Research on tor-based anonymous DDoS attack

Rui Wang^{1,*}, Zhiye Yang², Kun Li¹, Chen Chen¹, and Yanru Chen¹

¹Department of Information Security, First Research Institute of the Ministry of Public Security of PRC, Beijing China

²Network Security Detachment, Beijing Railway Public Security Bureau Tianjin Public Security Bureau, Tianjin China

Abstract. Based on Tor, an anonymous DDoS attack is proposed, and the attacker of this attack is very difficult to trace due to the strong anonymity of Tor. Through conducting experiments in different network environment and making analyzation of security, the experiments results demonstrate the effectiveness of this attack, and the strategy to defense the attack is also discussed.

1 Introduction

The Onion Router (Tor) is the most popular low-latency anonymous communication network. There are more than 2 million users, 7000 nodes and 8000 descriptors (one node can run two different descriptors) in the world. Denial of service (DOS) attack is considered to be one of the main threats to network security, and can be divided into network layer DoS attack and application layer DoS attack. DOS in network layer consumes resources of the target by flooding, which can be effectively defended by filtering the source IP address. In order to break through the limits, Sergey [2] et al. proposed an effective low bandwidth based DoS attack scheme, Park[3] et al. implemented and analyzed this attack in detail, and used the vulnerability of application layer protocol to complete this DoS attack. However, attacks from only a single node or several nodes are easily detected and blocked by target server. Distributed denial of service (DDoS) attacks can improve this situation, but the effect is limited.

In this paper, an anonymous slow read DDoS attack based on tor network is proposed and simulated in the actual network environment based on slowhttptest [4]. It is found that the effect of normal slow read DoS attacks is not only determined by the timeout parameter, but also affected by the network read permissions. If the attacker's IP address is filtered by the server, the attack will not take effect. However, when an attack is launched through tor network, the attacker can avoid the limitation of timeout parameters and IP filtering by taking advantage of the replaceable exit route and tor network's strong anonymity.

2 Tor based slow read DDoS attack

* Corresponding author: ruiwang114@163.com

2.1 Basic ideas

The encryption link of tor network takes exit router as the end point, and only the exit route can be used as a bridge between tor network and Internet. Starting from the exit route, network traffic reaches its final destination through Internet. Attackers can connect to the tor network before launching attacks and use tor nodes as cover.

2.2 System model

Because tor network does not support user authentication mechanism [1], attackers can disguise as ordinary users to access tor network, establish multiple links with target server to exchange data with the victim at a very low speed. By occupying and exhausting available connections and network resources of the victim, making the target cannot respond to normal users’ requests and making it denial of service.

The model of tor based DDoS attack is shown in Figure 1. $R = \{R_1, R_2 \dots, R_n\}$ is used for all tor nodes, $A = \{A_1, A_2 \dots, A_n\}$ is for n attackers, $n = \{n_1, n_2 \dots, n_n\}$ is for malicious links, V is for target server, and R_i is for intermediate node and leaf node.

An attack path is the intermediate node between A_i and V . for example, the attack path between A_i and V is $n_1 = (R_1, R_3, R_3)$ and the attack path is not unique.

- The characteristics of tor based DDoS slow read attack are as follows:
- Each link avoids being tracked through multiple routes;
 - Several attackers launch attacks together, resulting in continuous denial of service;
 - Attacked target can only trace to the exit route;
 - Transmission rate of tor network often fluctuates and slows, but it becomes an advantage of slow read attack, because the transmission rate can be ignored by slow read attacks, and the real network fluctuations make the attacks more difficult to detect.

Fig. 1. Tor based DDoS attack model.

2.3 Feasibility analysis

Firstly, the main factors affecting DoS attack are analyzed. The premise of a successful DoS attack is to satisfy $M < N$. there are two different situations in calculating $N(t)$ (the meanings of each variable are shown in Table 1)

$$t_o \geq t_r, N(t) = C \times t$$

(1)

In Eq. 1, the timeout parameter T_o is large enough that an attack launched by an attacker ends at T_t , and the effective state of the attack can last until T_o .

$$t_o < t_t, N(t) = \begin{cases} C \times t & (t < t_0) \\ C \times t - K \times (t - t_0) & (t \geq t_0) \end{cases} \tag{2}$$

In Eq. 2, $t \geq 0$ represents the duration of the attack. In this case, because $t_o < t_t$ is tiny, the connection of the attack will be invalid in a very short time, so the attack is difficult, and the effect of the attack can be ignored. Therefore, the attacker needs some conspirators to launch DDoS attacks to achieve the target.

Table 1. Variable description.

Parameter	Description
t_0	Timeout
t_t	Time to send all attack connections $t_t=N/C$
N	Total number of attack connections
C	Attack connections per second
K	Number of connections broken per second after timeout
M	Number of connections broken per second after timeout
$N(t)$	Total number of attack connections at timestamp t

The basic idea to keep the attack persistent is to send a new attack connection before the previous attacker's t_t . Therefore, other collusive attackers need to repeat this process to maintain the attack effect.

When an attacker launches a DDoS attack, it is assumed that N attackers $A_{t_1}, A_{t_2}, ..., A_{t_n}$ are currently connecting to the target server. An attacker $A_{t_k} (2 \leq k \leq N)$ attacks at t_{a_k} :

$$t_{a_k} = \sum_{i=1}^N \frac{N_i}{C_i} \quad (k \in [2, n]) \tag{3}$$

Consider a DDoS attack launched by three attackers. parameters of the server and each attacker are shown in Table 2. In order to satisfy $t_o < t_t$ and $MC / SL = 300$, attacker must keep more than 300 valid connections with the server. The ideal attack effect is shown in Figure 2. In theory, the effective time of the attack can last about 50 seconds. The second part describes the experimental results in detail.

Table 2. Parameter setting of simulation attack.

Parameter	Value
Timeout	100
Server limit	300
Max clients	300
Connection rate	50
Total connections	1000

3 Experiment and evaluation

2.1 Experimental deployment

Experiments are carried out in two environments: ordinary Internet and tor network, as shown in Figure 3. An apache (version 2.4.7) server was deployed on a Linux (CentOS 6.5) server, and a 92kb web page was run, and the open source tool slowhttptest (version number 1.6) was modified for testing. Tcpdump is used to observe and grab the packets between the attacker and the server. Apache server run in the perfork MPM (Multi Processing Modeule) mode, parameters are shown in Table 3 and the parameters of slowhttptest are shown in Table 4. According to the experimental results, it is found that attacks can be successfully implemented in both experimental environments, and the experimental data obtained were very close. Therefore, this paper only showed and analyzed DDoS attacks in tor network environment.

Fig. 2. DDoS attacks in ideal situation

Fig. 3. DDoS attacks in ideal situation

Table 3. Prefork MPM model.

Parameter	Value
KeepAlive	Off
StartServers	8
MinSpareServers	5

MaxSpareServers	20
ServerLimit (SL)	256
MaxClients (MC)	256
MaxRequestChild	4000

Table 4. DoS attack settings.

Parameter	Value
Total connections	500
Receive window range	8-16 byte
Pipe coefficient	1
Buffer read rate	5 byte/s
Connection rate	50
Probe connection timeout	10
Use proxy	none or tor

2.2 Experimental result

Experiments 1 and 2: results of Experiment 1 are shown in Figure 4. At 19th second, the established attack connections reached 448 (MC/SL), and the number of pending connections was 52. The attack then took effect and the server refused service. However, by setting the timeout parameter, the attack connections begin to decline after 109 seconds and the server can access normally. The attack lasted 250 seconds, and the attack took effect for 100 seconds.

Fig. 4. Timeout 100, MC/SL 300.

Although MC/SL is set to 300, the maximum number of TCP connections established is 462. The extra 162 connections are half connected with three handshakes. Since the timeout is set to 100, the number of connections to attack begins to decline after 101 seconds, and the total number of connections is less than MC/SL, so the server resumes service. As shown in Figure 4, the attack takes effect from 19th to 109 seconds.

Experiment 3 and 4: the experimental results are shown in Fig. 6 and Fig. 7. The attack cannot take effect because the server has sufficient resources. Through these two experiments, the target server still works normally under the attack, and the timeout

parameter still takes effect in 135 seconds. From the server status page of Apache, we observe that the number of child processes is about 520. This is because the total number of attack connections is 500, and the MaxSpareServer parameter is configured to 20, as shown in Table 2.

Fig. 5. Timeout200, MC/SL 300.

Fig. 6. Timeout 100, MC/SL 600.

Fig. 7. Timeout 200, MC/SL 600.

Experiment 5: as shown in Figure 8, the attack took effect for 8 seconds, mainly because the timeout parameter was set very short (10 seconds).
Through above five experiments, it can be determined that the timeout parameter is the decisive parameter to determine the effective time of the attack, and it also proved that the effect of slow read DoS attack with only one attack source is limited. Moreover, whether

the attack can take effect depends on three parameters: timeout, MC/SL and the total number of attack connections.

- Timeout: setting a short timeout can effectively prevent DDoS attacks, but QoS and user experience will be significantly reduced.
- MC/SL: setting too small will limit the available resources of the server.
- Attack total number of connections: theoretically, the more connections, the stronger the attack effect. However, the maximum number of attacks an attacker can launch is limited by the performance of his machine, and if all the attack connections come from one or only a few IP addresses, the attack can be easily detected.

Fig. 8. Timeout 10, MC/SL 300.

Fig. 9. 3 attack sources timeout20, MC / SL 300.

Experiment 6: the results are shown in Figure 9. The server denial of service lasted about 68 seconds (10 to 78 seconds) longer than the ideal 54 seconds. By comparing the results under the theoretical state (Fig. 2) and the experimental state (Fig. 9), it is found that:

● Time interval for child process creation

As shown in Figure 9, the attack takes effect after 10 seconds. However, in theoretical case shown in Figure 2, the attack should take effect after 6 seconds, and there is a 4 second delay between the actual situation and the theoretical state, which is caused by the creation of the sub-process. By predicting this delay, the attack effective time can be set more accurately.

● The influence of semi join

As shown in Figure 2, the attack will fail after 61 seconds, but in practice it will last for 78 seconds. This is because when the established connection timeout, the half connection in

the waiting state starts to take effect, thus maintaining effective state of the attack. So the attack takes longer in experimental case than in theoretical case.

4 Defense strategy

4.1 Defense strategy of application layer DDoS attack

Application layer DDoS attack is one of the main threats to Internet security. Zhang Yongzheng et al. [6] analyzed in detail the detection and control methods of application layer DDoS attacks, and analyzed the advantages and disadvantages of different control methods deployed in different network environments; Wang Jin et al. [7] focused on attack based on HTTP flooding, and proposed a detection scheme based on the deviation statistical model; Wang Fengyu et al. [5] analyzed stability of external connection behavior from the network community level, and gave the This paper presents a method to help web server Detect application layer DDoS. This scheme can not only detect abnormal access behavior, but also effectively distinguish burst access and application layer DDoS. Sun Zhixin et al. [8] proposed a detection and defense DDoS model based on aggregation algorithm.

On the one hand, Internet service providers (ISPs) can improve network facilities to mitigate the impact of DDoS attacks, such as increasing bandwidth, enhancing processing capacity and rationalizing network deployment structure, on the other hand, ISPs can adopt specific defense technologies at the gateway:

(1) Dynamic challenge algorithm

In transport layer and application layer, protocol stack simulation behavior is used instead of the server to return packets and send dynamic challenge information to users. Only users who can complete the challenge can access the server. SYN cookie, DNS cookie and sip cookie are commonly used dynamic challenge algorithms.

(2) Multi level restrictions

Traffic restrictions based on different network levels and granularity are adopted, such as from source IP, destination IP, and session of transport layer and application layer.

(3) Intelligent access control

Flexible control strategy is adopted from network layer to application layer. Taking HTTP protocol as an example, ISP can adopt discard, trust and speed restriction policies for different URL, user agent and cookie; for DNS protocol, ISP can set similar policies for query name, type and resource information recorded in network information.

(4) Behavior analysis and credit mechanism

Based on the data analysis technology, the traffic characteristics and IP behavior are modeled and analyzed. A credit database containing IP, URL and file information is established. Abnormal traffic fingerprint features are output in time, and the traffic is automatically cleaned up. This mechanism can effectively prevent botnet and abnormal packet attacks, such as slowloris header.

4.2 Defense strategy of application layer DDoS attack

By analyzing our experimental results, if an attacker can accurately analyze the creation delay of the subprocess and the time required to process the semi connection, an attacker can launch a more effective DDoS attack, even if the timeout parameter of the target server is very short. In order to effectively prevent slow read DDoS attacks, the server should consider strictly controlling the client TCP transmission window that is accessed. If the window of some connections is set to be very small, we can detect and disconnect these

connections to protect against DDoS attacks. However, because the access window of wireless network and mobile terminal is very small, the efficiency of this kind of user will be very poor when using this defense measure.

For the anonymous DDoS Attacks Based on tor network, another effective defense measure is to obtain the information of all nodes from tor's official website. When the user IP address of the server is in the list, the TCP window is strictly monitored.

5 Conclusion

This paper proposes an anonymous slow read DDoS attack based on tor. We analyze the relationship between DoS attack and its three important factors, and carry out experiments in Internet environment and tor network environment respectively. The experimental results show that our scheme can not only effectively cause denial of service of the target server, but also provide good anonymity. Moreover, our scheme has stronger attack ability than ordinary DOS. We also discuss and give the defense measures against this scheme. We will further study and deploy the detailed defense scheme in the future work, and find a more reasonable balance between system security and QoS.

This work was supported by the National Key R&D Program of China(No. 2018YFB0804704) .

References

1. Syverson P, Dingledine R, Mathewson N. Tor: the second-generation onion router[C]// Usenix Security. 2004.
2. Shekya S. Are you ready for slow reading?[J]. QUALYS BLOG, Available: <https://community.qualys.com/blogs/securitylabs/2012/01/05/slow-read> (Last access: Dec. 12, 2014), 2012.
3. Park J, Iwai K, Tanaka H, et al. Analysis of slow read DoS attack[C]// Information Theory and its Applications (ISITA), 2014 International Symposium on. IEEE, 2014: 60-64.
4. Shekya S. slowhttpstest-Application Layer DoS attack simulator[J]. accessed on, 2013, 8.
5. WANG F Y, CAO S F, XIAO J. Method of Detecting Application-Layer DDoS Based on the Out-Linking Behavior of Web Community [J]. Journal of Software, 2013, 6.
6. Zhang Y Z, Xiao J, Yun X C, et al. DDoS attacks detection and control mechanisms[J]. Journal of Software, 2012, 23(8): 2058-2072.
7. Wang J, Yang X L, Long K P. Http-flood DDoS detection scheme based on large deviation and performance analysis[J]. Journal of Software, 2012, 23(5): 1272-1280.
8. Sun Z X, Jiang J L, Jiao L. DDOS attack detecting and defending model[J]. Journal of Software, 2007, 18(9): 2245-2258.