International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-6, September 2015
ISSN: 2395-3470
www.ijseas.com

An Effective Prevention Mechanism for TCP/SYN Attack

Sumit Singh Panwar
Research Scholar, Department of Computer Science and Engineering, JB Institute of Technology, Dehradun, India
sumitpanwar67@gmail.com

Abstract- Distributed denial of service (DDoS) attack is the fast growing problem circumventing the world of Internet. Its main focus is to attack network systems in the Internet. DDoS attacks have become highly important that requires immediate attention for complete solution. These attacks are complex in nature and aims at poorly secured applications, servers and disrupting legitimate user's communication. This problem has curbed the entire world of Internet that hinders the legitimate users to access the authorized services and the resources. In this literature various schemes are discussed. This paper provides an holistic view of DDoS problem, the various prevention schemes used nowadays and a methodology to stop TCP/SYN DDoS flooding attack. Therefore, the study in this paper will help the researchers to have a complete and improved understanding about the DDoS problem, prevention schemes and an effective mechanism to curtail TCP/SYN flooding attack

Keywords- **Distributed Denial-of-Service (DDoS), Network Security, Attack mechanisms, Prevention schemes, Flooding Attacks**.

I. INTRODUCTION

Internet is very important aspect of our lives. It changes our way of communication, business mode, or even everyday life. Most of the today's services such as banking, shopping, education, medicine, business, etc are dependent on the Internet. Distributed denial of service attack is the most common threat to the Internet. Various defense mechanisms have been proposed but researchers are still struggling for the complete solution to protect Internet from DDoS attacks.

Distributed Denial of Service attack is an attack which prevents a computer or network to provide normal services. It is considered to take place only when access to a resources of the computer or is blocked by the malicious user [1]. DDoS is a huge threat to the sites on the internet, and now the DDoS problem has become more complicated and it is difficult to provide solution for it. This attack is launched by various compromised machines which are vulnerable to attacks as they have poor security mechanisms and control can be gained easily on them. These compromised machines send the useless traffic to the victim machine so that victim's resources are exploded and the Internet operations are also disrupted due to congestions caused by useless traffic.

Distributed denial-of-service (DDoS) attack is performed with the help of many compromised machines. DDoS attacks require multiple machines, which will send the traffic to the victim machine. These machines do not belong to the attacker. Such machines are poorly secured systems which are available at universities, homes etc. The attacker breaks the poor security mechanism, takes full control over them and starts misusing them for the attack. These attacking machines are frequently called as zombies, daemons, slaves, or agents. Attacker easily gets control over these machines because they are poorly secured as they are not updated and does not have recent software patches. They are not protected by a firewall or users have easily guessed passwords as they do not have powerful passwords. The DDoS attack [2] is composed of four elements Attack source, Control masters, Agents, and Victim:

- Attack source: Attack source is the machine, handled by attacker which starts the attack.
- Control masters: Control masters control various agents to implement the attack in a coordinated manner. Control masters are deployed on one or more host machines.
- Agents: Agents, also referred attack daemons, which actually conducts the attack on the target victim.
- Victim: A victim is a target host of the DDoS attack.

In this paper, we will discuss about the DDoS problem and various prevention schemes. In addition, we have proposed the scheme to stop TCP/SYN flooding attack.

Rest of the paper is structured as follows: Section II gives various DDoS prevention schemes. Section III discuses proposed methodology to stop flooding attack. Finally, Section IV concludes the paper.

II. DDOS PREVENTION SCHEMES

The most common technique for preventing DDoS attacks includes filtering technique. The filtering techniques can be classified as ingress/egress based filtering, router level packet filtering, IP filtering based on history, SAVE protocol etc. These techniques are classified as below:

1. Ingress/Egress filtering

Ingress filtering is proposed by Ferguson .This technique uses the method of dropping the packets with IP address that do not match a domain prefix associated with the router. Egress filtering basically works on the strategy that only allocated IP address space leaves the network. We must be aware of the expected IP addresses on the particular port. Another important technique is reverse path filtering. We can see the source address of the incoming traffic that whether it is reachable if traced in reverse. DDoS attacks do not need spoofed source addresses and they exploit a large number of compromised host. Here ingress and egress filtering is not efficient in preventing DDoS attacks.

2. Packet filtering at Router Level

Packet filtering at Router Level, given by Park and Lee, improved ingress filtering by using the information of packet route to filter out spoofed IP packets. The concept says that each link can get traffic from only a limited set of source addresses .It is assumed that source address has been spoofed if an unanticipated source address occurs in the IP packet present on a link and hence the packet is filtered. However, there are many limitations related to this scheme. The problem associated with RPF is that it is difficult to implement. The important limitation is that RPF may drop valid and genuine packets. The third potential limitation is that RPF depends on valid BGP messages which are used to configure the filter. If an attacker hacks a BGP session and send bogus BGP messages, then border routers can be mislead and they may update filtering rules which would help the attacker.

.

3. Capability based method

This method is based [3] on request and response strategy. In this approach, source first directs request packets to the destination. Router then marks each packet as it passes through the router. It depends on the destination that it wants to grant permission to the source or not for sending the packets. The capabilities are returned if the permission is granted and it will not be provided in the returned packet id if permission is not granted. The strength of this scheme is that the destination has control over the traffic, which can reduce the chances of DDoS attack. The packets without capabilities can be dropped at the router.

4. History based IP filtering

This filtering technique is based [3] on the concept that the a collection of IP addresses that is seen during usual process are even and occur frequently whereas during DDoS attacks, most of the source IP addresses are new and infrequent. In other words they are not seen before. So based on this an IP address database (IAD) is maintained with frequent source IP addresses. During an attack, the packet is dropped id the source address of a packet does not appear in IAD. This scheme is efficient as it does not require support of whole Internet community. But the limitation of this mechanism is that it is inefficient when the attacks is performed from genuine from IP addresses and it requires an offline database to save IP addresses which leads to storage overheads.

5. Secure overlay Service (SOS)

This technique is proposed by Keromytis et al [4].Here the traffic is verified to establish secure communication between the confirmed users. The secure overlay access point (SOAP) verifies the traffic from a source point. After authentication is complete the traffic is directed towards an overlay node called a beacon in an unidentified manner. The beacon then forwards traffic to next overlay node called a secret servlet to perform further authentication. The verified traffic is forwarded to the victim by the secret servlet. The traffic forwarded by the secret servlet is passed to the perimetric routers .It is an efficient method but the main challenge is deployment of SOAP. To implement SOS we need a secure protocol which itself is another issue.

6. Source Address Validity Enforcement (SAVE)

Li et al [5] have introduces a new protocol called the SAVE protocol that blocks any IP packet with a source IP address that is not known. SAVE protocol provides information about range of IP addresses to routers that it would expect at each interface. Hence, each router constructs an incoming table which connects each link of the router with a group of source address blocks that are valid and genuine. This protocol enables the router to filter packets that have source addresses that are spoofed. The major limitation of this scheme is it requires change in the routing protocol which is a very cumbersome job and time consuming. Second limitation is even if SAVE is deployed then also DDoS attacks can be performed with non spoofed source addresses.

III PROPOSED METHODOLOGY

This main idea behind this algorithm is to prevent the flooding attack. Here we are dealing with TCP SYN attack with spoofed IP addresses. The attacker is continuously sending the packets with source address spoofed. Each packet sent contains a different source IP address.

The algorithm allows 1 TCP connection/second. If a more than one connection request comes within 1 second then 1st connection request is accepted and the remaining requests are dropped within that 1 second. The details of dropped request is also written in the log

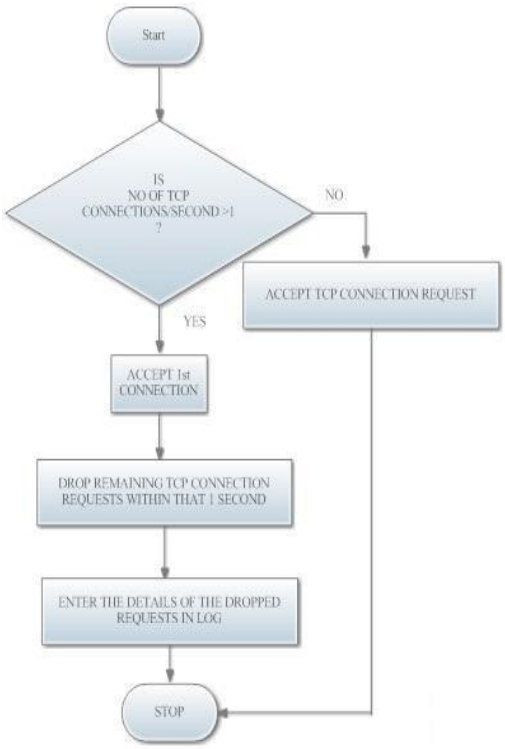
This assumption is considered keeping in mind the real life scenario. The algorithm limits the connection acceptance rate to 1/second. Flooding attack is a Denial of Service (DoS) attack that brings down the network or service by flooding the network with large amounts of traffic. IN these

attacks a network or service becomes so overburdened with packets initiating incomplete connection requests such that it cannot process genuine connection requests. This flooding of the server or host with incomplete connection requests fills the host memory buffer. As the s buffer is full so we cannot make further connections and this leads to Distributed Denial of Service attack. Our algorithm protects from such kind of attack as we have limited the no of connections to 1/second

ALGORITHM

1. Begin
2. If No of TCP connection requests/second > 1
   Begin
   Accept 1st connection request and drop the remaining connection requests arriving with in 1 second and enter the details of dropped packets in the log.
   End
3. Else if No of TCP connection requests/second=1 Begin
   Accept the Connection request. End
4. End

FLOWCHART



IV CONCLUSION

The proposed methodology protects the web server from flooding attack .Here we have limited the no of TCP connections that the server can accept to 1/second. The remaining connection requests are dropped and the dropped packets detail is entered in the log. This algorithm protects the server from flooding attack like (TCP SYN Attack).

REFERENCES

[1] B. B. Gupta, R. C. Joshi,and Manoj Misra Defending against Distributed Denial of Service Attacks: Issues and Challenges(April,2011),pp.1-11.

[2]Douligeris, C., and Mitrokotsa, A. (2003). DDoS attacks and defense mechanisms: Classification. In Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology(ISSPIT 03)

[3] T. Anderson, T. Roscoe, D. Wetherall, "Preventing Internet Denial-of-Service with Capabilities," In ACM SIGCOMM Computer Communication Review, Volume 34, issue 1, January 2004, pp. 39-44

[4] A. D. Keromytis, V. Misra, and D. Rubenstein, "SOS: Secure Overlay Services," in the Proceedings of. ACM SIGCOMM,pp. 61-72, 2002.

[5] J. Li, J. Mirkovic, M. Wang, and P. Reither, "Save: Source address validity enforcement protocol," Proceedings of IEEE INFOCOM, 2002, pp. 1557-1566.