Research on Information System Risk Analysis and Security Situation Assessment Method

Sheng Wang¹,a, LinHao Zhang¹,b, Jie Zhang¹,c, Yong Tang¹,d, YunHui Liang¹,e

¹Electric Power Research Institute of State Grid Sichuan Electric Power Company, ChengDu, SiChuan, 610000, China

a Wangs5813@sc.sgcc.com.cn; b Zhanglh9317@sc.sgcc.com.cn, c* Corresponding author: Zhangj6459@sc.sgcc.com.cn, d Tangy1593@sc.sgcc.com.cn, e Lianghh2115@sc.sgcc.com.cn

Abstract—Enterprise information system is the fundamental guarantee and important means of enterprise production and management, the security of the information system is the foundation of the stable and reliable operation of the information system. In order to improve the security and anti-risk ability of the information system, it analyzes the possible risks of the information system and gives an assessment of the security situation of the information system. When there is a risk, it will provide security situation assessment and early warning to avoid unnecessary losses and risks.

1. INTRODUCTION

The research of information system risk analysis and security situation assessment methods has always been an important research direction of network security situation research, and it is the most difficult point of network security situation awareness. Risk assessment must first identify the assets, threats and vulnerabilities of the information system. Mostly, the meaning of security situation assessment refers to the real-time extraction and processing of data generated by network equipment, based on a certain prior knowledge, calculation and evaluation with the help of some mathematical models and methods, in the form of security situation value reflect the actual security status of the network. However, the complexity of information system composition makes the assessment of its risk and security situation very cumbersome. Judging from the events that have occurred in recent years, the risk analysis and evaluation system of the information system is still in the process of continuous improvement, and there are still some shortcomings.

This article combines the actual operating environment and problems of a power company's network security system, mainly from the perspectives of equipment identification, abnormal behavior detection, attack behavior detection, vulnerability detection, etc. Combining the current mainstream research methods, we analyzed the most possible risks in each aspect and quantified the risks, thus introducing the methods of information system risk analysis and security situation assessment.

2. RESEARCH STATUS OF INFORMATION SYSTEM RISK ANALYSIS AND SECURITY SITUATION ASSESSMENT METHODS

At present, domestic and foreign concerns about information system risk analysis and security situation are increasing. Abad et al. [1] comprehensively assessed the network security situation by performing correlation analysis on network security alarm data, and developed and designed a situation assessment system. The system can discover new security events, analyze untrusted hosts, and find out the source
of attacks. Chen Liandong et al. [2] proposed a set of data fusion, network situation assessment and prediction models suitable for large-scale and complex power information networks based on power systems. First hierarchies the risk assessment of the power information system, and then integrate various data merging and mapping transformations to calculate the risk value of the entire information system. Fu Yu et al. [3] proposed a comprehensive information system security risk assessment model. It based on the entropy weight coefficient method, which uses the entropy weight coefficient method to determine the index weight vector and reduces the subjective influence of expert experience, and uses the idea of system integration to integrate the security risk value of each element, and then determine the security risk level of the information system. Xi Rongrong et al. [4] proposed an improved quantitative assessment model of network security situation, and improved the network security situation assessment model based on hidden Markov process proposed by Arnes. Based on the statistical characteristics of the alarm, the concept of alarm quality is proposed, and the observation vector obtained by the alarm quality is using to improve the effectiveness of the data source and the game process based on security events and protective measures. A method to determine the state transition matrix is proposed combined with the success of the attack. The probability of correcting is to increase the effectiveness of the transition matrix. Based on the original fuzzy analytic hierarchy process, Yang Linhui et al. [5] designed an improved network situation assessment model, which solved the current lack of attention to the characteristics of data distribution, greatly reduced the deviation, and made the assessment result more Accurate and objective. Wang Kun et al. [6] proposed a network security situation assessment method based on attack pattern recognition, which first fused the multi-source data in the network, then analyzed the result of the fusion, and then identified the attack intention and the current attack stage. The attack stage is using as a situation element for node assessment to obtain the security situation of the entire network. Finally, construct the state transition diagram of the attack stage, and combine the vulnerability and configuration information of the host to realize the prediction of the network security situation.

3. INFORMATION SYSTEM RISK ANALYSIS AND SECURITY SITUATION ASSESSMENT METHODS

At present, there are many research results on security situation assessment methods, which can be summarized into the following types:

According to the assessment focus, it can be divided into risk assessment and threat assessment.

According to the real-time evaluation, it can be divided into static evaluation and dynamic evaluation.

According to the form of evaluation, it can be divided into qualitative evaluation and quantitative evaluation, which is also a distinction, based on the attributes of information system security situation indicators.

According to the theoretical and technical basis of the assessment basis, it can be divided into three categories, namely based on mathematical models, based on probability and knowledge reasoning, and based on pattern classification.

Here we use a mathematical model-based method: Analytic Hierarchy Process to show the basic ideas of information system risk analysis and security situation assessment.

AHP is a decision-making method, which decomposes all elements related to decision-making into goals, standards and plans, and then conducts qualitative and quantitative analysis on this basis. In the information system risk analysis and security status assessment, the steps to determine the weight of the security status assessment are as follows:

1) Establish a structural model of the problem to be solved in accordance with the hierarchical approach of the highest layer (Target layer), the middle layer (Specification layer) and the lowest layer (Scheme layer). Among them, the highest level is the problem, which needs to be solved; the middle level is the factors and criteria that affect the problem; the lowest level is the most alternative for making decisions.
2) Construct judgment matrices at all levels. The factors and criteria in the middle layer are different in measuring their influence on the target problem. We compare the two factors with each other and quantify their importance in the form of a scale as Table 1:

| scale | Meaning (the factor i and the factor j) |
|-------|-----------------------------------------|
| 1     | factor i is as important as Factor j     |
| 3     | factor i is slightly more important than factor j |
| 5     | factor i is obviously more important than factor j |
| 7     | factor i is more important than factor j  |
| 9     | factor i is extremely important compared to factor j |
| 2,4,6,8 | Between the above two adjacent judgments |

To define the judgment matrix \( A = (a_{ij})_{nn} \) among them \( a_{ij} \) is the result of comparing factor i with factor j, and there is: \( a_{ij} = \frac{1}{a_{ji}} \).

3) Hierarchical order and its consistency check. After calculating the eigenvector of its maximum eigenvalue according to the judgment matrix, the consistency check of the result is still needed for us. Now, we use the consistency check formula to judge it:

\[
CI = \frac{\lambda_{max} - n}{n - 1}
\]

On this basis, we introduce a new parameter, which is called as Random one-time indicator: \( RI \)

\[
RI = \frac{\lambda_{max} - n}{n - 1}
\]

Check up the table method we can also be obtained RI, and the symbol n is the order of the judgment matrix, as the show of Table 2:

| n   | 1   | 2   | 3   | 4   | 5   | 6   | 7   | 8   | 9   |
|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| RI  | 0   | 0   | 0.58 | 0.90 | 1.12 | 1.24 | 1.32 | 1.41 | 1.45 |

After that, in order to ensure that the consistency test is not affected by random causes, it is still necessary to compare \( CI \) and \( RI \) to obtain the consistency ratio \( CR \).

\[
CR = \frac{CI}{RI}
\]

In the case of \( CR < 0.1 \), it can be confirmed that the consistency of the judgment matrix is acceptable, and the eigenvector calculated in the previous period is the final calculation result. Here we specifically give the formula for calculating the weight \( W \) vector using the eigenvector method as follow:

\[
AW = \lambda_{max} W
\]

At the last, we just need to normalize the calculated \( W \).

4. INFORMATION SYSTEM RISK ANALYSIS AND REALIZATION OF SECURITY SITUATION ASSESSMENT METHODS

Now, take a company as an example, we introduce some influencing factors that will appear in each part through the actual processing process of the following aspects. Some specific factors are listed in Table 3.

1) The first is to use active and passive information collection technology to collect device IP/MAC information, routing information, identity information, host name, operating system, location information, traffic information, etc. Based on device portrait technology, intelligently identify network topology, device type, device manufacturer, device status (new device/online device/offline device),
device security status (safe, safer, unsafe), connection relationship between devices, etc. In addition, there is also the identification of mainstream equipment types and manufacturers such as PC equipment, network equipment, mobile equipment, IoT equipment (including video terminals, etc.), ICS equipment, etc…

2) Then consider the detection and analysis of aggressive behavior. Detect the connection behavior between the device and C&C; detect DOS attacks on SMTP/MYSQL/RDP/DNS/HTTP protocols; detect brute force attacks on RDP/SSH/FTP protocols; detect ransomware, zombies Detection of attacks on networks, worms, Trojan horses.

3) After that, consider the detection and analysis of abnormal behavior. First, detect whether device counterfeiting occurs based on the type of device, IP/MAC address, behavior, etc.; it can automatically learn and recognize the normal network access behavior of the user device based on the unsupervised learning method, and also realize the learning of user network traffic Features, when sudden abnormal traffic occurs, it can also react quickly.

4) Finally, consider the detection and analysis of vulnerability. The first is to check the weak passwords of applications such as Web/SSH/TELNET/FTP in real time. Users can check the weak passwords of the system by importing their own account and password dictionary. The second is vulnerability detection, which finds vulnerabilities in terminals and servers. In addition, check the patch installation status; find the patch repair status of the terminal, server, etc.

| TYPES | INFLUENCING FACTORS |
|-------|----------------------|
| Hardware equipment | Device status (new device/online device/offline device) |
| | Connection relationship between devices |
| | Device location |
| | IP/MAC information of the device |
| Aggressive behavior | C&C attack |
| | DOS attacks on SMTP/MYSQL/RDP/DNS/HTTP protocols |
| | Network scanning behavior |
| | Brute force cracking attacks on protocols such as RDP/SSH/FTP |
| | Ordinary or super administrator authority cracking attack |
| | Malware attack |
| Abnormal behavior | Counterfeit equipment |
| | Abnormal connection |
| | Exception protocol |
| | Abnormal flow |
| | Abnormal online time |
| Vulnerability | Weak password |
| | Vulnerabilities in terminals, servers, etc. |
| | Patch repair status of terminals, servers, etc. |

Through the above parts, the risk analysis and situation assessment of the information system are refined with equipment status assessment, attack behavior assessment, abnormal behavior assessment, and system vulnerability assessment. Moreover, use various influencing factors as evaluation factors, in this way: we can also draw a basic hierarchical structure model.

The judgment matrix A of information system risk analysis and security situation is the target layer (that is, the highest layer); in the criterion layer (that is, the middle layer) of the model, we calculate the judgment matrix B1 B2 B3 B4 from the four perspectives of hardware equipment attack behavior, abnormal behavior and vulnerability. Of course, because these four judgment matrices are still affected by a large number of influencing factors, so the middle layer here also includes some parts. The device status (new device/online device/offline device); the connection relationship between the devices; C&C Attacks; DOS attacks on protocols such as SMTP/MYSQL/RDP/DNS/HTTP; device counterfeiting; abnormal connections; weak passwords and other influencing factors. At the scheme layer (ie, the bottom layer) of the model, equipment security, communication security and data security are alternatives. The specific model is shown in Figure 1:
Figure 1: The basic hierarchical structure model of information system risk analysis and security situation assessment

For example, in the type of hardware equipment, we compare the status of the equipment and the link relationship between the equipment. It can be judged that the influencing factor of the equipment status is obviously more important than the connection relationship between the two different factors and a quantitative scale can be obtained: 5. after such a comparison, the judgment matrix is obtained. Then carry out level list sorting and consistency check, and calculate the value of $CI$ and $RI$ and the eigenvector of the largest eigenvalue of the judgment matrix. Finally, compare the calculated $W$ value to judge the degree of influence of each type, and evaluate the security situation of the information. Of course, because of the seriousness of information system security requirements in real life, it is not rigorous to use the eigenvector method to obtain the weight vector $W$ and use it as an indicator to judge the security situation. We can also use geometric average method, arithmetic average method, minimum the value of $W$ is calculated by the method of two multiplications, and the consistency is checked. The value of $W$ calculated by a variety of methods can be effectively implemented for information system risk analysis and security situation assessment methods.

The last is the analysis and presentation of the situation, which is realized by risk treatment and visual management. As a post-task of the security situation assessment, risk treatment can realize active alarm and block according to the change of the calculated assessment coefficient. The main task of visual management is to display the risk status of equipment and the entire network in a qualitative or quantitative manner based on the results of equipment status evaluation, attack behavior evaluation, abnormal behavior evaluation, and system vulnerability evaluation.

5. CONCLUSION
The research of information system risk analysis and security situation assessment methods is an important direction that people have paid attention to information security in recent years, and the analytic hierarchy process is one of the more used methods. This paper uses the analytic hierarchy process to refine the risk analysis and situation assessment of the information system with equipment status assessment, attack behavior assessment, abnormal behavior assessment and system vulnerability assessment.

ACKNOWLEDGMENT
This work was supported by the State Grid SiChuan Electric Power Company of China (Project Name: Research and platform development of full flow Advanced Sustainable threat intelligent analysis technology based on deep learning).

REFERENCES
[1] ABAD C, YURCIKW. UCLog + : a security situational awareness system for incident storage, querying, and correlation [C] / / ICTSM 2006: Proceedings of the 14th International
Conference on Telecommunication Systems Modeling and Analysis. Washington, D.C. :IEEE Computer Society,2006: 316–322.

[2] Chen Liandong. Research on power industry network security situation awareness[D]. North China Electric Power University 2015.

[3] Fu Yu, Wu Xiaoping, Ye Qing et al. An Approach for Information Systems Security Risk Assessment on Fuzzy Set and Entropy Weight [J]. ACTA ELECTRONICA SINICA, 2010, 38(7): 1489-1494.

[4] Xi Rongrong, Yun Xiaochun, Zhang Yongzheng et al. An Improved Quantitative Evaluation Method for Network Security[J]. Chinese Journal of Computers, 2015, 38(4):749-758.

[5] Yang Linhui, Sun Shaohua, Sun Xiaodong. Research on improved network security assessment method based on fuzzy analytic hierarchy process[J]. Automation and Instrumentation. 2016(10):159-160.

[6] Wang Kun, Qiu Hui, Yang Haopu. Network security situation evaluation method based on attack pattern recognition[J]. Journal of Computer Applications,2016,36(1):194-198.