Research on Computer Security Focus and Its Key Technologies

Miao Wang

Xi'an Peihua Universtity, Xi'an, Shaanxi, 710125

Keywords: computer security; key technologies; big data

Abstract: At present, the development of computer networks has made computer applications more extensive and deeper, but it has also made security issues increasingly prominent and complex. Under normal circumstances, people consider computer security issues from two aspects: host security and network security. However, due to the difference in the foothold between the two, the technical means adopted by each of them is difficult to organically combine. Therefore, for some problems that need to be dealt with by both parties, they cannot be solved effectively.

1. Introduction

In today's society, the Internet has become a platform for people to exchange information, and the scale of development has also grown. At the same time, the corresponding security issues are also valued by many netizens. A large number of theories and practices have shown that electronic viruses and malicious code, hackers, etc. have caused certain damage to the operation of computers. The reason for these phenomena is that computers have security vulnerabilities, and computers design programs for people in their daily lives. Waiting for work provides convenience, but when the computer software is running, it often pops up some webpage information. If you don't pay attention to it, it will cause viruses in the computer. These phenomena are all because of the drawbacks of the security of the computer at design time. For this reason, it is absolutely necessary to carry out a comprehensive analysis of security vulnerabilities. It is very important for the improvement of network security and the maintenance of computer systems.

2. Overview of Computer Security Vulnerabilities

The study of computer weaknesses is extensive and complex, covering different fields such as formal linguistics and statistics. Computer vulnerabilities generally refer to flaws in their own hardware, software systems, or tactical levels, and provide the possibility of attackers with malicious attacks and illegal access. Weaknesses cover a wide range of aspects, including all aspects of computers and network systems, such as routers and firewalls. In order to prevent the phenomenon of title confusion, the author regards security loopholes, weaknesses, weaknesses and security weaknesses as weaknesses in this paper. When discussing the computer weakness problem, it is generally necessary to solve the following four problems. First, what is the computer weakness; second, how to clearly reflect the essential characteristics of the vulnerability; third, how the computer system belongs to the vulnerable category; and fourth, once the computer weakness occurs, Will cause a variety of asset losses. Based on the four issues discussed above, we can generally summarize the weaknesses in the following three aspects: description, detection, and assessment techniques. These three technologies are closely linked and influence each other. Weakness description technology occupies a fundamental position and weakness detection technology. As an assessment tool, Vulnerability Assessment technology provides the ultimate service to users, highlighting the initial goals of vulnerability research.

In order to fully understand the weaknesses of computers, we need to fully and clearly express the essential characteristics corresponding to computer weaknesses. Under such background conditions, the weakness description technology will appear. The description of weakness description mainly includes the two aspects of weakness classification method and description language. The former mainly discusses what kind of attributes can be clear and comprehensively

mark weaknesses. The latter discussion is used to deal with the means to make people clear. With the above attributes, the problem of weaknesses can be recognized correctly. For the weak point description technology, its application needs mostly from the disclosure, storage and learning of vulnerability information; detection; research and evaluation; software engineering category.

Vulnerability detection refers to the identification of weaknesses. It can promote the development of weak points assessment and provide them with reasonable weak-current information. From a conventional sense, it is mainly used to explore problems of weaknesses. Therefore, in practice activities, vulnerability detection is related to the final outcome of the vulnerability assessment and is the main influencing factor. In recent years, researchers have carried out research on a large number of systems and systems around weak current detection technology, and have provided corresponding classification results from different perspectives. Each detection method is closely linked. From the detection target level, the vulnerability detection technology can be divided into two known and unknown contents. The former mainly involves partial automatic detection methods, and the most common one is passive monitoring methods. However, the latter mainly explores manual detection methods.

3. Network System Weakness Assessment

The rapid development of computers has brought about earth-shaking changes in people's daily work and routine life. At the same time, it has increased the possibility of malicious attacks and illegal access. Life practice shows that although multiple independent weaknesses have a small scope, if they are used by hackers through the network, they will bury certain risks for network system security. From the perspective of the vulnerability assessment category, due to the interconnection of computers, the network system evaluation and the host system evaluation are quite different. For the network information security system, the security risk analysis and the degree of network interconnection are positively correlated, with the interconnection. As the degree increases, the analytical difficulty factor will continue to increase. With reference to descriptions, risk assessments can be divided into qualitative, quantitative, and mixed assessment methods. In general, qualitative assessment generally defines the systemic risk status based on the researcher's own knowledge structure and level of experience. This assessment method has comprehensive and in-depth advantages. Quantitative assessment refers to the risk assessment work carried out by means of quantitative indicators. The significant advantages of this method are intuitive, concise, reasonable and rigorous. The author will discuss the specific quantitative vulnerability assessment of the network system. This paper relies on network node association, organizational design, and develops a risk propagation model to judge network system risk.

In order to clarify the actual connection between the independent weaknesses within the network, in order to accurately judge the security risks, the researchers conducted a lot of research around the connectivity of the network nodes themselves. Analysis of relevant literature found that systematic understanding and comprehensive exploration of the connectivity of each node's own host itself is related to the evaluation of network vulnerability. In the actual work and real life, the network will be applied anytime and anywhere, for example, to disclose data information through the network and to carry out work activities through the network. In the above practice exploration, it is not difficult to find that there are always different access relationships within the network nodes and node users. This relationship has special characteristics, except for acting on the level of proprietary control rights, and also in the relationship specificity.

First, a model definition is made, and all concepts and definitions associated with it are proposed; subsequently, the propagation algorithm is clarified. Due to the inadequacies of NPR recognition, it is not difficult to find that in real life, few literature studies related to the algorithm used to solve the problem can be seen. Until the end of the problem, the problems similar to the problem mainly include DCMC and MRD problems. These two problems are different from the NRP problems. The latter solution focuses on spreading various risks along various directed paths to various types. Reachable node.

Combined with practical activities, we try to explore an approximation algorithm to significantly

optimize the performance of the algorithm on a precise basis. Based on this demand, the approximate propagation algorithm was officially released, and it was recorded as the APMI algorithm. Analyzing the RH algorithm can find that every directed path runs through the same part and will perform one operation. This will generally consume more time and occupy a certain space. In view of this phenomenon, the principle of approximate propagation is summarized and its specific content is summarized. As follows: Each component spreads the risk, causing it to move to adjacent components, ignoring the issue of continued propagation, while the components only need to be processed once. Under this basic condition, new problems emerged, mainly referring to the fact that the order of component processing will restrict the accuracy. In order to avoid this error, the principle of minimum degree is introduced, and adjacent propagation is implemented with the smallest component as the object. The APMI algorithm specifically involves initializing and accurately calculating the initial probability of all components themselves, clarifying the risks, forming a set of risk sources, scientifically calculating the initial penetration degree, and discarding the intrusion formed by the non-risk source components corresponding to the zero-input degree or the indirect formation degree. , Implementing neighboring dissemination of content. Then proceed from the return path and the non-return path to explore the accuracy of the algorithm. Based on this, the simulation experiment is carried out. In order to explore the influence of different factors such as network size type, network actual density and risk source density on the performance of the algorithm, this paper conducts simulation experiments with small and medium-sized networks and rationally sets up the experimental environment. A subject is set for each node, and the probability values and the hazard indicators corresponding to each weak point and the directionality are specified as 0.5 and 1.0, respectively. In addition, in order to reduce the size of the experimental error, for each group of experiments, RH and APMI were fabricated by means of a set of parameters by means of the average distributed random number, and the corresponding average values were selected. The types of network size, network density, and risk source density are discussed separately.

In recent years, the rapid development of network technology, at the same time, malicious attacks and illegal access activities are also more diverse and cumbersome, the most prominent network virus, mainly in accordance with automated methods, spread and spread through software security weaknesses, facing the computer system attack on purpose. The aforementioned security risks pose a serious threat to the normal operation and steady use of computer systems. In order to increase system security and improve information reliability, system administrators and developers are striving to explore independent and effective prevention technologies, that is, vulnerability assessments, and have triggered people's highly heated discussions. The vulnerability assessment specifically refers to the implementation of computers, the loss of the network caused by the security weaknesses, the weak point assessment, effectively control the actual security risk of the computer system, promote security, provide scientific decision-making information, and prevent danger The emergence of events. Vulnerability assessment technology is more active and has a certain degree of advancement, superior to intrusion detection technology. According to the evaluation object, the vulnerability assessment can be divided into host system evaluation, computer firewall evaluation and network software system evaluation. The author will focus on the host system evaluation. The host system usually includes multiple softwares, and each software can be regarded as a system component. The original evaluation method only analyzes the weaknesses of individual components and does not consider the undesirable threats arising from the interconnections within multiple component weaknesses. At the same time, the original assessment The method uses only the number of weaknesses to express systemic risk, which will induce weak misjudgment. In order to make up for this deficiency, the author proposes an assessment method based on the vulnerability map. This method not only applies the vulnerability association idea, but also applies the comprehensive analysis method and selects the index evaluation strategy to evaluate the security risks induced by weaknesses in organizational design, implementation and operation, and comprehensively compare each system with all versions. Any level of security.

4. Conclusion

On the network development of computers, all sectors of society have reached consensus, cooperated and worked together to build a platform for information networks. For how to achieve this goal, the first thing to do is to provide safe, reliable and stable protection. It can be seen from this that it is extremely important to propose effective and feasible measures to solve the problem of security risks, which requires the attention of the whole society. Whether it is analyzed from the Internet or from the local area network, the issue of information protection is involved. To this end, we should combine all kinds of security risks, put forward security countermeasures, weigh the characteristics of each threat, and actually protect the information and data of the network, and at the same time continuously improve the technical level of security. The long-term sustainable development of the computer itself.

References

[1] Zhang Hanying, Zhang Yanhua. Computer Security Weaknesses and Appropriate Policy Research [J]. Communications World, 2017, 1(03): 102.

[2] Yang Jian, Han Dong. Analysis of Computer Security Vulnerability and Corresponding Key Technologies [J]. Computer Knowledge and Technology, 2016, 1(08):64~66.

[3] Sun Bocheng. Analysis of the Security Settings of Computer Operating System [J].Science & Technology Economic Market, 2015, 2(11): 18.

[4] Sun Guilin. Analysis and Discussion on Computer Security Teaching [J]. Xue Zhou B, 2014(6):55-55.

[5] Cui Zhilei. Computer security behavior prevention model based on artificial immune [J]. Journal of Lanzhou University of Technology, 2014, 35(4): 107-110.