are divided by a firewall, and the entire network is connected to the Internet through a gateway. Among them, the external service area mainly includes a network server and a mail server. The two servers provide network services and mail services to external and internal users respectively. The internal management area includes a file transfer server, two database servers and two clients. The file transfer server mainly provides web-related file storage and management services for the web server and the two clients can operate the file transfer server through SSH links. Potential attackers on the network come from external attackers accessing the Internet. We use Nessus as a vulnerability scanning tool to obtain vulnerability information on each host/server in the network as shown in Table 2.

Taking into account the characteristics of enterprise X, we simulate two application scenarios for experimental analysis.

Scenario 1. In this network, the web server is just a common web server for publishing common sense and introductory, without storing important and valuable data and information. In this case, the enterprise has high demand for the availability of the network server.

Scenario 2. In this network, the network server bears the main service of the network, and the collapse of the network server will have a greater impact on the enterprise. In this case, the enterprise has higher requirements for the availability and confidentiality of the network server.

We use the proposed cybersecurity risk assessment method (NSRAEE) to calculate the risk quantified values of the servers in these two scenarios and use the method of [15] to calculate the risk quantified values of the servers in the two scenarios. The results are shown in Table 3.

Table 3 shows the calculation results of the server risk quantized values in the two scenarios of this method and the calculation results of the reference method. The reference method has the same result in both scenarios, so only a set of results is shown. It can be seen from Table 3 that the method of [15] does not consider the security requirements of the enterprise network and the risk quantified values of the respective servers calculated in the two scenarios are the same. With this method, the server's risk quantification value will vary depending on the enterprise environment. For example, in scenario 2, the network server assumes the main service of the network and is an important business asset of the enterprise.

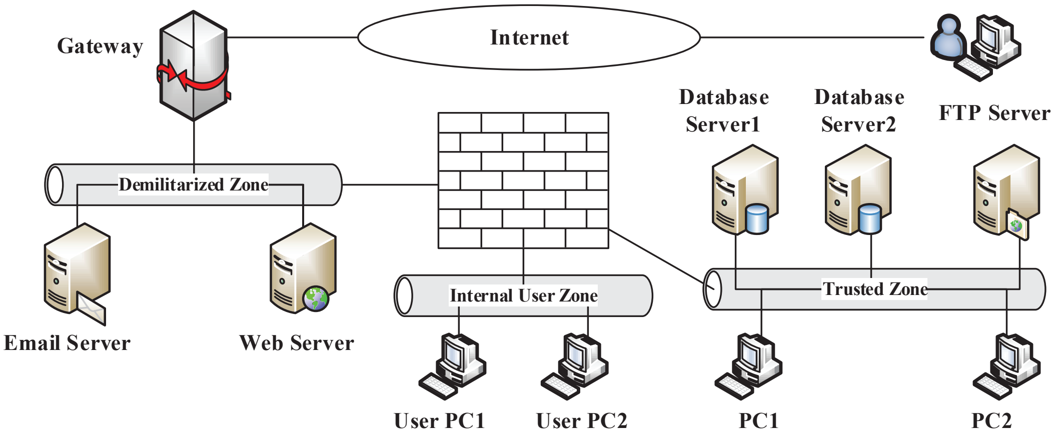

Figure 5: Network topology

Table 2: Vulnerability information

host	CVE number	Attack type
network server	CVE-2019-8952	DDoS
mail server	CVE-2019-12497	remote attack
	CVE-2019-10735	information leakage
ftp server	CVE-2019-10967	privilege escalation
	CVE-2018-7240	remote attack
	CVE-2019-11380	remote attack
database server 1	CVE-2019-5632	remote attack
database server 2	CVE-2019-7667	remote attack
gateway	CVE-2019-8319	information leakage

Table 3: Risk quantification values of servers

Host	Reference method	NSRAEE: Scenario 1	NSRAEE: Scenario 2
network server	0.6127	0.3891	0.7628
mail server	0.6854	0.5588	0.7359
ftp server	0.6987	0.4847	0.7983
database server 1	0.6218	0.3456	0.8742
database server 2	0.6142	0.5754	0.6877
gateway	0.5874	0.6683	0.7531

If it collapses or is invaded, it will have a greater impact on the enterprise. Therefore, the network server obtained using the calculation method of this paper has a larger risk quantized value in scenario 2 than in scenario 1.

In summary, the proposed network security risk assessment method considers the security requirements of the enterprise network environment and covers the impact of environmental threat information on the node risk, making the method more suitable for the network or information system being evaluated. The actual situation of the possibility of an attack is more objective and accurate.

6 Conclusion

In the process of cybersecurity management, cybersecurity risk assessment is the premise and foundation of network security management. In order to develop a reliable cybersecurity risk assessment method that is consistent with the actual situation of the enterprise, it is necessary to fully consider the environmental characteristics of a specific enterprise. In response to this problem, this paper proposes a method to assess the security risks of enterprise network systems based on the characteristics of enterprise environment. First, we assess the risk of security breaches based on enterprise security needs, the economic losses caused by the attack and the CVSS base metric. Then, we use the Bayesian attack graph model combined with the environmental changes of the enterprise network system for dynamic security risk assessment. Finally, the specific calculation process is illustrated by the case study, and the simulation experiment proves that compared with the existing methods, the quantitative evaluation method proposed in this paper is more suitable for the safety risk status of the evaluated enterprise. The evaluation result is more objective and accurate.

Future research work will further consider more possible metrics for corporate economic losses. In addition, how to simplify the scale of the attack graph is also the focus and difficulty of the research.

7 Acknowledgments

This work is supported by The Natural Science Foundation of the Jiangsu Higher Education Institutions of China (No.19KJD520002), and Jiangsu Province Higher Education College Students Innovation and Entrepreneurship Training Program (No. 202012078001Y).

References

[1] Allianz Risk Barometer 2020 - Top global business risks, 2021. (`https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html`)

[2] S. Atapattu, N. Ross, Y. Jing, *et al.*, "Physical-layer security in full-duplex multi-hop multi-user wireless network with relay selection," *IEEE Transactions on Wireless Communications*, vol. 18, pp. 1216–1232, 2019.

[3] Y. H. Chen, Y. Z. Xie, X. Y. Ge, *et al.*, "Vulnerability assessment of equipment excited by disturbances based on support vector machine and gaussian process regression," *IEEE Transactions on Electromagnetic Compatibility*, no. 99, pp. 1-8, 2020.

[4] W. U. Chensi, T. Wen, Y. Zhang, "A revised CVSS-based system to improve the dispersion of vulnerability risk scores," *Information Sciences*, vol. 62, no. 03, pp. 193-195, 2019.

[5] Common Vulnerability Scoring System v3.1. (`https://www.first.org/cvss/v3-1/`)

[6] B. Cruz, S. Gomez-Meire, D. Ruano-Ordas, *et al.*, "A practical approach to protect IoT devices against attacks and compile security incident datasets," *Scientific Programming*, vol. 2019, no. 4, pp. 1-11, 2019.

[7] S. Ding, Z. Zhang, J. Xie, "Network security defense model based on firewall and IPS," *Journal of Intelligent and Fuzzy Systems*, no. 12, pp. 1-9, 2020.

[8] M. Gao, J. Zhang, J. Yu, *et al.*, "Recommender systems based on generative adversarial networks: A problem-driven perspective," *Information Sciences*, vol. 546, pp. 1166-1185, 2020.

[9] N. M. Karie, V. R. Kebande, H. S. Venter, "Diverging deep learning cognitive computing techniques into cyber forensics," *Forensic Science International: Synergy*, vol. 1, pp. 61-67, 2019.

[10] P. Lin, Y. Chen, "Network security situation assessment based on text SimHash in big data environment," *International Journal of Network Security*, vol. 21, no. 4, pp. 699-708, 2019.

[11] S. Mahdavifar, A. A. Ghorbani, "DeNNeS: Deep embedded neural network expert system for detecting cyber attacks," *Neural Computing and Applications*, vol. 32, no. 6, 2020.

[12] A. Olagunju, "Where did I leave my keys?: Lessons from the Juniper dual EC incident," *Computing Reviews*, vol. 60, no. 4, pp. 168-169, 2019.

[13] S. Rosli, R. S. Abdullah, W. Mohamed, "Ransomware behavior attack construction via graph theory approach," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 2, pp. 10, 2020.

[14] M. Y. Ruan, H. D. Chiang, "On the accuracy of the online static security assessment under Different models: Assessment and basis," *IEEE Transactions on Power Systems*, vol. 99, pp. 1-8, 2019.

[15] S. S. Sathya, K. Umadevi, "An optimized distributed secure routing protocol using dynamic rate aware classified key for improving network security in wireless sensor network," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1-7, 2020. DOI:10.1007/s12652-020-02392-2.

[16] K. Senthilkumar, R. Ramadoss, "Optimized scheduling of multicore ECU architecture with bio-security CAN network using AUTOSAR," *Future Generation Computer Systems*, vol. 98, pp. 1-11, 2019.

[17] C. Shen, Y. Chen, X. Guan, *et al.*, "Pattern-growth based mining mouse-interaction behavior for an active user authentication system," *IEEE Transactions on Dependable and Secure Computing*, vol. 17, no. 2, pp. 335-349, 2020.

[18] N. Sun, J. Zhang, P. Rimba, *et al.*, "Data-driven cybersecurity incident prediction: A survey," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1744-1772, 2019.

[19] D. Wang, T. Muller, J. Zhang, *et al.*, "Information theoretical analysis of unfair rating attacks under subjectivity," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 816-828, 2020.

[20] Y. Xiao, Z. J. Fan, A. Nayak, *et al.*, "Discovery method for distributed denial-of-service attack behavior in SDNs using a feature-pattern graph model," *Frontiers of Information Technology & Electronic Engineering*, vol. 20, no. 9, pp. 1195-1208, 2019.

[21] B. Yang, W. Bao, Y. Chen, "Time series prediction based on complex-valued S-system model," *Complexity*, vol. 24, pp. 1-13, 2020.

[22] J. Zhang, Y. Chen, Y. Zhai, "Zero-shot classification based on word vector enhancement and distance metric learning," *IEEE Access*, vol. 99, pp. 1-1, 2020.

[23] L. Zhu, "Safety detection algorithm in sensor network based on ant colony optimization with improved multiple clustering algorithms," *Safety Science*, vol. 118, pp. 96-102, 2019.

Biography

Yunxue Yang was born in 1986. She received the B.S. in computer science from Qufu Normal University, China, in 2007 and M.S. in computer and information science from Nanjing University of Information Science & Technology, China, in 2011. She is currently a lecturer of the Department of Computer Science and Technology, Silicon Lake College, Kunshan, China. Her current research interests include network security, cryptography and information security.

Zhenqi Yang received his B.S. in Fundamental Mathematics from Qufu Normal University, China, in 1983 and M.S. in Applied Mathematics from Chinese Academy of Sciences, China, in 1988. He is current a professor at the department of Internet of Things, Binjiang College of Nanjing University of Information Science, China. His current research interests include information security, cryptography and mobile communications.

Qin Yang received her B.S. in Computer and Information Sciences from Wuhan University, Wuhan, China, in 2006 and M.S. in industrial engineering from Southeast University, China, in 2014. She is current an associate professor at the department of Computer Science and Technology, Silicon Lake College, Kunshan, China. Her current research interests include The Internet of Things and information security.

Guohua Ji received his B.S. in Computer and Information Sciences from Shanghai Normal University, Shanghai, China, in 2003. He is current an associate professor at the department of Computer Science and Technology, Silicon Lake College, Kunshan, China. His current research interests include information security and software security.

Shengjun Xue received his Ph.D. degree in computer science and information engineering at the Zhejiang University, China. Later on, he worked at Indiana University-Purdue University Indianapolis as a post-doctoral fellow. Then, he worked at Wuhan University of Technology, China, in 2000. He now is a distinguished professor at the department of Computer Science and Technology, Silicon Lake College, Kunshan, China. His current research interests include big data and cloud computing.