DOS attack analysis and study of new measures to prevent

Zhang Chao-yang

Network Center
Huanggang Normal University
Huangzhou, Hubei, China
zhangcy@hgnu.edu.cn

***Abstract*—Denial of Service (DoS) and distributed denial of service attack (DDoS) is now a common means of attack that affects seriously network security and the quality of online services. This paper analyzes the DoS (DDoS) attack prevention principles and gives an thorough analysis of existing prevention techniques, proposed to prevent DoS (DDoS) attacks in three ways: usinga router DoS attack prevention; increase the trusted platform module; increase system defenses.**

Keywords- *denial of service attacks; trusted platform; system defense*

I. INTRODUCTION

DoS, namely, the denial of service, resulting in a network denial of service attack known as DoS attacks, and its purpose is to make the server or network fail to provide normal services. The most common DoS attack against a computer network includes bandwidth and connectivity attacks. Bandwidth attack refers to attacks with great impact on network traffic, so that all available network resources are depleted, leading to legitimate users' requests cannot be passed. Connectivity attack with plenty of connection requests that the impact of server operating systems so that all available resources are exhausted. As a result, the server cannot process legitimate user's request. For DoS, it includes a lot of attacks, there are three main ways, namely, TCP-SYN flood, UDP flood and ICMP flood [3]. TCP-SYN flood attacks follow three-way handshake protocol TCP connection, send a SYN packet to the destination host, destination host makes no response after the SYN ACK is received. In this way, the destination host has to built up a substantial connection queue for these source host , and because of no response, it will maintain these queues all the time, resulting in consumption of large quantities of resources and failing to provide services to the normal request. UDP flood means that the attacker send UDP packets to the port of the victim system randomly, when the victim system receives a UDP packet, it will confirm the application waiting at the destination port. When it found that the port does not exist, it will generate an ICMP packets that the destination address connot reach and send it to the spoofed source address.

When a sufficient number of UDP packets is sent to the attacked computer port , the entire system will be paralyzed. ICMP flood means that the attacker find out which router on the network will respond to ICMP requests, and then send messages to the router's broadcast address with a false IP source address, the router will broadcast the message to each equipment connected to the Network.These devices then respond immediately, it will generate a lot of message traffic, which takes all the equipment and network bandwidth resources, and the address which generates a reply message is the target of attack.

For different DoS / DDoS attack type, the current method of attack detection and defense very much, can be divided into three categories: detection and defense based on protocol characteristics analysis [1], detection and defense based on the accumulation [2] and detection and defense based on network traffic statistical model [3]. Currently, the detection and defense methods also have the following problems: detection and defense based on protocol characteristics analysis can only be applied to the type of attacks with obvious protocol characteristics of abnormal flow [4], for many attack types with no clear protocols characteristics is invalid; and detection and defense based on accumulated statistical model and network traffic cannot distinguish between normal traffic and large attack traffic [5], in this case, legitimate users' traffic will be mistaken for attack traffic. This article will introduce several new defense methods from the Angle of application.

II. PRINCIPLES OF ATTACK

A. Attack principle

In the network communication with vulnerability of TCP protocol to achieve DoS attacks, TCP client and server using three-way handshake (Three-way Handshake) to establish a connection: the first handshake: The client sends a request with the SYN bit,that need to connect the server , And then wait for the response of the server. The second handshake: the server receives syn packet, you must confirm the customer's SYN (ack = j +1), while sending a SYN packet themselves (syn = k), the SYN + ACK packet, then the server into SYN_RECV state; The third handshake: The client sends a connection confirmation message to the server. Confirm the information bit is the server SYN bit of confirmation

978-0-7695-4480-9/11 $26.00 © 2011 IEEE
DOI 10.1109/ISIE.2011.66

information is ACK bit that the server sent, ACK bit is the SYN bit sent by the server plus 1. At this time, connection channel has established, the two sides can exchange some data.SYN Flood is one of the most popular DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks, the principle is to use TCP protocol flaw, sending a large number of forged TCP connection requests to exhaust the resources of the attacked party , in the process of TCP connection, if the host crashs, or is suddenly disconnected after a user send a SYN packet to the server, then the server cannot receive the client's ACK packet after SYN + ACK response packet is sent out (the third handshake cannot be completed),in this case the server will usually retry(send SYN + ACK to the client again) and discarded this connection after waiting for a period of time, we call this time the length of the SYN Timeout, general speaking, This time is minutes orders of magnitude (approximately 30 seconds -2 minutes); it is not a big problem that an abnormal problem of a user results in a thread of the server to wait for 1 minute, but if a malicious attacker simulated this situation largely, the server will have to maintain a very large queue and consume large quantities of resources, it gives rise to the TCP / IP stack overflow, and then the server system crashes --- even if it is strong enough, the server will also be busy with the attacker forged TCP connection requests and ignore the normal client requests, fulfilling the attacker's purpose: paralyse the services.

B. *Components of attacks*

1) Attacker: the attacker's computer is the main console to attack, which can be anywhere on the network host, or even an activity of the portable machine. The Attacker Manipulate the attack process, it sent the host attack command to the console.

2) Console: console is some host that attacker invade and control illegally and these host also control a large number of proxy host. the master host was Installed specific program, so they can accept special orders sent by the attacker, and these orders can be sent to the proxy host.

3) Agent : Agent is also some host that attacker invade and control illegally . Attacked program was running on them, receiving and running command the host sent . Agent of the execution host is an attacker who sends a real attack to the victim host.The first step the attackers conduct DDoS attacks is to find loopholes in the Internet host, then enter the system and install backdoor programs in its top,the more host he invades, the more stronger his team is; the second step is to install attack program on the invaded host, some of which is used as console ,the other as part of the agent side. Various parts of the host do their duties under the attacker's disposal and attack the target of attack. Because the attacker was behind the attack, attack will not be tracked by monitoring system and it is difficult to find.

C. *Attack Performance*

Denial of service attacks are a concrete manifestation of the following ways:

1) manufacturing high flow useless data, giving rise to network congestion, as a result, the injured host cannot communicate properly with the outside world.

2) Taking advantage of the services provided by the victim host or defects on the transport protocol, repeated high-speed service to issue a specific request to the victim host and let the victim host cannot process all normal request in time.

3) Taking advantage of defects on data processing services provided by the victim host and causing service program error by repeatedly sending malformed data, it takes a lot of system resources and the host is in suspended animation or even crash. Strictly speaking, denial of service attack technology is a technical way to damage the network services, and its fundamental purpose is to make the victim host or network lost the ability to receive timely process of requests and make the user's normal service request fail to get a response.

III. DEFENSE PROGRAM

A. *Defend DoS attack using a router*

Using the function of Unicast RPF Unicast RPF (Unicast Reverse Path Forwarding, a single address reverse route forwarding) is an effective measure to enhance the routing security. This function set the following data packet forwarding mechanism: When the router receives a packet, it checks the CEF (Cisco Express Forwarding) routing table to determine the return to the source IP address, if the packet is a route to the packet from the receiver out of the interface. the normally forward the packet, otherwise it will discard the packet. For example, the router receives an data packets which source IP address is 172.16.0.8 , if the CEF routing table not provide any routing for the IP address of 172.16.0.8, the router will discard it.

B. *Use TCP blocking to limit SYN attack*

After the IOS11.3 version CISCO introduce the TCP intercept feature, which can effectively prevent SYN Flood attacks on internal hosts. TCP intercept prevent this attack by intercept and confirmation before the request of connection reaches the target host, TCP intercept can work in intercept and monitor modes. In intercept mode, the router intercept to reached TCP synchronization request and establish the connection between the server and the client on behalf of the server, if the connection is completed, it means the client has establish a connection to the server, and the two connections merge transparently. During the entire period of connection, the router provide more stringent timeout for half-open limit for illegal connection requests, to prevent its own resources from being depleted. In monitoring mode, the router passively observing the connection request through the router, if the

connection exceeds the configured set-up time, the router will close the connection.

CISCO router in the TCP intercept feature requires two open Steps:

First, configure extended access list to determine the IP address that need protecting; Second, open the TCP intercept. Configure access list is to define the source and destination address that need intercepting, to protect the internal destination host or network. In the process of configuration, users usually need to set the source address as 'any', and specify a specific destination network or host.

C. crease the Trusted Platform Module

Trusted computing is an important concept in the area of information security. The basic idea is: firstly build a physical security of the trusted root part,and establish a chain of trust and authentication based on the trusted root , then put this trust relationship extended to the entire computer system through the pass of the authentication mechanism. Trusted Computing Group TCG (trusted computing group) is an industry organization which develops industry standards for trusted computing platform .TCG Trusted Platform Module had posted the main specification [13]of the trusted platform module TPM, which is the root of the credibility of the system coupled with the source of the chain of trust ,in addition it is the core of the credibility mechanism. TPM is a small chip system that can provide a range of password handling functions such as RSA accelerator, SHA-l engine algorithms, random number generator, and storage of key information such as non-volatile key memory and so on ,which contains a variety of password and storage components. These functions can be performed inside the hardware of TPM, while hardware and software agents outside of TPM just provide I / O interface for them, but they can not interfere with the implementation of the internal cryptographic functions of TPM . TPM has three important features: protection, integrity measurement and reporting and authentication. Ability of protection can be tightly protected important data signal line or storage area, so the inside of the data can not be obtained by the physical detection technology. Integrity measurement and reporting means that TPM can accurately and objectively report on whether the state of the system can be trust. Authentication can complete the authentication of net communication and identification of a platform environment configuration of communication objects.

The network data should transfer through a certain number of switches before it reaches to servers. under normal circumstances ,server uses DoS / DDoS attack detection method to determine whether there is an attack. If an abnormality of the network is detected, we can use the switch with a TPM chip which is called trusted switch [14], to verify the identity of the client which sends the request. If so, only the user which has the permission to visit the server, the attack source can also be shield. What should be noted is that the proposed method mentioned in this passage is targeted and limited. Because if the switch opens function of TPM,then only the registered users can access the server. With respect to the net such as Taobao that need registration to access the site, this method can be used to restrict user access. Because of the public nature of its content, public Web sites such as Sina, do not need registration to access, so use of this method to defend against attack is very limited. Specific process is as follows:

1) DoS / DDoS attack detection method monitor whether there is attack. If an abnormality of the net is detected, then notice the switch to open TPM authentication.

2) a request of the server public key PKS (Public Key of Server) to the server, and Client Certification authentication Table CCAT (Client Certification authentication Table), this table is signed by the server, expressed as Sig (CCAT, server). After receiving a request,server send PKS and Sig (CCAT, Server) to the switch.

3) client firstly send requests of access to server to the Switch Request.

4) TPM Random number generator of the switch generates a random number Ri (Random), and send it to the client.

5) After the client receiving the Ri, server which has the authentication of the server sign the random number, then signed random number Sig (Ri, Client) will be sent back to the switch.

6) switches get the client's public key PKC (Public key of Client) from CCAT and decrypt the received Sig (Ri, Client) , and the result is Rj, if Ri = Rj, then it prove that the client is authenticated by the server.

7) and then switch ask the server whether it allows client to access. This is to confirm whether the registered client has been infected and attacks the server. This step can also be complete by switch and server with the dynamic maintenance of a Client Permission Table, CPT records the data that whether the server allows a registered user to connect the server. The switch maintain this CPT signed by the server, the table is initialized to allow all registered clients to access. If the client is detected to be malicious users, the server will notify the switches to modify CPT notification content, meanwhile, forbidding the client to access.

8) the switch establish a virtual connection between the client and server after completing the verification work, and then it goes without switch.

9) When monitoring the attacks stopped, the server notifies the switch to stop validation. The use of random number Ri is aimed to prevent the attacker from attacking in the replay attack way, because the random number is not repeated, thus avoiding the attacker copying the signature on the random number of registered users. random number generator is installed in the TPM chip and

it is based on time stamps.so it fully meet the system's demand for Ri.

D. Certification System Defense

1) intranet identity authentication system should use a unified identity authentication system for the government, the whole network system using such a unified identity authentication not only effectively prevented the theft, but also effectively prevents hacker attacks, which improve the safety and reliability of user information as a whole.

2) public network VPN data across the secure transmission system uses a virtual private network technology, to ensure confidentiality and integrity in the process of data transmission, it conducts strong authentication for dial-up user access, however,in e-government you should adopt a safe VPN system that the cooperative institutions install VPN equipment unitedly. E-government system in general should have the following VPN features: transparency of information encryption and decryption functions; messge authentication function; and firewall work together; support for remote management Function; security audit and alarm functions.

IV. CONCLUSION

This paper analyzes the DoS (DDoS) attack principles and gives a thorough analysis of existing prevention techniques, proposed to prevent DoS (DDoS) attacks in three ways: using a router DoS attack prevention; increase the trusted platform module; increase system defenses. These are effective methods to defend DoS(DDoS) attacks from the angle of practical application.

REFERENCES

[1] CHEN J C, JIANG M C, LIU Yi-wen. Wireless LAN security andIEEE 802. 11i [J]. IEEE Wireless Communications, 2005, 12(1) : 27-36.

[2] XING Xin-yu, SHAKSHUKI E, BENOIT D, et al. Security analysisand authentication improvement for IEEE 802. 11i specification [C] //Proc of IEEE GLOBECOM. New Orleans, LD: [s. n], 2008: 1-5.

[3] KO C, RUSCHITZKA M, LEVITT K. Execution monitoring of securitycritical programs in a distributed system: a specification-based approach [C] //Proc of IEEE Symposium on Security and Privacy. Washington DC: IEEE Computer Society, 1997: 175-187.

[4] SHENG Yong, TAN K, CHEN Guan-ling, et al. Detecting 802. 11MAC layer spoofing using received signal strength [C] //Proc of IEEE INFOCOM. 2008: 1768-1776.

[5] Bagus Arthaya, Ali Sadiyoko, Ardelia Hadiwidjaja. The design of a mazesolving system for a micromouse by using a potential value algorithm [J]. World Transactions on Engineering and Technology Education, 2006, 5(3) : 509-512.