

Research on SynFlood Attack Target Locating Method

Liu Huiyu

school of computer sci. & tech.
huazhong univ. of sci. & tech.
wuhan,china
e-mail : liuhuiyu@mail.hust.edu.cn

Chen Kai

school of computer sci. & tech.
huazhong univ. of sci. & tech.
wuhan,china
e-mail :
kchen@mail.hust.edu.cn

Chen Xiaosu

school of computer sci. & tech.
huazhong univ. of sci. & tech.
wuhan,china
e-mail : x_s_chen@mail.hust.edu.cn

Abstract- This paper proposes a new SynFlood attack target location method based on the Abnormal TCP Connection Graph (ATCG). The method build an Abnormal TCP Connection Graph based on the status of TCP connections. Then the method calculates the Abnormal Source Number (ASN) and Attack Intensity (AI). If such two values exceed the threshold defined in advance, the node which the IP address indicated can be determined as attack target. The simulation results indicate that the method has favorable accuracy and higher data packet processing capability. It can be deployed at the backbone router in a large or medium-sized network.

Keywords- SynFlood Attack, Abnormal TCP Connection Graph, Attack Intensity

I. INTRODUCTION

Along with the rapid development of computer network, the problem of network security increasingly sharpens. Ways of attack emerge one after another. The SynFlood attack is a common attack means, but it is difficult to detect and defend. It imposes Three-way handshake mechanism in the TCP protocol. Numerous attackers send Syn segments to the target(s) at a certain rate, and discard the Syn+Ack segment responded by target in order to suspend the third step of Three-way handshake mechanism. The target will pre-assign resources for the establishing connection when it responds with Syn+Ack segment after it has received the Syn segment. It assembles the Timeout mechanism while pre-assigning resource to avoid misuse of resource. But the resource of target will be used out if the attacker sends the Syn segment exceeding certain rate. As a result, the target cannot accept any new connection establishment request. This means the target crashed ^[1].

To defend the SynFlood attack, many methods have been proposed, such as Syn Cache ^[2], Syn Cookies ^[3], Syn Proxying ^[4], Syn Defender ^[5] and Syn Kill ^[6]. These methods were deployed at the server which needs to be protected or deployed at the gateway firewalls which are connected to the network embodying the server. That means these methods can only protect a certain server; they cannot detect and defend the SynFlood attack in the entire network scope.

It is required to locate the attack target and trace back to attack source, then it can be possible to detect and defend SynFlood attack initiatively. And the result of locating and tracing will affect the effect of attack defending directly. This paper will build Abnormal TCP Connection Graph based on the TCP connection status, and then propose a new SynFlood attack target locating method. The method can be deployed at the backbone routers and work with the SynFlood attack detecting method to locate the attack target.

The rest of this paper is organized as follows: Section 2 analyze the features of SynFlood attack; Section 3 will propose the Abnormal TCP Connection Graph, and describe the SynFlood attack target locating method; Section 4 simulates the locating method in an actual SynFlood attack environment and analyzes the method's accuracy and effectiveness. Finally, conclusions and discussions are proposed in Section 5.

II. SYN Flood ATTACK FEATURE ANALYSING

Based on the prophase work ^[7] and several times SynFlood attack, it is clear that the SynFlood attack have features show as follows:

- (1) Attack target are certain one or some network nodes, and they always have true IP address;
- (2) The attack target will be attacked by numerous source nodes during a short time, or be attacked numerous times by one source node;
- (3) During a certain attack process, the source port and the target port are generated randomly.

So the work that this paper doing will based as follows:

- (1) The source dataset is the output of SynFlood attack detecting method proposed in [7];
- (2) This paper only considers the IP address of attack target, not consist the port of attack target.

III. SYN Flood ATTACK TARGET LOCATING METHOD

A. Abnormal TCP Connection Graph

1) Basic Teams

During SynFlood attacking process, a valid target will be attacked by numerous nodes during very short time. The attack behaves as jillion TCP half connections are established in network. So we can build Abnormal TCP Connection Graph to describe the status of abnormal TCP connections based on the segments' interactive sequence during normal TCP connection establishing process and SynFlood attacking process. Then we can locate the attack target by analyzing the Abnormal TCP Connection Graph. This paper assumes any connection is abnormal connection before it accomplishes full Three-Way Handshake process.

Definition 1 TCP Connection Source Point (TCSP): The IP address of the node which request to establish the TCP connection initiatively.

Definition 2 TCP Connection Target Point (TCTP): The IP address of the node which respond for the TCP connection establishing.

Definition 3 TCP Connection Source Sequence No (TCSSN): The sequence no of first segment during Three-Way Handshaking process.

Definition 4 TCP Connection ACK Sequence No (TCASN): The sequence no of second segment during Three-Way Handshaking process.

Definition 5 TCP Connection Serial No (TCSN): This value indicates a certain TCP connection during a certain TCP Connection Source Point (TCSP) and a certain TCP Connection Target Point (TCTP).

Definition 6 TCP Connection Status Edge(TCSE):The edge which connect a TCP Connection Source Point(TCSP) to a TCP Connection Target Point(TCTP), indicated by(TCSP, TCTP, TCSSN, TCASN, TCSN).

Definition 7 Abnormal TCP Connection Source Point Set (ATCSPS): The set which composed by TCP Connection Source Points which belong to abnormal TCP connections passed via router.

Definition 8 Abnormal TCP Connection Target Point Set (ATCTPS): The set which composed by TCP Connection Target Points which belong to abnormal TCP connections passed via router.

Definition 9 Abnormal TCP Connection Status Edge Set (ATCSES): The set which composed by TCP Connection Status Edges which indicate abnormal TCP connections passed via router.

Definition 10 Abnormal TCP Connection Graph(ATCG):This definition describe status of all abnormal TCP connections passed via router, indicated by(ATCSPS, ATCTPS, ATCSES).

2) Building and updating of Abnormal TCP Connection Graph

The time duration which exist SynFlood attack can be detected by the work described in [7].Every segment during such time duration will be analyzed to build and update Abnormal TCP Connection Graph. Each new TCP connection will not be looked upon as a normal TCP connection until it fulfill Three-Ways Handshaking process while the segment processing. The detail processing follow as below:

(1) If the segment is SYN segment

a) Get source IP address, target IP address and sequence no;

b) Judge the source IP address is in Abnormal TCP Connection Source Point Set(ATCSPS) or not and judge the target IP address is in Abnormal TCP Connection Target Point Set(ATCTPS) or not;

c) If the source IP address is not in ATCSPS and the target IP address is not in ATCTPS, then

i. Add the source IP address to ATCSPS;

ii. Add the target IP address to ATCTPS;

iii. Add a element (source IP address, target IP address, segment sequence no, 0, 1) to ATCSES;

d) If the source IP address is not in ATCSPS and the target IP address is in ATCTPS, then

i. Add the source IP address to ATCSPS;

ii. Add a element (source IP address, target IP address, segment sequence no, 0, 1) to ATCSES;

e) If the source IP address is in ATCSPS and the target IP address is not in ATCTPS, then

i. Add the target IP address to ATCTPS;

ii. Add a element (source IP address, target IP address, segment sequence no, 0, 1) to ATCSES;

f) If the source IP address is in ATCSPS and the target IP address is in ATCTPS, then find an element in ATCSES which first field's value is source IP address and second field's value is target IP address

i. If such element doesn't exist, then add a element (source IP address, target IP address, segment sequence no, 0, 1) to ATCSES;

ii. If such element does exist, traverse all such elements and get the max value of the fifth field call it SNMax, then add a element (source IP address, target IP address, segment sequence no, 0, SNMax+1) to ATCSES;

(2) If the segment is SYN+ACK segment

a) Get source IP address, target IP address ,sequence no and ACK no;

b) Judge the source IP address is in Abnormal TCP Connection Target Point Set(ATCTPS) or not and judge the target IP address is in Abnormal TCP Connection Source Point Set(ATCSPS) or not;

c) If the target IP address is in ATCSPS and the source IP address is in ATCTPS, then find an element in ATCSES which satisfied with follows:

i. The first field's value is target IP address;

ii. The second field's value is source IP address;

iii. The third field's value is (ACK no - 1);

iv. The fourth field's value is 0;

If such element is existed, then update such element's fourth field's value with the segment's sequence no;

d) Do nothing for other case;

(3) If the segment is ACK segment

a) Get source IP address, target IP address ,sequence no and ACK no;

b) Judge the source IP address is in Abnormal TCP Connection Source Point Set(ATCSPS) or not and judge the target IP address is in Abnormal TCP Connection Target Point Set(ATCTPS) or not;

c) If the source IP address is in ATCSPS and the target IP address is in ATCTPS, then find an element in ATCSSES which satisfied with follows:

- i. The first field's value is source IP address;
- ii. The second field's value is target IP address;
- iii. The third field's value is (sequence no - 1);
- iv. The fourth field's value is (ACK no - 1);

If such element is existed, then delete such element from ATCSSES;

d) Do nothing for other case.

B. Attack target locate thinking

As discussed above, the Abnormal TCP Connection Graph should be updated according to each segment during the time duration detected by SynFlood attack detect method proposed in [7]. After all segment processed, the Abnormal TCP Connection Graph will describe all possible abnormal TCP connection during the time duration, such as the source IP address, the target IP address of each connection.

As discussed in section 2, the attack intention could be achieved by using numerous nodes trying to build abnormal TCP connection with the attack target to exhaust the resource of attack target. So, each connection in Abnormal TCP Connection Graph can be treated as a SynFlood attack. To describe the attack status, defined two parameters which named Attack Source Number (ASN) and Attack Intensity (AI).

Definition 11 Attack Source Number (ASN): The number of source node which attack the target.

Definition 12 Attack Intensity (AI): The average number of attack which the target suffered per time unit. It can be calculated by (1).

$$AI = (\text{All attack number} / \text{ASN}) / \text{length of time duration} \quad (1)$$

To really damage the target node, it need huge numerous source node to attack the target node frequently. This mean there exist threshold for ASN and AI. The attack can achieve the goal only when the ASN and AI exceed one certain threshold. Thus we can set Threshold of Attack Source Number (TASN) and Threshold of Attack Intensity (TAI) to help locate the attack target.

C. Algorithm description

(1) Detect the existence of SynFlood attack by using the method proposed in [7]. If existed, get all segment during the time duration which attack existed;

(2) Build ATCG of the attack time duration;

(3) Calculate ASN and AI for each node in ATCTPS:

- a) If $ASN \geq TASN$ and $AI \geq TAI$, then the node is the attack target;
- b) Else, the node is not the attack target.

IV. SIMULATION AND RESULT ANALYSIS

A. Simulation Platform

Table I gives out the platform for the simulation.

TABLE I. SIMULATION PLATFORM

CPU	Intel Core2 Duo T5600
Memory	2GB DDRII 533
OS	Windows XP Pro SP3
Language	C# 3.0

B. Simulation Dataset

This paper adopt the dataset from file dec-pkt-1.sf which concluded in the dataset dec-pkt-1 come from The Internet Traffic Archive to acted as background network flow.

The dataset's feature described below:

(1) The dataset only conclude SYN segment, FIN segment and RST segment, which indicated by S, F and R separately;

(2) The dataset do not conclude ACK segment. The second segment of the Three-Way Handshaking is indicated by S which should be SYN+ACK segment, and the third segment which should be ACK segment is absence;

(3) All nodes are indicated by Integer furthermore IP address.

The dataset is pretreated as below to get fit dataset which can be used in the simulation:

(1) Insert ACK segment: Assume that node x connect to node y on its own. In such case, if there exist an S segment from node x to node y, and exist a S segment from node y to node x, then we can consider that there exist a normal TCP connection between node x and node y. For which, we act as below:

a) Update the S segment from node y to node x with SA segment to indicate SYN+ACK segment;

b) Insert an A segment from node x to node y to indicate ACK segment;

(2) Insert SynFlood attack dataflow during the time duration from 2180s to 2240s with the rate at 3000pps. We set the source node marked by the integer from 0 to 99, and set the target node marked by the integer from 0 to 10.

C. Parameters Setting

The parameters involved in the location algorithm are TASN and TAI. TASN indicate the extent of attack source, and TAI indicate the frequency of attack. The attacker will use numerous source nodes to attack the target node in a upper frequency during the SynFlood attack process. But it will really harm the target node only when the number of source node and the frequency of attack is higher than a certain value. We can locate the node target by such certain value. But the value of TASN and TAI should not be set too high for that will miss some real target node. After simulating with different parameter combinations, this paper decides TASN and TAI use the value shown in table II finally.

TABLE II. PARAMETERS SETTING

TASN	100
TAI	50

D. Simulation Result Analysis

Based on the parameters in table II and the dataset described in section 4.2, table III gives out the simulation results.

TABLE III. SIMULATION RESULT

Target Node	ASN	AI
0	100	180.9
1	100	182.6
2	346	68.7
3	100	178
4	100	175.2
5	137	150.73
6	100	181.6
7	100	183.2
8	155	122.4
9	100	185.3

Table III indicates that 10 target nodes are all located accurately. These nodes' ASN and AI's value are exceeding TASN and TAI separately. That's mean the algorithm's accuracy rate is 100%, the rate of false location is 0%, and the rate of miss location is 0%.

V. CONCLUSION

Based on the mechanism of TCP Three-way Handshaking and the theory of SynFlood attack, this paper introduces the Abnormal TCP Connection Graph to describe the abnormal TCP connection existed in the network, and regard the abnormal TCP connection as attack.

To achieve the attack intention, it needs numerous source node to attack the target node frequently. So propose two parameters named Attack Source Number and Attack Intensity to evaluate the attack status which target node which in the ATCG suffered. This paper set threshold for above two parameters to distinguish the victim node and the no-harmed node. All these doing can help locate the attack target node exactly.

It must be pointed out that, though the accuracy of the detection algorithm is up to 100% based on dec-pkt-1 Dataset, the threshold affect the result seriously. At the same time the algorithm can only used in direct SynFlood attack scene. So the remaining work will focus on how to get the optimal threshold in a certain attack scene, and we'll also focus on how to locate the target node in the reflect SynFlood attack scene. We want the locating algorithm will be more practicability.

REFERENCES

- [1] CHEN Bo, "Principle Implementation and Defense of SYN Flood Attack", Application Research of Computers, SiChuang, China, 2003, vol.12, 80~83.
- [2] J.Lemon, "Resisting SYN Flooding DoS Attacks with a SYN Cache", Proceedings of USENIX BSDCon'2002, February, 2002.
- [3] D.J.Bermtan and Eric Schenk, "Linux Kernel SYN Cookies Firewall Project", <http://www.bronzesoft.org/projects/scfw>.
- [4] Netscreen 100 Firewall Appliance, <http://www.netscreen.com/>.
- [5] Check Point Software Technologies Ltd. SynDefender: <http://www.checkpoint.com/products/firewall-1>.
- [6] C. L. Schuba, I. V. Krsul, M. G. Kuhn, E. H. Spafford, A. Sundaram and D. Zamboni, "Analysis of a Denial of Service Attack on TCP", Proceedings of IEEE Symposium on Security and Privacy, May 1997.
- [7] Liu Huiyu, Chen Kai, Chen Xiaosu. SynFlood attack Detection based on Distance computation in Space Geometry: Proceedings of 2010 International Conference on Computer Application and System Modeling, 2010[C]. Taiyuan, Shanxi, China: IACSIT, 2010: V4-585-V4-591.
- [8] Detection Scoring Truth : <http://www.ll.mit.edu/mission/communications/ist/files/masterlistfile-condensed.txt>