Analysis of Network Attack Technologies and Network Security

Xu Pei

NanChang Institute of Science & Technology

Keywords: Network attack; Network security; Attack graph

Abstract. With the continuous development and progress of Internet technology, network security has become the focus of social concern. Internet technology occupies a place in all areas of the society and provides a new model for people's lives and learning. While giving full play to the advantages of Internet technology, network attack technology is also more and more high-end, and becomes a serious threat to the security of the network. Based on analysis of the current situation, to strengthen the understanding of common network attack technology and understand the relationship between network attack technology and network security is very important for the healthy development of the Internet. It is necessary to further strengthen the information security of the Internet network, effectively prevent the loss of leaks from the common network attack technology, analyze the Internet operation and explore the relationships between the technology of network attack and network security.

Introduction

The rapid development of Internet has brought great convenience to people's production and life, but while obtaining conveniences, some problems have gradually emerged, especially the problem of information security has now become an issue of common concern, because the network is essentially belongs to the open nature of the main reasons for this is the network insecurity, the network security, many in the network security services company will spend lots of money to hire hackers to conduct real-time detection of network security, and constantly develop new products network. Although the development of the Internet in China is still in the initial stage of construction, but also because the time is short, do not have enough experience, the final presentation of the results is not very good, plus the network management personnel are mostly computer professional graduates, these graduates are not what the network experience, but also did not accept before they start network security training, and in the development of information technology today, whether hardware or software facilities, updates faster, the computer virus is more and more difficult to solve, we also introduced many foreign network technology in the construction stage of the network, so from this point of view, the domestic network security issues always have not been fundamentally solved.

In this paper, the basic principle of network security analysis method is analyzed, including the concept of attack graph, the model of attack tree, and the modeling of other models. At the same time, on the basis of domestic and foreign research results, this paper discusses the automatic generation algorithm of attack path and the advantages and disadvantages of the algorithm. Then, through in-depth research on attack graph theory, put forward a security analysis system prototype based on the realization of each module in detail and technical methods required or tools are compared and discussed.

Analysis of Network Attack Technologies

Network attack mainly refers to the use of special tools to complete all kinds of information of the other mobile computer network and system crashes, failure or wrong work, its purpose is to destroy the network security confidentiality, integrity, availability, reliability, controllability and non-repudiation. Any unauthorized acts that interfere with or disrupt the network system are called network attacks. There are several methods of network attack.

Loopholes to Network System. The computer network system flaw mainly refers to the actual operating system has the flaw in the logic design, in the process of writing the program has appeared the compilation mistake. These errors will be used to spy or remote control computer hackers, in this time the hacker control computer, all the information in the computer will be stolen, and stolen way is generally based on the password as the main target of attack. Sometimes it will be posing as legitimate users directly into the attack of the computer, thereby gaining control of the computer.

Password is too Simple. In order to protect their privacy, most users will use a password to restrict unauthorized access, like computer password, user password system and so on, but in order to facilitate, most users choose one password, but it is very easy to remember, a password that is very easy establish air links to the attacker, the attacker will then remote user computer and easy, even if the user password is set, but because the password is relatively simple, so it is time to crack problems.

Trojan Software. Trojan software is a highly covert remote control software, the computer Trojan is mainly composed of a Trojan and keeping control center, in order to prevent the security personnel of Trojan software tracking, Trojan software will increase the springboard to bridge it belongs to the Trojans and keeping control center. Trojan will be used to control the center of the springboard and contact, behind the control center will have a direct control of the user through the network technology of the computer, thus easy access to passwords. Even personal communications will be fully mastered. In other words, as long as you have some information on the computer resources, the attacker will know, if there is a camera and microphone, then the attacker can also listen to the user's real-time conversation content.

Methods to Analyze Network Security

The analysis method in network security can be divided into two types: one is the network security of the unknown vulnerability analysis, and the main prevention measures include: one is the network security vulnerabilities known for effective analysis, so as to make up for the weakness in the network link, the network security is to improve. In terms of the unknown, information security experts at home and abroad have long been a lot of research, the main methods are:

1. Analysis loopholes in protocol, such as ARP address resolution protocol loopholes. After careful research, researchers find loopholes in the protocol, conduct actual test and summarize the vulnerability in some links so as to propose the solutions to make up for the deficiency of agreement and achieve the purpose of prevention.

2. Analyze program code. At work, programmer will inevitably introduce fatal loopholes due to their lack of knowledge and the neglect of some common errors, such as the buffer overflow loophole. Through studying some important codes, researchers take some necessary preventive measures to those places that may produce serious errors and give software patches so as to improve the overall security of the software.

Although these methods are effective and take preventive measures, it is still very difficult, and there are few research results. However, starting from the already known network security vulnerabilities, it is relatively easier, such as a variety of graph based model detection methods, such as the commonly used attack graph. For the existing tens of thousands of vulnerabilities, security vendors have given the basic defense measures; Microsoft has also been updated windows operating system, given the necessary patches to prevent hacking. In this way, we can continue to make up for vulnerabilities and vulnerabilities in the network, to improve the overall security.

Network Attack Modeling Method Based on Attack Graph

Attack Tree Modeling Method. Attack tree uses a tree structure to describe the attacks on the system , the total target to achieve as the root node of the tree, to achieve the overall goal of the sub goals as child nodes, a gradual breakdown of leaf node at the end of last tree is specific attack method.

The relationship between nodes may be one of the three relations, "or", "and", "order" and "relationship", which means that the acquisition of any child node can lead to the acquisition of the parent node. The relationship indicates that the acquisition of all child nodes can result in the acquisition of the parent node. The sequence and relationship indicates that the order of all child nodes can be achieved in order to achieve the goal of the parent node. The graphical representation of the three relationships is shown in Fig. 1.

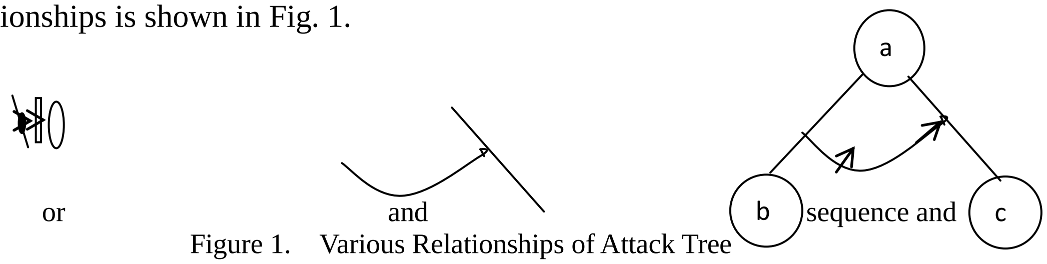

Figure 1. Various Relationships of Attack Tree

1. Attack Net Modeling Method

Attack net is a hexatomic group, AN=(S, A, F, W, S0 , M). Herein, S0is the attack state set, A is the attack method set; S ∩ A=Φ , S ∪ A≠Φ; F is the node flow relationship set, i.e., directed arc, F ⊆ S×A∪ A×S. W is function of the attack method, W(A)is used to measure characteristics of the attack method. S0 is the original attack state, and M is the marked original state distribution.

Attack net divide the specific attacks into attack state, attack methods and progress of the current attack, which correspond with place, transition and token in the Petric network. When the attack progresses to a certain state, if the attack method is satisfied, then the attack progresses to the next state, that is, an attack is completed, as shown in Fig. 2.

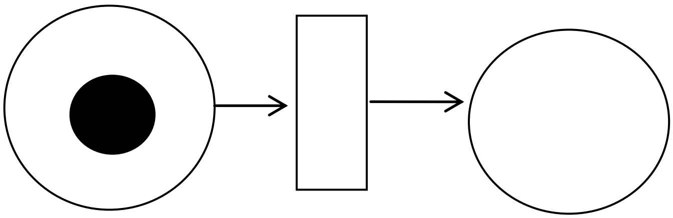

Figure 2. Example of Attack Net Atomic Attack

The circle represents the attack state, the box represents the attack method, the black point in the circle represents progress of the current attack, and the directed arcs represent the relationship between attack methods and attack state.

Conclusion

From the analysis of the relationship between the technology of network attack and network security, between the two is a process of interaction, and the face of the need of network security, network vulnerability, the need to strengthen the understanding of network security, network attack technology, and make effective defense and response, so as to achieve victory in the war in the network security. The main work of this paper is to large-scale network as the experimental background, research on network security analysis method based on attack graph, and attack detection algorithm based on symbolic model diagram, and the automatic generation of attack graph, based on the proposed large-scale network security detection system prototype for future targeted development. This paper introduces the network security attack trends, and then introduces the research status of information security at home and abroad, and the research focus of network security, and understand the situation of network attack technology, network attack steps and levels, provide some basic knowledge for the in-depth study of network security protection.

Project funding: Nanchang Intelligent Building Network Engineering Key Laboratory & Specialty of Jiangxi Province (NGTSZY201001)

References

[1] Jiang T. Network attack technique and network security analysis [J]. Heilongjiang Science, 2016.

[2] Qin Y. Computer Network Attack Modeling and Network Attack Graph Study [J]. Advanced Materials Research, 2014, 1079-1080:816-819.

[3] Cook C L. Input translation for network security analysis: US, US 20060021045 A1[P]. 2006.

[4] Kadhem H, Amagasa T, Kitagawa H. MV-OPES: Multivalued-Order Preserving Encryption Scheme: A Novel Scheme for Encrypting Integer Value to Many Different Values [J]. Ieice Transactions on Information & Systems, 2010, 93-D(9):2520-2533.

[5] Lopes C C, Times V C, Matwin S, et al. Processing OLAP Queries over an Encrypted Data Warehouse Stored in the Cloud[M]// Data Warehousing and Knowledge Discovery. Springer International Publishing, 2014:195-207.

[6] Dehne F, Kong Q, Rau-Chaplin A, et al. A distributed tree data structure for real-time OLAP on cloud architectures[C]// IEEE International Conference on Big Data. IEEE, 2013:499-505.

[7] Kong Q. Scalable real-time OLAP systems for the cloud [J]. Real-time, OLAP, Cloud, distributed PDCR-tree, 2014.

[8] Dehne F, Kong Q, Rau-Chaplin A, et al. A distributed tree data structure for real-time OLAP on cloud architectures[C]// IEEE International Conference on Big Data. IEEE, 2013:499-505.

[9] Dawkins J, Hale J. A systematic approach to multi-stage network attack analysis[C]// IEEE International Information Assurance Workshop. IEEE Computer Society, 2004:48.

[10] Yuan J. Research on attack graph generation for industrial control network security and vulnerability analysis [J]. Modern Electronics Technique, 2016.

[11] Hong J, Kim D S. HARMs: Hierarchical Attack Representation Models for Network Security Analysis [J]. 2012.

[12] Bush S F, Evans S C. System and method for network security analysis: US, US20040250128[P]. 2004.