Research on the computer cyber security posture assessment model based on information fusion

Xin Ge

Information Office of University of Shanghai for Science and Technology, Shanghai 200093, China

Keywords: Information fusion; Computer network security; Situation assessment model

Abstract: The network is becoming an indispensable part of people's life. At the same time, the attack behavior in the network is becoming more and more intolerable. People pay more and more attention to the network security technology. In order to reduce more serious information leakage and economic losses caused by network attacks, in recent years, a variety of network security devices have been put into network protection, such as firewall, intrusion prevention system, Honeynet system, anti-virus system, data backup system, security management system and so on. Combining objective weight with subjective weight, the combination weight is optimized by sequential quadratic programming algorithm, which reduces the uncertainty of fusion. The Cyber security posture assessment model can help network security managers master the comprehensive security situation and future development trend of the network in a period of time as a whole, and provide reference for administrators to take corresponding protective measures and improve network security.

1. Introduction

At present, the computer Internet is playing an increasingly important role in all aspects of my country's politics, economy, culture, and social life [1]. With the rapid development of communication technology and computer networks, people's demand for computer networks is increasing, and computer networks are increasingly being applied to every corner of people's lives. The classic models of situation assessment mainly include the JDL model, the Endsley model, and the TimBass model. After these three classic models are proposed, subsequent research on the Cyber security posture assessment is basically based on these three classic models [2]. Alarm data analysis is the most important part of situation assessment system. Institute of computer science, Chinese Academy of Sciences and others believe that Cyber security posture assessment refers to obtaining the overall network security situation by analyzing the relationship between security data and refining and fusing them through relevant mathematical algorithms on the basis of obtaining massive network security data, The core of Cyber security posture assessment is the extraction and fusion of security data [3]. Today, with the rapid development of computer information technology, the computer information system itself has become increasingly complex and huge. However, due to the diversity, openness and interconnection of network data transmission characteristics, the security of the computer system itself has been increasingly reduced [4]. In the past, when the threat from the network was not serious, the traditional computer network security technology could well protect the security of computer information systems. However, with the gradual escalation of various attacks from the network, in order to effectively ensure the security of computer information systems in China, it is necessary to develop and apply new computer information system network security technologies. Under this background, it is of great practical significance to study the application of Cyber security posture assessment based on information fusion[5].

2. Information fusion cyber security posture assessment

2.1. Overview of cyber security posture assessment

Over the years, the application technology of the network has become wider and wider, which

  DOI: 10.25236/mmmce.2021.039

has brought great convenience to the society and the people. However, more and more network security incidents have caused more and more social and economic losses. There are two reasons for cybersecurity incidents. On the one hand, there are more and more vulnerabilities in computer hardware, operating systems, application software, and network protocols. Another aspect is: more and more automated attack tools are launched on the network. Due to the large-scale scope of security incidents, network security administrators do not have time to deal with it, and cannot understand the overall network security situation from a macro perspective. Therefore, facing a severe security situation in computer networks, network security with comprehensive analysis skills is urgently needed. The core of cyber security posture assessment is network security situation awareness. The concept of "situation awareness" originated from the study of human factors in spaceflight. Since then, situational awareness has been widely used in air traffic control, nuclear response control, military battlefields, and emergency medical dispatch. The focus of situational awareness is to understand the acquired information, such as the enemy's situation, user behavior, network behavior, network device operation, etc., and use these data to obtain statistical data, graphs and other easy-to-understand information. Understand the information. The focus of situation assessment is how to improve the accuracy of decision-making while shortening the time from information acquisition to decision-making.

2.2. Network security situation assessment based on information fusion

Computer network contains a large number of host nodes and detection devices. Different detection devices monitor and detect different aspects of the network, and they have a lot of relevance. The traditional cyber security posture assessment usually only uses a single detection alarm or log, and the single data leads to a large deviation in the assessment results. Therefore, this assessment model integrates the data of multiple detection devices to quantify attacks, vulnerabilities and services respectively. The evaluation model is shown in Figure 1.

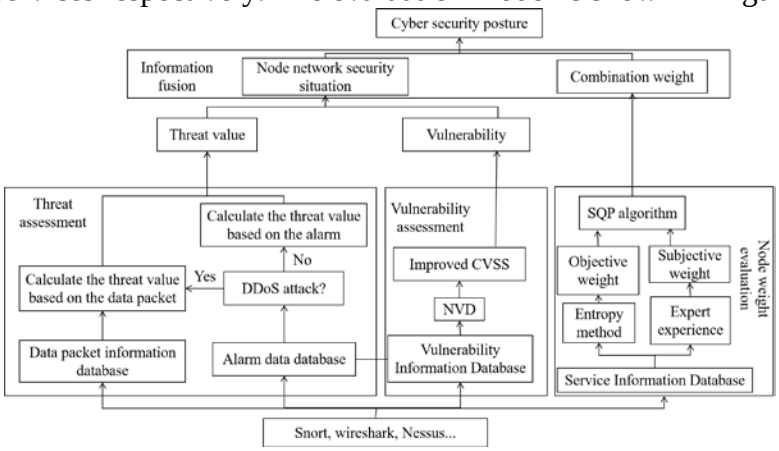

Figure 1 Information Fusion Network Security Situation Assessment Model

Threat value. It refers to the damage degree caused by different attacks to the host node, mainly explaining the influence of external attacks on the node situation, which is expressed as T(t). Vulnerability. It refers to the vulnerability degree of vulnerabilities existing in host nodes, mainly explaining the influence of internal vulnerabilities on node situation, which is expressed by V(t). Combined weights. It is a weight that takes into account the advantages of objective weight and subjective weight, and mainly describes the importance of nodes, which is expressed by w. This model starts from three aspects: external attack threat, internal vulnerability and importance of host node, and fuses the information of the three to get the current network security situation.

3. Computer Information Fusion Network Security Situation Assessment Model

Endsley is the first scholar to conduct a relatively comprehensive research on the situation assessment model. He conducted a detailed analysis and definition of situation awareness and assessment, as shown in Figure 2.

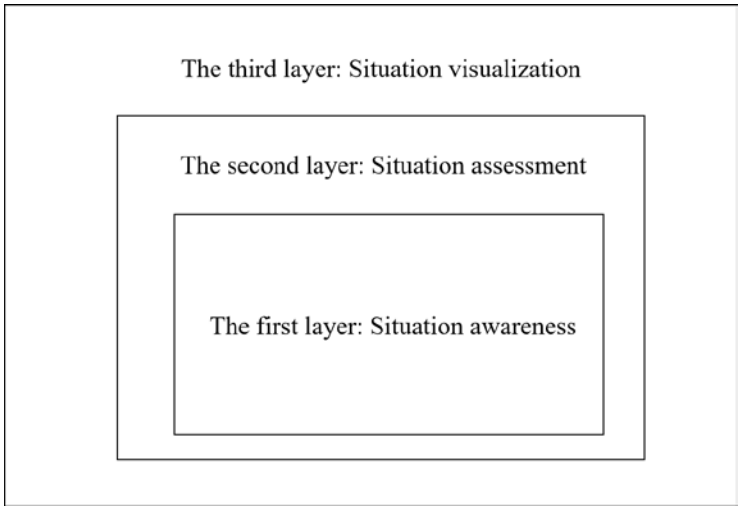

Figure 2 Hierarchical model of cyber security posture assessment

The situation assessment is summarized into three levels. The first layer is the situational awareness stage. Network security detection equipment such as intrusion prevention systems are used to obtain the attackers' attack behaviors against the network. Vulnerability scanning tools are used to scan and discover the network's own vulnerabilities and vulnerabilities, obtain important information in the network, and perform Preliminary standardization and arrangement provide support for the subsequent situation assessment and prediction. The second layer is the situation assessment stage, which integrates and analyzes the data and information detected in the situation awareness stage. The third layer is the situation visualization stage, which collects and analyzes the data of network security state obtained in the situation assessment stage, and displays the face-to-face network security situation in various forms. Network security situation assessment system can make statistical analysis of network security elements from assets, vulnerability, threat, performance and other aspects, and then synthesize these security data to obtain high-level security situation assessment results, and use time series prediction model to predict the future trend of network security situation, Help network security administrators to take appropriate security protection strategies to improve network security.

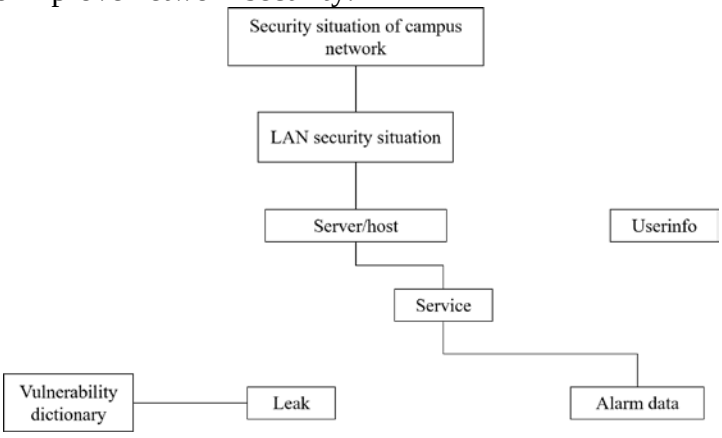

Figure 3 Database structure of cyber security posture assessment

As shown in Figure 3, the database structure of the cyber security posture assessment model is divided into eight parts, namely vulnerability database table, vulnerability table, alarm data table, service table, server/host table, LAN security situation table, campus network security situation table and user information table.

The information layer fusion of the hierarchical structure of Information Fusion Network Security Situation Assessment Model is mainly responsible for the integration of information resources of the whole model. Therefore, in the specific fusion of information layer, the relevant technical personnel need to do a good job in the establishment of vulnerability association database

and dynamic database, In order to ensure the normal function of Information Fusion Network Security Situation Assessment Model. Specifically, the establishment of vulnerability association database is due to the fact that the network security risks of computer information systems mainly come from network attacks outside their own systems, which directly indicates that the network security vulnerabilities of computing information systems have relevance, and as long as this relevance is well analyzed, a specific Information Fusion Network Security Situation Assessment Model can be built according to this relevance, which greatly improves the network security of related computer information systems. In the process of establishing the dynamic database, because the database itself analyzes the historical situation information of the computer information system network security, summarizes its future network security development trend, so as to better carry out the network security situation based on information fusion. The construction of the evaluation model ensures the network security of the computer information system.

4. Conclusions

In recent years, with the development of computer, computer network has been applied to all aspects of people's life. At the same time, network security incidents are also increasing, and the frequency is also higher and higher. With the development of the Internet, all kinds of network attacks are more and more random, which bring immeasurable economic losses and security problems to the national government, enterprises and people. At the same time, the explosive growth of cyber attacks has brought very serious cyber security threats to many areas such as services, health, culture, education, military, and politics. People are paying more and more attention to network issues. In network security defense technology, Cyber security posture assessment based on information fusion is one of the more effective technical forms. In this context, this article studies the application of cyber security posture assessment based on information fusion, hoping to promote the development of China's network security technology. Due to the complexity of the network architecture, the cyber security posture assessment technology should have both usability and practicality while accurately analyzing the overall network security situation. The application of Information Fusion Network Security Situation Assessment Model is studied, and various applications of information fusion in cyber security posture assessment model are discussed. It is found that the network is playing an increasingly important role in people's work, life and study, as well as the limitations of traditional network security technologies. Therefore, in the current cybersecurity protection of China's CIS, the cybersecurity situation assessment model based on information fusion can ensure the cybersecurity of China's CIS.

References

[1] Qi Xiaojing. Information Fusion Network Security Situation Assessment Model. Science and Technology Innovation and Application, no. 30, pp. 190-191, 2017.

[2] Meng Jing, Yang Miaosheng. Information Fusion Network Security Situation Assessment Model. Science and Technology Information, vol. 15, no. 8, pp. 18-19, 2017.

[3] Shi Zhaojun, Zhou Xiaojun, Li Ke, Wu Yue, Zhang Jianwei. Network security monitoring technology based on multi-source information fusion. Computer Engineering and Design, vol. 41, no. 12, pp. 69-75, 2020.

[4] Li Junjie. Application of Information Fusion Technology in Network Security Management. Network Security Technology and Application, no. 3, pp. 28-29, 2018.

[5] Sun Haoran, Li Runlong, Li Yijin. Computer network information security and protection in the era of big data. Flights to China, no. 19, pp. 1-2, 2019.