Research on Computer Network Security Analysis Modeling Based on Artificial Intelligence Technology

Huang Yan
College Of Science & Arts Of Jianghan University, Hubei, Wuhan, 432200, China

Abstract. With the development of network technology, network is more and more closely related to people's lives. Network security has been paid more and more attention, and the research on network security has gradually been put on the agenda. The main purpose of computer network security research is to extract the system data and factors related to computer network security and establish a model to analyze computer network security. Computer security concerns people's vital interests. Now, hacker attacks and virus intrusions often occur, which threaten people's privacy and security. The research work of security analysis needs to extract the system resources and security factors related to computer network security and establish a security model oriented to security analysis. Based on the analysis of the connotation and current situation of computer network security, this paper points out the main problems existing in the network security model, in order to explore a practical model for improving computer network security analysis.

1. Introduction
With the widespread use of the Internet and the continuous deepening of network applications, people have become accustomed to using the services provided by the network to participate in various network activities, especially e-government, e-commerce, etc. [1]. Computer information technology continues to develop and innovate, and is widely used in many social fields. Computer networks have penetrated into all aspects of people's lives, and the security of computer networks has gradually received attention. [2] In the actual life and work, it will be applied to computer network communication. Computer network communication has become an important platform for people to live, study, live and communicate [3]. With the increasing coverage of computer Internet technology, the scope of Internet applications has gradually expanded, involving many areas of our lives. The sensitive information stored and processed on the network is increasing, so network security management has become the primary problem in computer network systems [4]. At the same time, network security incidents emerge one after another. A large number of data transmission and data storage are completed in the network link. Now the computer network security issues often discussed are becoming more and more serious. Among them, the information security content mainly displays in three aspects: confidentiality, integrity and effectiveness.

With the emergence of new network modes, especially the emergence of distributed systems, the traditional network security management methods gradually show some deficiencies [5]. Hacker intrusion, worm and denial of service and other types of network attacks have found more ways to attack and become the main security problems faced by computer network systems. These malicious attacks, from stealing confidential information and tampering with systems and data to large-scale network paralysis or unavailability of network services [6]. At present, network security is in a backward and passive situation from technology to management. Therefore, it is particularly important
to study computer network security technology and explore the causes of network security [7]. The ways to attack computer networks are increasingly complex, and private information such as enterprises and individuals are easy to be leaked. It is urgent to conduct modeling research on computer network security [8]. Based on the analysis of the connotation and current situation of computer network security, this paper points out the main problems existing in the network security model, and puts forward corresponding solutions in order to explore a practical model to improve the computer network security analysis.

2. Security Analysis of Computer Network

2.1 Properties of Computer Network Security

The evaluation of computer network security system is to study and analyze the security system when it is used, and to prevent or prevent the infiltration changes of the related system by detecting the relevant software. When installing a computer system, we should fully consider the security performance of the system, check whether the specific structure of the computer network meets the requirements, whether the intrusion can be blocked, and ensure that the network system meets the current development needs. After the computer is connected to the Internet, on the one hand, it can realize the transmission and sharing of data and information, on the other hand, it is also facing the invasion of viruses and Trojans. Network security is very important. The research on computer security issues has gone deep into almost all fields of computer science theory and engineering. Software security failure analysis has different characteristics in software design, testing and use [9]. At present, the existing computer network security analysis model has problems with the division of security levels, mainly because the basis for the division is not very reasonable, and the equipment of computer network hardware is not taken into account. Computer network security mainly includes users' requirements for the confidentiality, integrity and effectiveness of their own information transmission or storage process, and the guarantee of security policies is the premise for the realization of good computer network security.

2.2 Factors Affecting Computer Network Security

Information is the result of personal and enterprise labor, which has high privacy. The extensive use of computer technology has begun to become the memory of information, and the use of information technology illegally controls personal computers. The main reason for the network security problem is that in the early stage of the design of computer network system, people pay more attention to the study of network practicability than the network security problem. In the process of using software system, the popularity of network and the importance of computer security increase rapidly. More and more network security incidents and security vulnerabilities are exposed. Computer network physical security refers to the objective existence of network transmission system equipment, such as routers, workstations, network servers and other computer network hardware equipment. Physical security is the premise of network security assurance, which is more convenient for enterprise internal management. When the system is invaded, users cannot normally use the information and cannot operate the system. They can only allow viruses to encroach on their own private information and may even be invaded again in the later use process. Network security technology to a certain extent ensures that computer systems are not attacked and user data are not stolen.

The system security evaluation should consider the security analysis of the existing system, mainly checking whether the target software has known penetration changes, and needs a simple, flexible and complete model. The shortest distance between mobile nodes, the shortest distance between mobile nodes and the average network distance are analyzed. With the increase of social relations among nodes, the shortest path between nodes and the average distance of the whole network are decreasing, as shown in Fig. 1. The success rate data of sensing service node search is shown in Fig. 2.
Table 1 Analysis of Mobile Social Network Structure

| Network            | Number of nodes | Number of relationships | Network density | Central potential |
|--------------------|-----------------|-------------------------|-----------------|-------------------|
| Encounter information | 171             | 225                     | 0.721           | 0.239             |
| Mutual information | 175             | 221                     | 0.578           | 0.226             |
| Weighted summation | 165             | 213                     | 0.582           | 0.214             |

Figure 1 Distance Analysis Of Mobile Social Network Nodes

Figure 2 Perceived Service Node Search Success Rate

The internal network security model is based on the fact that all users are untrustworthy. The focus is only on all users of the external network, and there are also internal network users that cause information security. Some criminals will mechanically destroy the network hardware or create malicious codes to be introduced into the user's computer through network transmission, causing a series of consequences such as computer system paralysis, malicious deletion of important computer software and data, etc. According to the analysis of different phases of the network to detect the
security status of its information system engineering and software system, this is an active defense model, which will regularly detect, find and solve problems of computer network systems. Through various basic theories and mathematical experiences, we can study and establish a computer network attack model, simulate possible attack modes and entrances from the perspective of hackers, combine various technical equipment in advance to formulate protective measures, and accurately find out system defects when faults occur.

3. Computer Network Security Analysis Model
Information system developers have also developed different methods to analyze attack data, find out the structured and reusable patterns, and provide guidance for system security analysis and design. As the content of computer network security design is more and more extensive, it is basically related to all aspects of computer engineering and computer network science. Computer network logic mainly designs the integrity and effectiveness in the process of information transmission. The main characteristic of computer network is that it can realize resource sharing. Some software protection means such as firewall and data encryption model should be used to protect information [10]. There are many hidden dangers in the computer network. Malicious attacks by criminals will cause system paralysis and information loss of the computer network, causing huge losses to enterprises and the country. Because the network is connected to each other, and the wide-area distribution of the network, the sharing of information, the openness of the network system, and the commonality of the channel, the network has many serious vulnerabilities, that is, the network security is fragile.

After the existing vulnerability detection, for each vulnerability, according to the knowledge in the vulnerability database, a fuzzy evaluation value similar to high, low, and low is given. This representation method is difficult to reflect the real security problem caused by the weakness in the system. In solving the problem of cyberspace security, it is necessary to learn based on the off-the-shelf deep learning method of image data, and redesign the processing method of discrete data. Determine and calculate test statistics. In the hypothesis test of two independent sample ratios, the statistics used are:

\[ e_j = -k \sum_{i=1}^{n} f_{ij} \ln f_{ij} \]  \hspace{1cm} (1)

Can get:

\[ W_j = 1 + k \sum_{i=1}^{n} f_{ij} \ln f_{ij} / \sum_{j=1}^{m} (1 + k \sum_{i=1}^{n} f_{ij} \ln f_{ij}) \]  \hspace{1cm} (2)

Replace the data with the calculation:

\[ W_j = d_j / \sum_{j=1}^{m} d_j \]  \hspace{1cm} (3)

In the design stage, the experimental stage and the use stage of a software, there must be corresponding systems and measures to ensure network security. Nowadays, most computer experts and scholars are researching ways to find out the attack path and change the system information when the system is attacked. Computer network security information system realizes the protection of the overall network operation through physical and logical aspects, but there are many factors threatening its information security in computer network. Topological structure model is based on the structure and function of computer network equipment to detect its main working mode and connect various equipment to ensure the safety of information data. While enjoying the convenience brought to us by the network, we have to face the problem of network security. Through this model, the system structure can be optimized, and the computer equipment can be connected by dotted line connection, which can enhance the degree of security protection. Under such circumstances, criminals who want to invade the system through technical means need to find out the entrance of the system and break through the protective barrier, which makes it even more difficult, thus ensuring the safety of the network.
4. Conclusion

With the continuous development of computer network technology and the frequent occurrence of various network security incidents, people are extremely worried about the complete situation of network technology. The situation of computer network security is closely related to people's own interests, so we will not stop studying the model of computer network security analysis. In order to ensure the security and privacy of user information on the network, it is necessary to block the illegal invasion of malicious elements, improve the technical level of network staff, and improve the computer network environment. While enjoying the convenience brought by the network, we must take precautions against its security problems, which requires us to fully enhance our awareness of network prevention and make good use of network resources. With the development of computer network technology, the research on computer network system security assessment has been deepened gradually. Compared with the early methods of relying solely on manual management, the rapid automatic information discovery technology and tools have brought great convenience. Based on the analysis of the connotation and current situation of computer network security, this paper points out the main problems existing in the network security model, and takes this opportunity to explore a practical model to improve the analysis of computer network security.

References

[1] Wurzenberger M, Skopik F, Settanni G, et al. Complex log file synthesis for rapid sandbox-benchmarking of security- and computer network analysis tools[J]. Information Systems, 2016, 60(C):13-33.

[2] Xue, Ming. An Approach to Evaluating Computer Network Security with Intuitionistic Trapezoidal Fuzzy Information[J]. Journal of Control Science and Engineering, 2014, 2014:1-4.

[3] Bolanowski M, Paszkiewicz A. The Use of Statistical Signatures to Detect Anomalies in Computer Network[J]. Lecture Notes in Electrical Engineering, 2015, 324:251-260.

[4] Tan S, Li X, Dong Q. TrustR: An Integrated Router Security Framework for Protecting Computer Networks[J]. IEEE Communications Letters, 2016, 20(2):376-379.

[5] Li A S, Li X C, Pan Y C, et al. Strategies for network security[J]. Science China Information Sciences, 2015, 58(1):1-14.

[6] Wang S, State R, Ouardane M, et al. Mining NetFlow Records for Critical Network Activities[J]. Lecture Notes in Computer Science, 2014, 6155:135-146.

[7] Cooperative Resource Allocation in Multicast Networks for Outage Probability Minimization[J]. International Journal of Wireless Information Networks, 2015, 22(1):1-9.

[8] Fernández-Blanco, Ricardo, Arroyo, José M, Alguacil N. Bilevel programming for price-based electricity auctions: a revenue-constrained case[J]. EURO Journal on Computational Optimization, 2015, 3(3):163-195.

[9] Belenky, Alexander S. Finding an optimal strategy of incorporating renewable sources of energy and electricity storing systems in a regional electrical grid[J]. Energy Systems, 2015, 6(2):291-308.

[10] Pillac V, Cebrian M, Van Hentenryck P. A column-generation approach for joint mobilization and evacuation planning[J]. Constraints, 2015, 20(3):285-303.