COMP90007 Internet Technologies

Research Report

SYN Flood and defensive strategies

Group member: Wendong Chen

Student ID: 931018

Username: wendongc1

Group member: Yuming Lin

Student ID: 883717

Username: YUMINGL

CONTENTS

1. Introduction

1.1 Background

Denial of service (DoS) is an attack on network devices exploiting defects of network protocol and vulnerabilities of system which renders network or system unavailable. A distributed denial of service (DDoS) is an attack on a host orchestrated by multiple computers scattered in a network, which is more harmful.

1.2 Scope

Currently, DDoS has become a worldwide attack method exploiting vulnerabilities of system. According to statistics in 2014, the number of attacks identified as large-scale DDoS has reached an average of 28 times per hour (Preimesberger, 2014). This paper conducted a research on SYN Flood and proposed a feasible defense method.

2. SYN Flood and common defensive strategies

2.1 Three-way handshake

SYN Flood is the most common and the most effective DoS form. This paper begins with TCP three-way handshake for connection establishment to understand the principle of SYN Flood. The first-step handshake process: a host sends a TCP message including a SYN to a server, informing it of port and initial sequence number for TCP connection. The second-step handshake process: In response, the server replies with a SYN+ACK. The third-step handshake process: after receiving the SYN+ACK, the host sends an ACK to the server. At this point, connection is established (Tanenbaum & Wetherall, 1996) .

2.2 SYN Flood

According to figure 1, an attacker sends multiple SYN requests to the server but does not respond to ACK acknowledgment message, which results in many half-open connections. The server is busy with processing falsified TCP connection requests and has no spare time for requests of legitimate users. In severe cases, stack overflow and server crash will be caused (Lemon, 2002).

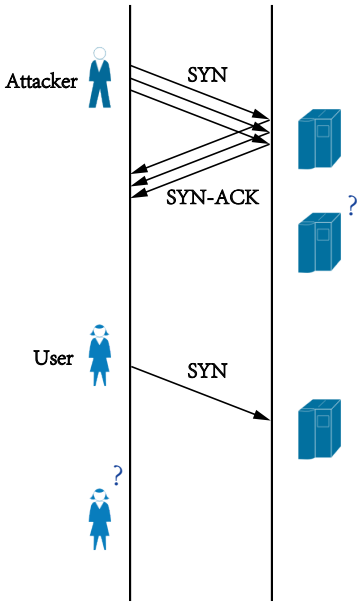


Figure 1 SYN attack

2.3 Common methods

There are some simple and effective countermeasures to SYN Flood. The first is to reduce SYN Timeout value. Lemon (2002) presented that the maximum quantity of half-open connections which can be maintained by a server

$$\text{Max. quantity of half-open connections} = \text{SYN attack frequency} \times \text{SYN Timeout}$$

By reducing SYN Timeout value, a host will release resources occupied by half-open connections as soon as possible, so that server load will be reduced exponentially. The disadvantage of this method is that when SYN Timeout value is reduced, visit of legitimate users may be affected (Eddy, 2007).

The second is to adopt SYN Cookie technique. A server will generate an encrypted sequence number instead of memorizing a sequence number. In the third-step handshake process, the sequence number of ACK message returned by the client is the encrypted initial sequence number plus 1. At this point, the server will run the

same encryption algorithm to regenerate correct sequence number. Connection will be established if the regenerated sequence number is matching to the sequence number of ACK message (Zuquete, 2002). The disadvantage of this method is that hash algorithm has high complexity and will occupy a considerable amount of RAM and CUP resources when attacked. A hacker can wage a targeted ACK Flood attack exploiting this defect (Kiesel, 2002).

One of server-based defense methods is introduced as below, which has been designed to address the shortcomings of the aforesaid two commonly used methods.

3. Receiving two same source SYN messages

3.1 Method introduction

According to JIAN Xiao-chun, WU Zhen-qiang, HUO Cheng-yi, ZHANG Jie (2008, March), two same source SYN messages refer to two SYN messages have the same source address and source port, which request the same service from the same server. The two SYN messages are respectively marked as SYN1 and SYN2. The principle behind this method is that if the client doesn't receive ACK acknowledgement within a certain period of time after the client sends SYN, the client will retransmit a new SYN connection after timeout. As a result, the server will receive two SYN messages with the same source address and port number within a certain period of time, then judge whether the request is legitimate based on time difference.

3.2 Method analysis

Firstly, retransmission time difference is defined:

X = the time when SYN packet is received for the second time - the time when SYN packet is received for the first time

Reasonable time period X = {x| $T_{\min}$ < x < $T_{\max}$}, in which T_{min} refers to minimum

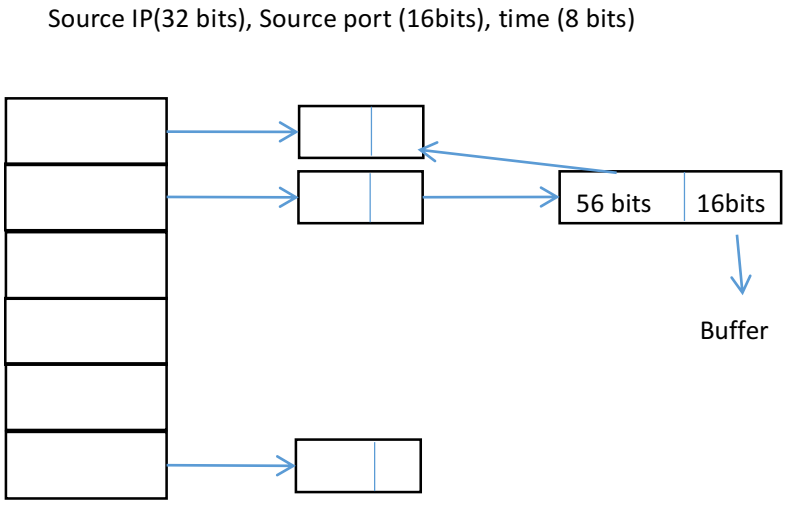
value of retransmission time difference, which is defined as the time of timeout retransmission of the server (generally several seconds). T_{max} refers to maximum value of retransmission time, which is defined as double of the time of timeout retransmission of the server(JIAN et al., 2008).

Therefore, a reasonable connection request needs to satisfy the below conditions:

1. $time_{SYN2} - time_{SYN1} \subseteq X$
2. $IP_{SYN2} = IP_{SYN1}$
3. $port_{SYN2} = port_{SYN1}$

Only SYN message which satisfies the above-mentioned three conditions can enter the third-step handshake process, while other SYN requests will be abandoned with only source address and reception time saved to retransmission time $T_{\max}$. In DDoS, different from DoS in which superfluous SYN connection requests are sent using an address, SYN messages are sent using different IP and ports. The method of receiving two same source SYN messages can effectively judge whether there is a DDoS malicious attack (JIAN et al., 2008).

As shown below, this paper introduces in details how to receive and record two same source SYN messages. Firstly, a HASH table is created to record SYN message sent from the client for the first time. Secondly, a HASH function is determined with 16-bit port number of 32-bit source IP address as a key. In consideration that an attacker usually uses an random function to forge its IP source address, therefore use HASH(s)=s mod 65535. In which, “s” refers to 48-bit source IP address and source port number. The definition domain is (00000000,0000~FFFFFFFF,FFFF). Each HASH table node stores contents such as source IP, port and time (JIAN et al., 2008).



Graph 2 Hash Table Structure

The below formula can be concluded using η (usage ratio of total memory) of the HASH table:

$$T = \frac{\eta \times \text{Total memory}}{\text{SYN attack frequency} \times \text{Each hash node length}}$$

Based on the optimum η given by experts from the server side, update time T of HASH table can be achieved. With a cycle of T, traverse the HASH table to release space of timeout nodes so as to prevent the overflow of HASH table (JIAN et al., 2008).

JIAN et al.,(2008) explain that if the server is not overloaded, it means an attack has not been received. Go through TCP three-way handshake process as normal. If the server is overloaded, use this method to check if each SYN message received has been stored in the HASH table. The below three circumstances exist:

- If there is no record of the SYN in the HASH table, establish a new record and abandon the SYN message
- If there is a record of the SYN in the HASH table, but time difference falls out of a reasonable scope, abandon the SYN request and update the time recorded in the HASH table.
- If there is a record of the SYN in the HASH table, and time difference falls within a reasonable scope, a legitimate connection request is determined. In such case, go

through TCP three-way handshake process and release node space in the HASH table.

4. Method Summary

If a SYN Flood attack has not been received, a server functions normally. If such an attack is received, this method works in various circumstances:

- An attacker continuously sends SYN packets using a forged IP address and then forges an IP address again. Time difference of sending continuous SYN is obviously less than reasonable time period X. The method works because a server abandons a SYN packet after receiving it each time and updates the time in a HASH table. In other words, no half-open state of connection exists.
- An attacker discontinuously sends SYN messages and directly changes IP addresses. A server abandons SYN packets and a HASH table is updated after timeout. The method works because if an forged IP is reused for a long time, time difference is obviously larger than normal interval.

This method effectively blocks a SYN Flood attack and addresses the shortcomings of the aforesaid methods. Its advantages lie in simple strategy and calculation as well as low consumption of system resources.

5. Conclusion

This paper first introduces DoS and analyzes in detail general attack process and form of SYN Flood. Besides, two methods, which are widely used nowadays to prevent SYN Flood, are introduced. This paper then explains in detail the method of receiving two same source SYN messages. In this method, normal time interval is first set up, a HASH table is then adopted for recording reception time of SYN messages and whether SYN messages should be abandoned is determined after comparing reception time with normal time interval, which effectively prevents and blocks DDoS. In the end, the paper compares this method with other two commonly used methods in terms of advantages and shortcomings.

A simple and effective method to prevent and block DDoS is to increase safety awareness of computer users. Vulnerabilities of operating system should be timely patched and network security devices and software should be updated so that malicious software attacks can be blocked and DDoS scale can be reduced.

Word count: 1500 words

Reference

Chang, R. K. (2002). Defending against flooding-based distributed denial-of-service attacks: a tutorial. IEEE communications magazine, 40(10), 42-51.

Eddy, W. M. (2007). TCP SYN flooding attacks and common mitigations.

JIAN Xiao-chun, WU Zhen-qiang, HUO Cheng-yi, ZHANG Jie (2008, March). Method of defending SYN Flooding attack by receiving two same source SYN packets:Computer Engineering and Design (Vol. 29 No. 6)

Kiesel, S. (2002). On the use of cryptographic cookies for transport layer connection establishment. Proc. EUNICE Summer School, 177-184.

Lemon, J. (2002, February). Resisting SYN Flood DoS Attacks with a SYN Cache. In BSDCon (Vol. 2002, pp. 89-97).

Preimesberger, C. (2014). DDoS attack volume escalates as new methods emerge. Eweek.

Tanenbaum, A. S., & Wetherall, D. (1996). Computer networks (pp. I-XVII). Prentice hall.

Zuquete, A. (2002). Improving the functionality of SYN cookies. In Advanced Communications and Multimedia Security (pp. 57-77). Springer, Boston, MA.

Individual Reflection

Wendong Chen:

When doing the research, I had a clear division of work with my group member. Selecting the topic at first, then searching and reading scholarly literature individually. After the preliminary study, we selected the direction for further study which is SYN Flood. When writing the paper, we are responsible for writing different parts of the article, exchanging the results and discussing with each other until the report has been finalized.

The research report focuses on theoretical research: reading academic literatures, extracting key points, analyzing and summarizing. The difficulty lies in the in-depth study. The network analysis focuses on the practical application, repeatedly experimenting and summarizing the conclusion. The difficulty lies in the complexity of the actual network that the real condition is far more complicated than the textbook theory.

Yuming Lin:

The network analysis assignment allowed me to learn the relationship between bandwidth, distance, and routing. However, due to the instability of the testing environment and the insufficient number of test sites. Therefore, many problems cannot get a reliable conclusion. Nowadays, as long as the hardware is good enough, distance can no longer effectively affect the delay and jitter.

The research of the dissertation gave me detailed and in-depth understanding of network DoS attacks, especially SYNLlood. In addition to that, I also learned about other DoS attack. In conclusion, there is never a perfect network protocol in the world. The difficulty is how we can find out what is missing and protect the computer from attack.

From the discussion to determine the subject, review the literature and write the paper.

We completed these together. Before we starting to write a module, we will hold a group meeting. The difficulty is to analysis and comparison the advantages and disadvantages of different defensive methods, and then integrate the articles together.