A Network Information Security Risk Assessment Method Based on Cloud Model

Chuntao Li¹, Jing Nie²*, Fan Lin³, Xi Wang⁴

¹Xiamen Nanyang College, Xiamen 361000, Fujian, China;
²Xiamen Institute of Software Technology, Xiamen 361000, Fujian, China;
³Software School, Xiamen University, Xiamen 361000, Fujian, China;
⁴School of Information Science and Engineering, Xiamen University, Xiamen 361000, Fujian, China

Abstract

As an information security technology that can make the system more secure and robust, network security assessment not only can integrate various security assessment elements such as information assets, vulnerability and threats, but also can help users actively identify potential security threats that the system is encountering. Current network security assessment theories and methods require large amount of historical data to conduct statistics analysis or machine learning. Besides, the means of network threats change with each passing day, which implies that new network security assessment theories and methods should be formed by considering from network information's own characteristics and finding out its behavior patterns of vulnerability and threats. Cloud model is an uncertainty analysis method, which can be used for the grading of network security status. Based on access graph model, this paper proposed the assessment method based on threat event occurrence probability and the assessment method based on information assets, and calculate the integrated security value of network information system. Then, the paper combined the network security assessment value with cloud model, obtained the eigenvalue of the cloud model after sampling and calculation, and established a certain cloud model. At last, the paper took the random sampling value as the input of the cloud model, and confirm the network security grade after judging the cloud model.

Keywords: cloud model, network information security risk assessment, access graph model, backward cloud generator

1. INTRODUCTION

Under a distributed environment, network security mainly provides security protection for information carrier and the information. The main operations of the protection include transmission, storage and access of data, prevention of data, information or ability being used or revised unauthorized, as well as refusal of services (William, 2005). With the development of internet, the transmission of information became more and more fast and variable, which exerted profound influences on economics, politics, science and education as well as the society of the whole world. In the 21st century when the security of information matters the stability of a country and the society (Fred, 1985), network security became one of the important factors that affect the global strategic
deployment and social economic development, which also turned into a cutting-edge research area in the information

Among all the stages that network security has experienced, the main three stages include (ITSEC, 1991): The first stage mainly assure a relatively secure computer system by establishing a Fortress Model (May, 1998). The second stage mainly realize the Information Assurance by adopting real-time monitoring technology to detect network attacking behaviors (Wiggins, 2006). In the third stage, researchers started to consider the survivability and robustness of network. The security assessment technology mainly concerns the assessment from the product security to the micro system security. The Trusted Computer System Evaluation Criteria (TCSEC) (Schneier and Sehneier, 2000) was raised mainly to assess the confidentiality of different computer systems; the Information Technology Security Evaluation Criteria (ITSEC) (Andrew and Moor, 2001; Dacier et al., 1996; Dacier, 1994) was raised mainly to assess the information security of multiple security products; the Evaluation Criteria for Information Technology Security (Common Criteria/CC) is to assess the information security of different security products under a more open environment than that of ITSEC. Various types of analysis assessments such as threat analysis and vulnerability analysis can be realized by strengthening risk tolerance (Ortalo and Deswarte, 1997). In literature (Ortalo et al., 1999), Shen Changxiang pointed out that, on the basis of a complete information security lifespan of PDRR model, grade protection, risk assessment, emergency treatment and disaster recovery are the four main parts of establishing the information security assurance system.

In Literature (Phillips et al., 1998) and Literature (Thomas, 2001), Feng Huiping et al. proposed the method of calculating the cost—Expectation of Exploitation cost (EEC) that attackers used in realizing their targets through the vulnerability of the system. This paper would introduce the method into the concept of reliability principle, and construct the function relations between the occurrence probability of the threat event, the attacking complexity of vulnerability, as well as the attacking ability of the attackers. Reliability principle used to be a traditional theory that was used to evaluate the reliability of elements products. Owing to the full considerations on the network vulnerability (security vulnerability) and power of attackers, the results of the calculation may be more accurate and objective.

2. NETWORK SECURITY RISK ASSESSMENT BASED ON ACCESS GRAPH MODEL

Currently used risk assessment methods usually take the impacts of a certain threat event on the information security properties as the loss of the information assets caused by this event (John and John, 2000; Jack, 1994). Lacking of a unified theoretic rule, it is hard to judge the influences on the information assets by this event through the assessment tool automatically. Manual intervention is usually required. The introduction of safety strategy of network information system can enable that the harm grade (damage degree on information assets) on the security properties of information assets by the safety event can be measured by different degrees of violating security strategies. This means that, for each security strategy, after the damages on the information assets by different violation degrees were predefined, the information assets damage by the threat event can be measured subjectively and accurately through the violation degree on the safety strategy of the threat event (Anselm, 2006; Ye et al., 2006; Ye et al., 2006). This method not only solved the subjective and automatic assessment on information assets damages, but also can treat the internal (inequitable conducts by internal personnel) and external (attacks by external illegal attackers) threat events in a unified way. Access graph model can provide such a technological basis, which is also the basic concept of assessing the information assets loss caused by the threat events of safety strategy.
All the safety strategies of a network system can be expressed by the set \( P \),
\[ P = \{ p_0, p_1, p_2, \ldots, p_z \} = \{ p_j | h_{vb}, o_j, h_{vb}, o_j, \text{precon}, \text{access} \}, \]
which means a tetrad can define a safety strategy. That is to say, if the user can satisfy the condition “precon”, then
the condition of the user accessing the targeted element from the original element is in accordance with the security strategy. The security can be used to check whether a certain side in the access graph is a threat event that violates the security strategy.

The process of the assessment algorithm of information assets loss caused by threat event which is based on the access graph and safety strategy is shown as following:

(1) Establish the sample set for all the samples violating the security strategy

Based on the security strategy set \( P = \{ p_0, p_1, p_2, \ldots, p_z \} = \{ p_j | h_{vb}, o_j, h_{vb}, o_j, \text{precon}, \text{access} \} \), the paper established a threat event sample set for all the samples violating the security strategy, which is also the complementary set of \( P \):
\[ P = \{ \text{ep}_\text{abj} | \text{No}, \text{Eff}, h_{vb}, o_j, h_{vb}, o_j, \text{precon}, \text{access} \}, \]
where \( \text{ep}_\text{abj} \) stands for the access relationship between the samples violating the security strategy between element \( h_{vb}, o_j \), \( h_{vb}, o_j \); \( \text{Eff} \) refers to the loss of the information assets \( h_{vb}, o_j \) managed by the target element \( h_{vb}, o_j \) due to the threat event of a sample violating safety strategy. The value of \( \text{Eff} \) is ranged from 0 to 1; \( h_{vb}, o_j, A \times \text{Eff} \) means the loss of the information assets \( h_{vb}, o_j, A \) caused by the threat event satisfying the sample; \( \text{No} \) stands for the numbering of the samples, which is designed to distinguish different samples that violated the security strategy between element \( h_{vb}, o_j \) and element \( h_{vb}, o_j \).

(2) Identification of threat event: confirm all the sides that violated the security strategy in the access graph.

In a certain network system, if the resulting access graph is \( \text{AG}(N, E) \), and the sample set that violated the security strategy of the network system is \( \tilde{P} \), then \( \tilde{P} \cap E \) can be used to represent all the sides that violated the security strategy in the access graph \( \text{AG}(N, E) \), which means the set of all the current threat events in the network system.

(3) Assess the loss of the information assets caused by a certain threat event

For any side that belongs to set, which also means a threat event, the loss of the information assets caused by the threat event can be assessed by Formula (1):

\[
\text{Loss of information assets} = h_{vb}, o_j, A \times (\text{ep}_\text{abj}^{\text{No}}, \text{Eff})
\]

\[ \forall e_{\text{abj}} \in \tilde{P} \cap E, \text{ep}_\text{abj}^{\text{No}} \] is matched to \( e_{\text{abj}} \)

3. RESEARCH ON THE NETWORK INTEGRATED RISK ANALYSIS AND ASSESS ALGORITHM

Traditional method usually sums up the risks of the isolated weaknesses to be the integrated risk of the network system. In the threat environment constructed based on network security model, the global risks brought by single weaknesses through a high-level interaction in the network system were fully considered. Hence, the integrated risk analysis and assessment of the network can be conducted by the method of combining reductionism and holism according to ALE theory (Saaty, 1980). According to reductionism: the total risks of all the elements formed by the combined effect of several
threat events were the integrated reflection of the risks of each threat event acted on each element; then, based on the holism theory, the combined probability and integrated risks of each element were calculated according to the probability distribution of each threat event (Ahti and Raimo, 1997; MustafaMA, 1991); after that, the integrated risks of the host nodes can be calculated by weighted sum of all the element risks on the nodes. Similarly, the integrated risk of the total network can be obtained.

Superstition was with me at that moment; but it was not yet her hour for complete victory: my blood was still warm; the mood of the revolted slave was still bracing me with its bitter vigour; I had to stem a rapid rush of retrospective thought before I quailed to the dismal present.

With the above achievements of the assessment algorithm of threat event probability based on reliability theory and the assessment algorithm of information assets losses caused by threat events of safety strategy, as well as the resulting access graph centered on elements, the integrated risk analysis and assessment algorithm of the target network can be obtained. The specific steps include:

1. Calculate the risk values of each element $h_{h_o}o_j$:

$$h_{h_o}o_j,R = h_{h_o}o_j,A \times \left( \sum_{a} (e_{p_{No}}^{a_{ibj}}.Eff \times p(e_{aibj})) \right)$$

(2)

Where, the calculation of each is conducted with the assessment algorithm (Formula (2)) which is based on the threat event probability of reliability principle:

$$h_{h_o}R = \sum_{j=1}^{j=|h_o|} h_{h_o}o_j .R$$

(3)

2. Calculate the integrated risk value of the network

$$R(H) = \sum_{h=1}^{h=|H|} h_{h_o}W \times h_{h_o} .R$$

(4)

Except for the calculation of the integrated risk values of the network information system as well as the comprehension of current status of the system, the most vulnerable part of the system needs to be identified. The timely fixes on bugs will be very helpful in promoting the security of the whole system. Hence, we proposed the Severity of Vuls (H, A) algorithm, trying to find such vulnerable parts, as shown in Algorithm 1. As shown, for the $meansSeq$ properties of the sides $e_{aibj} \in P \cap E$ of all the threat events in the resulting access graph AG(N,E), all the appeared $means$ relative properties se were accumulated. After checking the values of the “se” properties of each weakness, the weakness with the most sides $e_{aibj}$ of threat event in the resulting access graph AG(N,E), which is the also the weakness that requires the most urgent fix. As the algorithm has a relative low time calculation complexity, we can re-operate the access graph algorithm after eliminating the weakness that requires the most urgent fix.

Severity of Vuls (H, A):

**Input:** the set of hosts of network $H=\{h_0,h_1,h_2,...,h_z\}$, the resulting access graph AG
Output: \( H = \{ h_0, h_1, h_2, \ldots, h_z \} \) with the resulting severities of each vulnerability

For each \( e_{aibj} \in P \cap E \)

For each element \( el \) in \( e_{aibj}.meansSeq \)

// is the times of the bugs appeared in the method sequences during the calculation

\[
\text{If (el is vulnerability) } \{ \\
\quad \text{el.se = el.se + 1} \\
\}
\]

Then, this paper conducted the case analysis in respect to the small-scale network information system shown in Fig. 1. There are three hosts in this network information system: a Web Server (W,W,W=0.8); a file server (F,F,W=0.8), and a Data Base Server (D,D,W=0.9); Host (A) refers to the machine that is being attacked.

**Table 1** Trust relationship between the elements

<table>
<thead>
<tr>
<th>ID</th>
<th>Precon(ditions)</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>sAccess</td>
<td>dAccess</td>
</tr>
<tr>
<td>W.www.t1</td>
<td>Any.os.user</td>
<td>---</td>
</tr>
<tr>
<td>F.ftp.t1</td>
<td>Any.os.user</td>
<td>---</td>
</tr>
<tr>
<td>F.ftp.t2</td>
<td>W.os.user</td>
<td>---</td>
</tr>
<tr>
<td>D.oracle.t1</td>
<td>W.os.user</td>
<td>---</td>
</tr>
<tr>
<td>D.oracle.t2</td>
<td>F.os.user</td>
<td>---</td>
</tr>
<tr>
<td>---</td>
<td>other</td>
<td>other</td>
</tr>
</tbody>
</table>

The trust relationship between the elements is shown as Table 1. Besides, weakness exists in each element of the machine (as shown in Table 2). After penetrated successfully with these weaknesses, the access rights of the attackers were also shown in Table 2. To put it straightforward, in the access graph, the names that can reflect the host functions and related elements were used as the node identity. For example, D.oracle refers to the oracle element on the data base server, and D.os refers to the operation system element on the data base server.

**Table 2** Weaknesses and penetration templates on the elements

<table>
<thead>
<tr>
<th>ID</th>
<th>Vulnerability</th>
<th>Precon(ditions)</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Name</td>
<td>sAccess</td>
<td>dAccess</td>
</tr>
<tr>
<td>W.www.v1</td>
<td>Apache</td>
<td>5033</td>
<td>Remote.os. user</td>
</tr>
<tr>
<td></td>
<td>Chunked</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>W.www.v2</td>
<td>Wu-Ftpd</td>
<td>8668</td>
<td>Remote.os. user</td>
</tr>
<tr>
<td></td>
<td>Socketprintf()</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
After obtaining the trust relationship between the elements and the weakness information on the element, further calculations were conducted according to Algorithm 1, the produced access graph is shown as Fig. 1.

**Figure 1 The produced access graph**

### 4. RANKING PROCEDURE OF NETWORK INFORMATION SYSTEM RISKS

(1) The network information system risks were divided into four levels (High, Relatively high, Relatively low, Low). Each level corresponds to a concept cloud, and the corresponding system security properties are: Low, Relatively low, Relatively high, High.

#### Table 3 Definition of risk level

<table>
<thead>
<tr>
<th>Risk level</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>The risk level of the network is very high; a lot of bugs existed in the network, and urgent measures need to be taken.</td>
</tr>
<tr>
<td>Relatively high</td>
<td>The risk level of the network is relatively high, and certain measures need to be taken to further promote the security performances.</td>
</tr>
<tr>
<td>Relatively low</td>
<td>The risk level of the network is relatively low, and certain measures can be taken to further promote the security performances.</td>
</tr>
<tr>
<td>Low</td>
<td>The risk level of the network is very low; no actions are required.</td>
</tr>
</tbody>
</table>

(2) Take samples from the network integrated risk values, classify the collected data qualitatively, calculate the variable digital characteristics of each level successively.
through the reverse normal cloud generator algorithm, and give out the four concept clouds (High, Relatively high, Relatively low, Low). The reverse normal cloud generator algorithm will be specifically introduced in Part 5.

(3) Put the four concept clouds in the same coordinate system to construct the cloud scale.

(4) Cloud strategy. Take samples from the integrated risk values of the current network information system, take the collected data as the input of each concept cloud for assessment, and calculate the membership degree of the sampling values of each concept cloud. Then, use the maximum membership degree selector to select the concept cloud of the maximum membership degree, and get the qualitative evaluation output of the object, which is one of the risk levels (High, Relatively high, Relatively low, Low) of the current network information system.

5. BUILDING THE BACKWARD CLOUD GENERATOR

This paper raised an improved reverse normal cloud generator algorithm (Algorithm 1) with uncertain membership degrees to calculate the digital characteristics of the cloud. This algorithm made some improvements compared with previous two reverse normal cloud algorithms (Fatih, 2006). When hyper-entropy $H_e$ is larger than entropy $E_n$, the algorithm can solve the problem of large error of the point estimation between entropy and hyper-entropy. In addition, the algorithm is simple and accurate, which can be easily promoted for high dimension.

Input: sample point $R_i$, where $i=1,2,3,...,n$; $R$ refers to the n data of the collected integrated risk values of the network information system under different circumstances.

Output: reflection of the digital characteristics on the integrated risk value $R$ of the network information system ($E_x$, $E_n$, $H_e$).

Steps of the algorithm:

1. According to $R_i$, calculate the sample average $\bar{R} = \frac{1}{n} \sum_{i=1}^{n} R_i$ of the data group, the first-order sample absolute central moment $\frac{1}{n} \sum_{i=1}^{n} |R_i - \bar{R}|$, and the sample variance $s^2 = \frac{1}{n} \sum_{i=1}^{n} (R_i - \bar{R})^2$;

2. $E_x = R$,

3. $E_n = (R - s^2 \frac{1}{2})^2$,

4. $H_e = (R - s^2 \frac{1}{2})^2$

Algorithm 2 Improved reverse normal cloud generator algorithm.

Certainly, the parameters selected when constructing “High” cloud are the integrated risk values of the system when the risk level of the network information system was
characterized as the “High” risk level, while the parameters selected when constructing “Low” cloud are the integrated risk values of the system when the risk level of the network information system was characterized as the “Low” risk level. But the two clouds used the same constructing algorithm (Ido and William, 2002).

Ideally, the intersections between “High” concept cloud and “Low” concept cloud showed that the two concepts have covered the whole state space. However, considering the risks and security performances of network information system, it is not appropriate to divide the state into only “High” and “Low”. Hence, this model further classified the uncovered areas between the two concept clouds, and generated four-dimension concept clouds (High, Relatively high, Relatively low, Low), aiming to better qualitatively describe the risks and security performances of the network information system.

The model equally divided the area between the centroid Ex4 of the “High” concept cloud and the centroid Ex1 of the “Low” concept cloud into “Relatively high” concept cloud and “Relatively low” concept cloud. In the discourse domain, the cloud droplets that have contributions to the concepts were mainly located at the interval $[Ex-3En, Ex+3En]$ interval (Dennis and Daniel, 1995). In this model, based on the cloud production method with the golden ratio, preset the smaller entropy or hyper-entropy of the neighboring cloud 0.618 times of the larger, and calculate Ex3 (Relatively high) and Ex2 (Relatively low). The calculation formula is shown as following:

$$Ex3 = Ex4 - 3 \times 0.618 \times En4$$

$$Ex2 = Ex1 + 3 \times 0.618 \times En1$$

After this process, a four-dimension concept cloud (High, Relatively high, Relatively low, Low) was formed as Fig. 2.

![Figure 2 Diagram of concept cloud](image)

6. EXPERIMENTS

The algorithm was realized through the programing tool of MATLAB2010 under Windows 7 operation system. The specific procedure is shown as following:

(1) For the system parameters, the integrated risk values $R$ of the network information system were collected 10 times; then the reverse normal cloud generator algorithm (Algorithm 2) was used to draw the system state cloud to get the digital characteristics:
cloud_{High} (Ex,En,He) = (52,12,6), cloud_{Relatively high} (Ex,En,He) =(29,9,2) \\
cloud_{Relatively low} (Ex,En,He) = (12,4,2), cloud_{Low} (Ex,En,He) = (6,3,1) \\

(2) Establish a cloud scale according to the obtained results, and form a (High, Relatively high, Relatively low, Low) state cloud set (as shown in Fig.3)

(3) After inputting the current integrated risk values of the network information system, assess the current risk levels of the network. Table 4 showed the membership degree of several sampling points to each concept cloud. Table 5 presented the assessment results of these sampling points.

**Table 4** Membership degree of sampling values to the concept clouds

<table>
<thead>
<tr>
<th>Sampling value</th>
<th>cloud_{High}</th>
<th>cloud_{Relatively high}</th>
<th>cloud_{Relatively low}</th>
<th>cloud_{Low}</th>
</tr>
</thead>
<tbody>
<tr>
<td>60.2</td>
<td>0.81315525</td>
<td>0.00245681</td>
<td>0.00000000</td>
<td>0.00000000</td>
</tr>
<tr>
<td>35.5</td>
<td>0.38858813</td>
<td>0.77043309</td>
<td>0.00000003</td>
<td>0.00000000</td>
</tr>
<tr>
<td>15.8</td>
<td>0.01056574</td>
<td>0.34110820</td>
<td>0.63683161</td>
<td>0.00481723</td>
</tr>
<tr>
<td>2.2</td>
<td>0.00018205</td>
<td>0.01187189</td>
<td>0.04972487</td>
<td>0.44833158</td>
</tr>
</tbody>
</table>

**Table 5** Assessment results of risk levels of network information system

<table>
<thead>
<tr>
<th>Sampling value</th>
<th>Network integrated risk value</th>
<th>Cloud characteristics (Ex,En,He)</th>
<th>Assessment results</th>
</tr>
</thead>
<tbody>
<tr>
<td>60.2</td>
<td>52,12,6</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>35.5</td>
<td>29,9,2</td>
<td>Relatively high</td>
<td></td>
</tr>
<tr>
<td>15.8</td>
<td>12,4,2</td>
<td>Relatively low</td>
<td></td>
</tr>
<tr>
<td>2.2</td>
<td>6,3,1</td>
<td>Low</td>
<td></td>
</tr>
</tbody>
</table>

The results showed that this model can preferably assess the current risk levels of the network information system and provide a reliable basis to take proper measures. The assessment results are in line with our common thought: the higher the integrated risk...
value, the higher the network security risk level will be; the lower the integrated risk value, the lower the network security risk level will be. This showed that the assessment result has a certain reference value.

Traditional network security risk assessment method would compare historical data, learn from historical experience, and conduct a detailed and all-around study and analysis on the historical data, then make an integral assessment on the state of the whole network to have some knowledge of the security performances of the network, and make a qualitative judgement on the risk level of the network security. However, there is a huge defect of the traditional network security assessment method. When we want to know the network state and make an integral analysis on the network, we need to implement artificially all along according to historical experience or historical data. This kind of assessment process requires a huge amount of labor forces, and expenses especially when inviting experienced experts to conduct the assessment for the school, enterprise or the government.

However, the cloud-model-based method of judging network security risk levels introduced in this paper only needs to conduct the qualitative method and quantitative calculation simultaneously to confirm the quantitative characteristics of qualitative concept and qualitative levels. In the following assessment, it only needs to calculate the integrated values of the network security risks according to the process stated in Part III, and input the values into the confirmed cloud model to get the judgement of a qualitative level. Compared with traditional artificial analysis, this method has better efficiency.

7. CONCLUSION

the current assessment theories and methods of network security risks, historical materials are playing an important role. The whole assessment process requires a detailed study on historical materials, and the assessment results also depend on the skills of the assessor to some extent. However, network information change with each passing day with new threats and new bugs emerging continuously. The traditional way of thinking can no longer keep up with the pace. In addition, the skills of the assessor also need to be improved to gain better assessment results. Hence, under the new environment, the assessment on network security risks needs to be re-examined.

The assessment of judging the level of the network security according to historical experience is a qualitative approach. However, there is no more artificial participation in the process of automatic assessment. Instead, quantitative calculation will be conducted, which needs to be integrated with the qualitative concepts and qualitative levels. With respect to the defects of current assessment model of network security risks, this paper mainly adopted cloud model to solve the problem of qualitative and quantitative transformation. First, the paper conducted the network modeling and constructed the access graph model. Secondly, based on the access graph model, the paper assessed the threat events occurrence probability and the information assets loss caused by the threat events, and then calculated the integrated risk value of the network information system. At last, the paper combined the network security risk assessment with cloud model, taking the integrated values of network security risks as the parameters of cloud model, and constructed a certain cloud model with the eigenvalue of the cloud model obtained through sampling and calculation. Then, the paper used the random sampling values as the input of the cloud model, and conformed the network security risk levels after judging with cloud model.
8. REFERENCES