Protection Strategy and Assessment of Computer Network Information Security Considering Fuzzy Immune Network Algorithm

BaoQing Pu*, JunFeng Cheng

Department of Mathematics, Longnan Teachers College, Longnan, Gansu, China, 742500

*Corresponding author e-mail: wanqiu0122@163.com

Abstract. With the popularization of big data, cloud computing, mobile computing, and other new computing modes, network information technologies have gained continuous development. Large enterprises rely more and more on the convenience and benefits offered by information technology, while they have to face severe information security threats at the same time. Through analyzing the status quo of information security protection strategy, we propose an assessment method for information security in a complex network environment in this paper to guide the information security protection and provide a reference for assessing the effectiveness of network protection.

Keywords: Computer Network, Information Security, Protection Strategy; Assessment Algorithm

1. Introduction

With the continuous popularization and development of network application technology, the security situation is becoming more and more severe. In recent years, network attacks are characterized by specialization, collectivization, clear targets\(^1\), covert attack forms, and various attack modes. With the popularization of cloud computing, big data, and other computing modes, the trend of data centralization\(^2\), computing centralization, and network complexity is increasingly evident. How to ensure the confidentiality, integrity, and effectiveness of information systems in a complex network environment has become a focus of various research topics\(^5\).

Currently, with the development of data centralization, computing centralization and network complexity, the form of information security is becoming more and more serious. In the initial stage of network construction, enterprises often only consider the applicability of business but lack the overall
planning of security, which makes the network prone to security risks due to improper design, configuration, and application. Hence, how to continuously improve the information security mechanism, ensure the security of system services, ensure the stability and normality of network and infrastructure, and prevent and control the risk of information security are the key issues to be solved in companies. In this paper, how to handle new network threats is analyzed based on the current network security prevention strategies and a calculation method for assessing the effectiveness of network security in a complex network environment is proposed.

2. Assessment based on fuzzy immune network algorithm

The overall idea of fuzzy immune network algorithm is to analyze the ability of security strategies to resist attacks at all levels based on system weaknesses. Through a comprehensive assessment of systems, vulnerabilities, attacks, and security strategies, the interaction and influence between them are analyzed, and the security defense strategies are gradually evaluated from local to overall. In the design of fuzzy immune network algorithm, this paper considers the use of assessment process model, according to the topological structure, business flow, risk point, configuration, and other system information of the evaluated system, and uses modeling tools to uniformly define and model the system business, vulnerability, attack, security strategy, and other elements, so as to realize the correlation analysis among the elements, and get all possible successful network penetration. The defect of network security strategy utilizes attack data. Using the improved shortest path recognition fuzzy immune network algorithm to identify the attacker to achieve the minimum cost of the attack target, and to evaluate the priority of defense strategy against malicious attacks.

The data dictionary includes a detailed description of data items and data structures. Before describing the fuzzy immune network algorithm, the input and output permissions, risk vulnerability impact system, and risk vulnerability dictionary described in the logic process of the fuzzy immune network algorithm are established. Input/output permission dictionary data item name: input/output permission. Brief description: used to describe the weight of each level of permission. Type (length): float (2). Value: as shown in Table 1.

| Project name | Item value float (2) |
|--------------|---------------------|
| root         | 1                   |
| user         | 0.5                 |
| anonymous    | 0.25                |
| none         | 0                   |

Table 1. Values for input and output permission items

In the complex network environment, to achieve the goal, malicious attackers often approach the goal based on one or more springboards (devices). Due to the weakness of the device and the association relationship on the network, multiple weaknesses are used by malicious attackers to form a path in the network, which is the attack link. In the information construction of enterprises, we usually pay more attention to the protection of external attacks, but often ignore the attack behavior from the internal. Through the link attack, it is only required to identify a breakthrough point from the external. Subsequently, the internal weakness of the system can be used to carry out the springboard attack.
3. Protection policy for computer network information security

The independent protection effectiveness score is used to evaluate the successful utilization of a vulnerability or vulnerability in the system by the attacker, so as to realize the difficulty of the attack. It is recorded as pr. Attack path is a directed edge sequence starting from source node Z and ending at destination node D in network topology G. The success rate of attack path protection is the assessment of effective protection of an attack path in complex network environment, which is based on the equation:

\[ Pr = Pr_1 + (1-Pr_1)Pr_2 + (1-Pr_1)(1-Pr_2)Pr_3 + \ldots + (1-Pr_1)(1-Pr_2)(1-Pr_3)\ldots(1-Pr_{n-1})Pr_n \]

The independent protection effectiveness of each node is calculated. The detailed calculation process is as follows:

1) It is assumed that a node is the origin of the attacker, which can be any system or device, generally an external network attacker. It is assumed that any attacker that can obtain the input permission of the origin device is anonymous, i.e., he can view the information of the origin device or system, but cannot log in;

2) Through risk assessment, security check, and other methods to obtain the vulnerability information of the system and determine whether there is a risk vulnerability in the attacker's device. If there is a risk vulnerability, check the output permission that the attacker can obtain after exploit. If the output permission is \{user, root\}, the attack behavior may continue. Otherwise, the attack process is over.

3) Due to the risk vulnerability of the node where the attacker is located, the privilege of an attacker is enhanced. If the attacker cannot get the privilege to observe the next node (i.e., user or root privilege), the attack process is terminated, and the scope of the attacker's influence is the host or device currently viewed. If the attacker can obtain the privilege higher than anonymous by using the vulnerability, the attacker can view it Connect other nodes of, and then proceed and check whether the next node is reachable (depending on the input permission of the next system); the attacker will continue to repeat step 3 until the target node is reached or the process is terminated due to excessive cost.

4) As the attack behavior is often blocked by security devices and security policies, the time, energy, and even capital cost for the successful implementation of its attack purpose are increased. All the behavior costs paid by the attacker to achieve its attack goal are the attack cost, and the maximum attack cost it can receive is the attack cost threshold. If the protection policy of network security policy to the target area makes the cost of using any attack link greater than the attack cost threshold T, then the target area is safe; otherwise, there is an acceptable attack link, so that the attacker can enter the target area.

4. Instance calculation

If the attacker's target is server 1 and core server, it will reach the target "server 1" through firewall A and router a and reach the target "core server" through firewall a, router a, router B and intrusion detection system. Calculation equation of protection success rate based on attack path:

\[ Pr = Pr_1 + (1-Pr_1)Pr_2 + (1-Pr_1)(1-Pr_2)Pr_3 + \ldots + (1-Pr_1)(1-Pr_2)(1-Pr_3)\ldots(1-Pr_{n-1})Pr_n \]

It can be seen that the protection success rate of the two attack paths is:

\[ Pr_1 = 0.5 + (1-0.5)\times 0.5 = 0.75 \]

(1)
\[
\text{Pr} = 0.5 \times 0.5 \times 0.5 \times 0.5 \times 0.5 \times 0.5 \times 0.5 \times 0.9 = 0.9875
\]

Figure 1 describes how the fuzzy immune network algorithm affects the information security of the computer network to cooperate and protect information assets.

**Figure 1.** Protection strategy and assessment framework of computer network information security

Fuzzy immune network theory provides an interesting way to explain some social activities in organizations. The fuzzy immune network represents the attachment to the company, the commitment to the community, the involvement and the view on the importance of problematic behaviors (computer network information security protection cooperation). Fuzzy immune networks focus on individuals in groups or communities. Attachment refers to the feeling of binding a person to a person, an idea, a thing, etc. In this study, attachment is a relationship between fuzzy immune network algorithm and organizational values, which provides a functional guarantee for information assets. Commitment involves the effort and energy of fuzzy immune network algorithm to protect information, while involvement refers to the importance of information protection and the consideration of computer network information security protection policies and procedures in daily activities. The personal standard is related to the fuzzy immune network algorithm's view and view on computer network information security protection. Protecting information assets is a valuable task in an organization. Involvement refers to the energy, time and involvement that an individual spends on a subject. The involvement of customers/consumers, the involvement of a fuzzy immune network algorithm, the involvement of students, and the involvement of computer network information security protection are all examples in different fields. Sharing information protection knowledge, participating in computer network information security protection courses and workshops, paying attention to computer network information security protection news on the media, reporting computer network information security protection events to experts and complying with OISP are all examples of our computer network information security protection participating in daily activities affecting our research. The involvement of computer network information security protection has a positive impact on the awareness and knowledge of computer network information security protection of fuzzy immune network algorithm.

5. Conclusions

With the continuous expansion of the information technology application, information technology has...
promoted the production and improved efficiency as a useful tool; while in rapid development, special attention should be paid to the problem of information security. How to ensure the security of the computer network information system, the popularity of cloud computing, big data, and other computing modes has put forward new subjects and challenges to the information field. The trend of data centralization, computing centralization, and network complications has become increasingly evident. Users have higher and higher security requirements for data and privacy, and the value of data assets is growing. Information security will play an increasingly significant role in this system. Only by controlling the information security gate can we fully leverage the maximum benefits of the information system and create higher value.

References
[1] Li Shi, QiongHua Zhou, Yinghe Zhao, Yixin Ouyang, & Jilin Wang. (2017). Oxidation mechanism and protection strategy of ultrathin indium selenide: insight from theory. Journal of Physical Chemistry Letters, 8(18), 4368-4373.
[2] C. Li, G. Li, Y. Dong, W. Hu, & W. Chao. (2019). Protection strategy of current suppression resistor used in mmc-hvdc startup process. Gaodianya Jishu/High Voltage Engineering, 45(1), 39-45.
[3] Mingxin, Y., Sun'An, R., Canyang, R., & Kunpeng, R. (2010). Hybrid ant colony and immune network algorithm based on improved apf for optimal motion planning. Robotica, 28(6), 833-846.
[4] D.M. Zhao, J.X. Liu, & J.F. Ma. (2010). Risk assessment of information security based on improved wavelet neural network. Computer Science - Research and Development, 37(2), 90-93.
[5] S M Wörmann, Diakopoulos, K. N., Lesina, M., & H Algül. (2013). The immune network in pancreatic cancer development and progression. Oncogene, 33(23), 2956-2967.
[6] Wang, R., & Li, P. (2015). Research on network malicious code immune based on imbalanced support vector machines. Chinese Journal of Electronics, 24(1), 181-186.