Research on Security Protection Technology Based on Terminal Information Jump

WANG Yi, GAO Yang, Luo bing-bing
ZhangJiaKou Electric Power CO., LTD. 075000, China
*YuH@sjtu.edu.cn

Abstract. This paper proposes a security protection model based on end-to-end information hopping to meet the actual needs of enterprise intranet protection. The problem has enhanced the proactive protection capability of the intranet.

1. Introduction
Nowadays, the Internet is becoming more and more popular. With the rapid development of Internet of things, big data, artificial intelligence and other technologies, the network has become the largest bearing facility, bringing us great benefits and convenience. According to the 44th statistical report on the development of China's Internet network issued by China's Internet Information Center in 2019, by June 2019, the number of Internet users in China has reached 854 million, The Internet penetration rate had reached 61.2% [1]. Therefore, it can be seen that the network has deeply affected people's life and thinking habits, making it more and more dependent on the network. The terminal host can easily join the network and communicate with any other host by exchanging data packets. However, the Internet is also a double-edged sword, While enjoying convenience, we are also facing severe security threats. According to the report, in the first half of 2019, the national Internet Emergency Center detected and coordinated the disposal of 40000 tampered websites in China, About 14000 IP addresses at home and abroad were detected to embed backdoors into 26000 websites in China. The national information security vulnerability platform included 5859 common vulnerabilities and 2055 high-risk vulnerabilities. Various Trojans, viruses, worms and malicious codes plagued the whole Internet world. For example, servers provide standard network services by opening a well-known port. At the same time, the static service model also exposes the application to potential attackers for a long time. Attackers can perform network scanning, locate the system, obtain detailed information, and launch DoS/DDoS or other advanced attacks to destroy the server system. Traditional security protection systems, such as firewall and IDS IPS, are passive and incomplete in nature, so they are not enough to ensure security and can only detect known attacks. Active defense technology is an effective way to deal with this threat. The aim is to change the attack surface of the system and increase the attacker's use of the target system's work and cost to defend the attacker.

2. Related work
End to end information hopping is inspired by frequency hopping technology and electronic countermeasure technology in wireless communication. By jumping communication frequency, defenders make it more difficult for attackers to listen and interfere. In end-to-end data transmission, one or both sides change port, address, protocol and other end information randomly, thus disturbing the attacker's listening and blocking and realizing active defense. In order to improve the level of
network security. This paper focuses on the address and port hop in the end information hop.

In reference [3], address and port hopping is a novel and effective active defense technology, which can hide network servers and applications by constantly changing IP addresses and ports.

However, it is difficult to find a hidden danger in the process of changing the communication time between the TCP port and the server by changing the communication time between the TCP port and the server. Too long TCP connection will lead to the risk of cracking the jump port.

In reference [4], a network address space randomization scheme called Nasr is proposed. It is a LAN level network address randomization scheme based on DHCP update. Since the address space of this method is limited, there will be limited hop problem.

In reference [5], a spoofing port address hopping technology is proposed, which camouflages the IP address and port of the server during data transmission between the server and the client, so as to confuse the attacker. The technology does not change the IP address and port of the server, but only camouflage it. It is effective to prevent external attackers, but is limited to its own limitations. Cannot effectively defend against internal attacks.

Reference [6] proposed a strict time synchronization port hopping method, by dividing the service time into fixed length slots, mapping different time slots to different service ports, so as to prevent denial of service attacks. However, the disadvantage is that when there is delay or congestion in the network, the strict time synchronization based on time is not applicable.

In this paper, we propose a method of packet synchronization which is not subject to packet hop in the server.

In this paper, we propose a method of address and port jump, which can dynamically change IP address and port by synchronous hop between end to end, so as to increase the difficulty of attacker detection and improve the security of network communication.

3. Dynamic defense model based on address and port hop

3.1. time synchronization

The existing address and port hopping methods are mainly strict time synchronization [6] and ACK synchronization [7]. However, strict time synchronization is greatly affected by network delay and blocking. Ack synchronization is easy to be intercepted and requires high performance of the server. In view of the above shortcomings, this paper adopts the PTP [8] time synchronization protocol of IEEE 1558 with high precision. The basic principle of PTP is to add "time stamp" to each message, and calculate the delay between the end-to-end clock according to the "time stamp", so as to achieve the purpose of time synchronization. After the time synchronization between the end-to-end, both sides can calculate the corresponding address and port through the time, so as to achieve the purpose of subsequent communication.

3.2. address and port hopping

Suppose the IP range of Intranet is 192.168.1. X-192.168.255. X (1 ≤ X ≤ 255). Then it can be constructed into 255×255 matrix M of 255, m_{ij} ∈ M, ij denotes the value range, M = 0, 1.0 indicates the idle state of the IP, and 1 indicates the occupied state:

\[
M = \begin{bmatrix}
m_{11} & \cdots & m_{1255} \\
m_{2551} & \cdots & m_{255255}
\end{bmatrix}
\]

The value range of the port is: in this range, 0-1023 port number has been assigned by common application programs, so the port number dynamically assigned is selected after 1024.

Address calculation process: Firstly, the value I is obtained by modulo 256 operation on the current time. Then, the current time is hashed by using the irreversibility of MD5 algorithm and the fixed 128 bit output result. The last 8 bits of the result are taken out to get J, which is checked in the matrix Mm_{ij}0, indicating that the current IP address is available, the current IP address is used, and then m_{ij} Value becomes 1; if m_{ij} If the current IP address is not available, the value will be shifted to the left by one bit
to get the new value of J. the new value is checked again in the matrix M until the selected IP address is idle.

The port calculation formula is as follows:

\[
\text{port} = \begin{cases} 
    f(t) & \text{if, } \text{port} \geq 1024 \\
    f(t) + 1024, & \text{port} < 1024
\end{cases}
\]

Port is port number and function \( f \) is module\(2^{16}\) Operation, \( t \) is the current time.

Through the above formula, the corresponding port number can be calculated according to the current time.

3.3. Dynamic defense model based on address and port hop

This paper presents a dynamic defense model based on address and port hop. As shown in Figure 1, the model includes time synchronization module, address and port hop module and port hop module.

Control module: In the process of end-to-end communication in the intranet, the current IP address matrix M is constructed, \( m_{ij} \) Attribute assignment transformation, that is, when the IP address is occupied, \( m_{ij} \) When the IP address is idle, \( m_{ij} \) It also provides the function of checking whether the IP is occupied and idle, as well as the function of reclaiming and allocating IP (i.e. resetting the attribute of matrix M).

Time synchronization module: PTP protocol is used to realize time synchronization between end to end.

Address and port hopping module: According to the synchronization time of time synchronization module, the corresponding IP address and port number are obtained, and the address and port are used in subsequent connection.

The dynamic defense model based on address and port hopping ensures that the communication IP and port are different at different time on the basis of ensuring the normal communication between end to end. It can effectively resist the detection and detection of attackers and improve the security of communication.

4. Summary

Taking active defense as the breakthrough point, referring to the thought of frequency hopping communication, and by comparing and analyzing the advantages and disadvantages of the existing address and port hopping technology, this paper proposes a method based on address and port hopping, which can effectively deal with network security threats by PTP time synchronization and hop function, and establishes a dynamic defense model based on address and port hop. The feasibility of the model and the effectiveness of dealing with network security threats are analyzed theoretically, which enriches the connotation of network security dynamic defense.

Reference

[1] China Internet Network Information Center. The 44th statistical report on China's Internet development [R], 2019.

[2] Shi Leyi, Jia Chunfu, LV Shuwang. Research on active network protection based on terminal
information jump [J]. Journal of communications, 2008 (02): 112-116

[3] H.C.J. Lee, V.L.L. Thing. Port hopping for resilient networks[C]/ Vehicular Technology Conference, 2004. VTC2004-Fall. 2004 IEEE 60th. IEEE, 2004.

[4] S. Antonatos, P. Akritidis, E.P. Markatos. Defending against hitlist worms using network address space randomization[J]. Computer Networks, 51(12):3471-3490.

[5] Applications That Participate in Their Own Defense (APOD).

[6] Yue-Bin Luo, Bao-Sheng Wang, Xiao-Feng Wang,. RPAH: Random Port and Address Hopping for Thwarting Internal and External Adversaries[C]/ 2015 IEEE Trustcom/BigDataSE/ISPA. IEEE, 2015.Gal Badishi, Amir Herzberg, Idit Keidar. Keeping Denial-of-Service Attackers in the Dark[C]/ International Symposium on Distributed Computing. Springer, Berlin, Heidelberg, 2005.

[7] Li Hongliang. Design and implementation of high precision network time synchronization system based on PTP protocol [D]. Tianjin University.