Defense method against TCP SYN flooding Attack

Ms. Mrudula R. Thakre
M.Tech. III Sem (Comp. Sci. & Engg)
PG Dept. Of CSE
G. H. Raisoni COE,Nagpur
91-9881129315,91-712-2239948
mrudula_thakre@yahoo.co.in

Mr. Manish B. Gudadhe
M.E. II Sem (Wireless CC)
PG Dept. Of CSE
G. H. Raisoni COE,Nagpur
91-9881129815,91-712-2239948
mbgpatil@yahoo.com

Prof. A.N. Jaiswal
Asst. Professor
PG Dept. Of CSE
G. H. Raisoni COE,Nagpur
9881713338
jaiswal-an@yahoo.com

ABSTRACT

This paper proposes a defense mechanism against TCP SYN flooding attacks. The proposed method is a hybrid method as it defend the Internet against Denial of Service(*DoS*) and the Servers using TCP by sniffing both incoming and outgoing IP packets at ISP edge router providing both attacker side as well as victim side defense. Server firewalls find it difficult to distinguish between SYN flood attack packets and Normal TCP connections . Another problem is single-point defenses (e.g. firewalls) lack the scalability needed to handle an increase in the attack traffic.

Attack mitigation techniques are broadly classified into two types: Server based and Router based. In sever based defense methods server will be overloaded with the defense mechanism and sever itself is vulnerable to attack.In Router Based method the mechanism is needed to implement on all the edge routers of the ISP. Hence no method is providing faster and effective solution .This problem prompted us to go for the router based defense method using hybrid approach involving attacker-side and server-side or victim-side. The proposed system is expected to run on the edge router of the ISP. The edge router will have added functionality of using layer 4 protocols.

Our method can propose a better solution as attack packets are limited at source only. This can avoid excess consumption of bandwidth and it is scalable to incorporate various similar kind solutions against the DoS attacks.

Router based Defense mechanism is basically collaborative approach since ISP router dump and IP address list of network computer is required form Internet service provider. The benefit of hybrid approach is unnecessary flooding is avoided since attack packet is controlled at attacker side.

Categories and Subject Descriptors

C.2 [Computer-Communication Networks]: Network Protocols & Security : Attacks and Defense

C.2.6 [Internetworking]: Standards (e.g., TCP/IP) – *SYN Flood Attacks, Defense*

General Terms

Performance, Security

Keywords

TCP SYN packets, SYN Flooding, Attacks, Defense, ISP, Traffic

1 INTRODUCTION

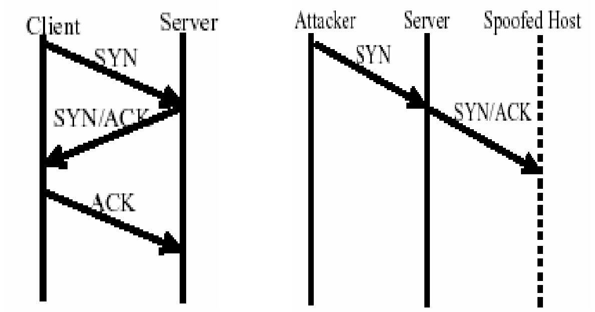
As the number of attacks is increasing ,the complexity of the attacking techniques is also increasing. We will find that the most of attacks are TCP SYN Flooding attacks. In TCP SYN Flooding attack, the attacker send number of TCP SYN request to the victim because of which many half open connections are in the waiting state in the backlog queue disallowing the legitimate user from getting connected to the system. Because of this the victim system will be prone to DoS (Denial of Service) attack.

SYN flood attacks exploit the transmission control protocol (TCP) specification. In the TCP, a client node communicates with a remote node (i.e., a server) by way of a virtual connection established through a process called a 3-way handshake. As shown in Figure 1(a), a client first sends a server a SYN packet requesting establishment of a connection. The server then sends the client a SYN/ACK packet acknowledging receipt of the SYN packet. When the client receives the SYN/ACK packet, the client sends the server an ACK packet acknowledging receipt of the SYN/ACK packet and begins to transfer data[8].

In DOS Attack Single computer will send may no of SYN packet containing random source IP addresses which will fill the resources like backlog queue preventing legitimate user to establish the connection

A denial of service attack is characterized by an explicit attempt by an attacker to prevent legitimate users of a service from using the desired resources. Examples of denial of service attacks include [9]:

- attempts to “flood” a network, thereby preventing legitimate network traffic attempts to disrupt connections between two machines, thereby preventing access to a service
- attempts to prevent a particular individual from accessing a service
- attempts to disrupt service to a specific system or person.



(a) 3-way Handshake (b) SYN Flood attack

Figure 1

The following steps take place during a distributed attack [10]:

- The real attacker sends an "execute" message to the control master program.
- The control master program receives the "execute" message and propagates the command to the attack daemons under its control.
- Upon receiving the attack command, the attack daemons begin the attack on the victim.

Many solutions are proposed these attacks such as[11]

- Configuration optimization containing System configuration improvement and Router configuration improvement
- Infrastructure improvement
- Connection establishment improvement
- Firewall Approach containing Firewall as a Relay and Firewall as a semi-transparent gateway

A satisfactory solution must detect the flooding as early as possible that is as the attack launched. Existing Distributed DoS defense schemes are most based on detecting sustained confection on communication. Because of which incoming and outgoing volume of traffic on routers are increasing.

Wang et al [16] adopted the nonparametric CUMSUM method to detect TCP SYN flooding attacks . This technique detect the change at gateway level. This solution will not work if there are more that one gateway routers.

Peng et. Al. [17] monitor the source IP addresses and keep track on IP addresses using offline data base in normal cases.

This method suffer from long detection delays

Functionality is added to each router to detect and preferentially drop packets that probably belong to an attack. Upstream routers are also notified to drop such packets (hence the term Pushback) in order that the router's resources be used to route legitimate traffic.[14]
Some mechanism detects attacks near the victim servers and alert messages are sent via the overlay networks. Then defense nodes identify legitimate traffic and block malicious ones. The legitimate traffic is protected via the overlay networks. We simulate and verify our proposed method can effectively block malicious traffic and protect legitimate traffic. We also describe the deployment scenario of our defense mechanism.[15]

Pushback is a mechanism for defending against distributed denial-of-service (DDoS) attacks. DDoS attacks are treated as a congestion-control problem, but because most such congestion is caused by malicious hosts not obeying traditional end-to-end congestion control, the problem must be handled by the routers. Functionality is added to each router to detect and preferentially drop packets that probably belong to an attack. Upstream routers are also notified to drop such packets (hence the term Pushback) in
order that the router's resources be used to route legitimate traffic. [16]
It is more efficient to perform detection at victim level [13][20]. This solution needs implementation on all routers. Server based defense methods are Client pazzle[1], Defenssive Programming[2], Hop-Count Filtering[3], Path Identifier[4], SYN Cache[5], SYN cookies, Synkil and some commercial products available are Checkpoints SYN Defense, Netscreens and SYN Proxying. , Router based defense methods are Distributed Packet Filtering[13], Ingress filtering[6], Push Back[7],SAVE[12] and some Commercial are MAzu's Enforce, Arbar Networks Peakflow

In this paper, we are proposing the hybrid approach which will include both victim side and attacker side defense. So that unnecessary flooding is avoided and more bandwidth is available for use for legitimate user.

2 PROPOSED WORK

2.1 Overview

Attacker-side defense can protect legitimate packets from higher-rate attacks than victim-side defense and that our proposed method can effectively block malicious traffic and protect legitimate traffic.

In this paper we are deploying on two important defenses

Attacker-side defense **:** Try to avoid generation of attack packet in the network also dropping the attack packet generated in the network so as to protect other networks.

Victim-side defense : Protect our network from the attack packet from other network

Attacker-side defense

Here we are planning to deploy the following mechanism on edge routers. And implementing this mechanism by other edge routers will protect the whole network from malicious attack packets. In this approach at the router side we will perform the following

Router will have the list of IP addresses of machines in the network. First we will check the incoming packet IP address. And compare it with the list of IP addresses of machines in the network available with the router. From comparison we will easily trace out the spoofed addressed packet. And the spoofed addressed packet will be dropped at router only so as to protect other network machine (victim).

Our Program will also watch the SYN packets. If incoming SYN packet rate is more then it will do analysis on SYN packets if only SYN packet is passing through the router without final ACK then it is a DOS attack drops all the SYN packets coming from the destination.

Here we are also checking the SYN packet rate if it crosses the threshold value then it indicates that there may be a SYN Flooding attack

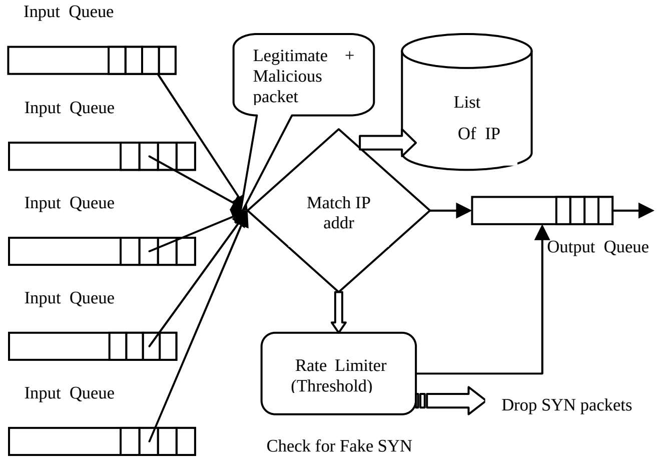
Victim-side defense

Here the middle box lets SYN and ACK packets go through but monitors the traffic and reacts to it

Here middle box passes SYN packets and when host responds with SYN + ACK packet the middle box forward it but also reacts by generating and Sending ACK packet to destination which seems to come from the source .this will move the connection out of backlog Queue in the host freeing the recourses that were allocated for half open connection .

If the middle box has not received the legitimate ACK for time out period then it will send RST packet will in tern terminate the connection.

2.2 Victim side architectural model



3 FUTURE WORK

We will extend this project by combining attack pattern matching and for this ISP Router dump is required. Making available ISP Router dump is one task and then we will try to find out the attack patterns from the available data. This patterns will be recorded for future use. If same attack pattern encountered again in the network, it will be easy and faster for us to take further actions depending on the prior knowledge from the recorded patterns.

4 CONCLUSION

This paper reports our work of filtering the attack packets at edge routers only so that legitimate packet will get more bandwidth .our major contribution are summarized here

-Restricting and discarding Fake SYN Packet at edge router only
-Restricting and discarding Spoofed IP addressed SYN packet at edge router only
- Making more resources available at victim side.

Our system will be scalable enough for extending both attacker side and victim side defense as well no need of delta adjustment at the victim side. Unnecessary flooding is avoided because packets are controlled at attacker side.
The overhead of this method is the need to implement attacker side model on all the routers and the middle box at victim side which is also vulnerable to DoS attack and hence solution is to go for Pattern matching approach and the only requirement is ISP router dump for processing.

5 ACKNOWLEDGMENTS

Our thanks to ACM SIGCHI for allowing us to modify templates they had developed.

6 REFERENCES

[1] A. Jules, J. Brainard,Client Puzzle; A Cryptographic defense against connection depletion attacks. In proceeding of NDSS,99,Feb1999.

[2] X. Qie,R. Pang & L. Peterson: Defensive Programming: Using an annotation toolkit to build Dos resistant software In proceedings of USENIX OSDI2002,Boston,Dec2002

[3] C. Jin, H, Wang & K. G. Shin, Hop count filtering: An effective defense against spoofed DDOS traffic In proceeding of ACMCCS2003,Oct2003

[4] A. Yaar,A. Perrig & D. Song,PI: A path Identification mechanism to defend against DDOS attacks In proceeding of IEEE Symposium on security & privacy,Oakland,May2003

[5] J. Lmon, Resisting SYN flooding DoS Attacks with a SYN Cache In proceeding of USENIX BSDCON2002, San Francisco,Feb2002

[6] P. Ferguson & D. Senin, Network ingress filtering: Defeting DoS attacks which empkoy IP source address spoofing in RFC2267,Jan1998

[7] J. Ioannidis & S.M.Bellovin, Implementing pushback: Router based defense against spoof DDOS traffic In proceedings of NDSS2002 San Diego,feb2002

[8] Master's Thesis , Detection and Defense Method against Distributed SYN Flood Attacks Supervisor Professor Masayuki Murata Author Yuichi Ohsita February 15th, 2005 Department of Information Networking Graduate School of Information Science and Technology Osaka University

[9] CERP Coordination Center, Cert Advisories: "CA-2000-01 denial-of-service developments:" http://www.cert.org/advisories/CA-2000-0 1 .html; "CA-99-17 denial-of-service tools," http://www. cert.org/advisories/CA-99- 1 7-denial-of-servicetools.html; "CA-98-1 3-tcp-denial-of-service: vulnerability in certain TCP/IP implementations," http://www.cert.org/advisories/ CA-98- 13-tcp-denial-of-service.1itml.

[10] CERP Coordination Center, "Results of the distributed systems intruder tools workshop," Nov. 1999,http://www.cert.org/reports/dsit-workshop.pdf.

[11] Christoph L. Schuba, "Analysis of a denial of Service Attack on TCP" IEEE symposium on security privacy Publication: 1997

[12] J. Li & J. Merkovic, M.Wang,P. Reiher & K. Zang, SAVE: Source address Validity Enforcement Protocol In

proceedings of IEEEINFOCOM2002, NewYork City,June2002

[13] L. Park & H. Lee,On the effectiveness of router based packet filtering for DDOS attack prevention in powerlaw internets in proceeding of ACM SIGCOMM2001, San Diego,August2001

[14] Implementing Pushback: Router-Based Defense Against DDoS Attacks John Ioannidis Steven M. Bellovin ji@research.att.com smb@research.att.com AT&T Labs Research AT&T Labs Research

[15] Deployable overlay network for defense against distributed SYN flood attacks Ohsita, Y.; Ata, S.; Murata, M. Computer Communications and Networks, 2005. ICCCN 2005. Proceedings. 14th International Conference on Volume , Issue , 17-19 Oct. 2005 Page(s): 407 - 412 Digital Object Identifier 10.1109/ICCCN.2005.1523897

[16] H.Wang,D. Zang & K. Shin,Change point monitoring for the detection of DOS attack,IEEE transaction on dependable & secured computing,Vol I, No. $, Oct-Dec2004

[17] Peng,C. Leckie, K. Ramamohanarao,Detecting Distributed DOS attacks by sharing distributed beliefs,ACISP2003