Monal R. Torney, Prof. A R.Patil Bhagat / IOSR Journal of Engineering (IOSRJEN)
www.iosrjen.org ISSN : 2250-3021
Vol. 2 Issue 1, Jan.2012, pp. 106-110

New Integrated Defence and traceback approach for Denial of service attacks

Monal R. Torney[1], Prof. A R.Patil Bhagat[2]
[1] P.G,Student
Department of Computer Tecnology
Yeshwantrao Chavan Collage of Engineering
Nagpur, India
[2] Department of Computer Technology
Yeshwantrao Chavan Collage of Engineering
Nagpur , India

ABSTRACT
Information security is one of the most challenging problems facing network designers and operations managers. Along with viruses and worms, Denial of Service (DoS) attacks constitutes one of the major threats to the current Internet. Denial of Service attacks aims to crash a server or a network in order to paralyze its normal activity. Today, most organizations provide services over the internet hence an attack which targets their resources on the Internet. Denial of service is major class of security threat today. As attacker usually uses fake IP to hide their real location. One effective means to defend against such attacks is to locate the attack source and to filter out the attack traffic. To locate the attack source, this paper proposes an effective defense and IP trace back mechanisms. For implementing effective defense and trace back mechanisms against Denial of Service attacks such as SYN Flood and ICMP Flood we construct a simulation environment Using Network Simulator version 2.

Keywords - **Denial of Servie (DoS) Attacks , Firwall , ICMP, , Spoofed Address , SYN Flood , TCP ,Traceback.**

I. INTRODUCTION
The recent rapid growth and the wide use of the Internet are making Internet security issues increasingly important. Denial-of-service (DoS) attacks are one of the most serious problems. Attacks designed to make a host or network incapable of providing normal services are known as denial of service attacks. There are different types of DoS attacks, a few of them abuse the computers legitimate features; a few target the implementations bugs and a few exploit the misconfigurations. DoS attacks are classified based on the services that an adversary makes unavailable to legitimate users. In DoS attacks the adversary mainly targets a few services like network bandwidth router or server CPU cycles system storage, operating system data structures, protocol data structures and software vulnerabilities [1]. DoS can be a single source attack, originating at a single host, or can be a multi-source attack, where multiple hosts and networks are involved.

The SYN flooding attack is a denial of service method affecting hosts that run TCP server processes. The attack takes advantage of the state retention TCP performs for some time after receiving a SYN segment to a port that has been put into the LISTEN state. The basic idea is to exploit this behavior by causing a host to retain enough state for bogus half-open connections that there are no resources left to establish new legitimate connections. TCP SYN Flooding causes servers to quit responding to requests to open new connections with clients a denial of service attack. Denial of service attacks prevents people from using the affected system or networks. These attacks usually proceed by overloading the target in some fashion. The TCP SYN Flooding attack takes advantage of the way the TCP protocol establishes a new connection. Each time a client attempts to open a connection with a server. Some information is stored on the server. Because the information stored takes up memory and operating system resources, only a limited number of in-progress connections are allowed, typically less than ten (more commonly six or less). When the server receives an acknowledgement from the client, the server considers the connection open, and the queue resources are freed for accepting another new connection.

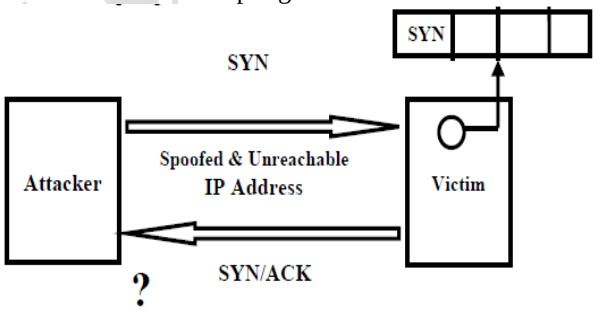

Figure 1: SYN Flood Attack

The attacking software generates spoofed packets that appear to be valid new connections to the server. These spoofed packets enter the queue, but the connection is never completed leaving these new connections in the queue until them time out. Only a few of these packets need to be sent to the server, making this attack simple to carry out even using a slow, dial-up connection from the attacker's computer. The system under attack quits responding to new connections until sometime after the attack stops.

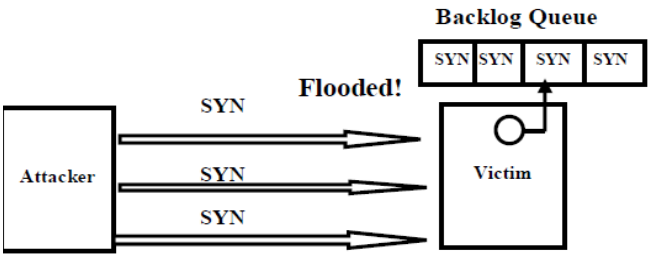

Figure 2: SYN Flood Attack

II. RELATED WORK

Currently there are several mechanisms to counter DoS attack. Methods that build a model of normal traffic often use machine learning algorithms. Clustering has been used in and uses BIRCH clustering algorithm. A vector with 'n' parameters is extracted from the normal traffic data and is used to create CF Trees. If the distance of the test data is more than a certain threshold, test data would be considered anomalous. Similarly, in labeled data (that include both normal and anomalous data) with 'n' parameters is arranged in the form of a grid with every parameter as a dimension and clusters of normal and anomalous data are created. Test data is also distributed in the grid and is classified depending on the type of cluster it falls in. To prevent DoS attacks, three different types of method are classified: prevention, detection and counterattack. Prevention method tries to prevent attacks based on the preemptive measurement to build the tolerant system. Detection method focuses on early detection for intrusions or attacks and focuses on notification by the alarm as soon as possible. In this method, accuracy and quickness are important factors. Counterattack method tries to some actions after detecting the attack. Types of these actions are included the filtering pushback and trace back.

III.PROPOSED SYSTEM

A. For detection and Defense mechanisms of SYN Flood Attack.

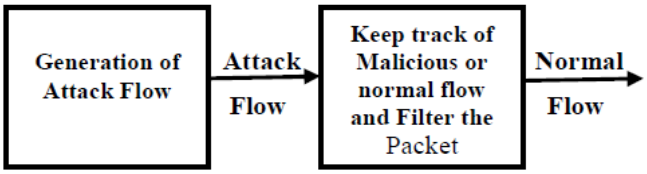

Figure 3: Block schematic of proposed approach for Defense.

DoS attacks can be detected either by using traffic signatures or by recognizing anomalies in system behaviors. A signature-based approach uses the signatures of the well-known attacks to determine if the packet represents a suspicious activity. Anomaly-based approach will detect abnormal behaviors by monitoring network traffic and comparing it with the baseline behaviors. The baseline will identify what is "normal" for that network. The baseline activity could be identified by a combination of average packet size, number of packets per second, flows per second, and bytes per second. Then the system can trigger an alert when it finds a significant deviation from the baseline

Our approach for DoS detection is a focus on two types of DoS attacks, namely SYN flood, ICMP flood. First, SYN flood exploits vulnerability of the TCP three-way handshake. During SYN flood, an attacker sends a lot of TCP SYN packets with source IP addresses that does not exist or is not in use. The attacker also uses many random source ports to connect to a single destination port of a victim. Since the number of requests is large, the system will run out of resources and starts dropping normal connection requests. Internet Control Message Protocol (ICMP) is based on the IP protocol and is used to diagnose network status. An ICMP flood is a type of bandwidth attack that uses ICMP packets. On IP networks, a packet can be directed to an individual machine or broadcast to an entire network. When a packet is sent to an IP broadcast address from a machine on the local network, that packet is delivered to all machines on that network. When a packet is sent to that IP broadcast address from a machine outside the local network, it is broadcast to all machines on the target network (as long as routers are configured to pass along that traffic).IP broadcast addresses are usually network addresses with the host portion of the address having all one bits.

B. Firewall as Semitransparent Gateway.

The firewall monitors the traffic sent from source to destination. When it sees ACK+SYN being sent from D to S, it responds by creating an ACK message and sending to D, thus reallocating the resources and moving the connection out of the queue. If it is an attack, the firewall then sends a RST message to D and connection is dropped. If the connection request is from a proper source, he sends back ACK, which is passed by firewall. D merely sees it as the duplicated packet and discards it.

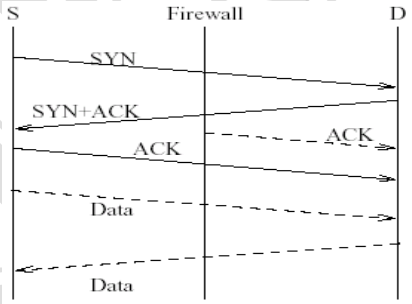

Figure 4: Firewall as a semitransparent gateway (Legitimate connection)

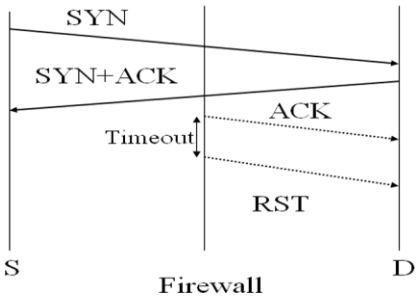

Figure 5: Firewall as a semitransparent gateway (Illegitimate connection)

C. Ingress / Egress Filtering.

Ingress Filtering is one of the source-end defense mechanisms to block spoofed packets before entering the Internet core. The purpose of ingress/egress filtering is to only allow traffic to enter or leave the network if its source addresses are within the expected IP address range. Ingress filtering is a filtering scheme that filters incoming traffic according to a specified rule.

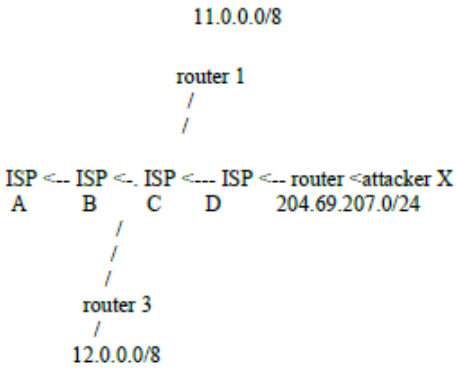

Figure 6:Ingress/Egress Filtering

The purpose of ingress/egress filtering is to only allow traffic to enter or leave the network if its source addresses are within the expected IP address range. Suppose an attacker X resides within the leaf network. An input filter is placed in the input port of router 2 that is connected to the leaf network. This input filter only admits packets having a source IP address with the 204.69.207.0/24 prefix. If attacker X sends traffic with spoofed IP addresses that do not have the 204.69.207.0/24 prefix, that traffic will be dropped by the input filter in router 2. This filtering function provided by router 2 is called ingress filtering as it deals with traffic coming into the network of ISP D. However, if router 1 provides the same function, that function is called egress filtering as it deals with traffic leaving the leaf network. This stops an attacker from using hosts within that network as DDoS agents. If these two solutions are widely deployed all over the internet, then they will go a long way in stopping all attacks that rely on IP spoofing to be effective. Furthermore, they will enable easy trace back of the attacks to the true origin as the attacking hosts are forced to use their true IP addresses. Ingress/Egress filtering do not provide protection against bandwidth based DDoS attacks though. Ingress and Egress filtering depend on their widespread use for their efficacy.

D. IP Traceback

The problem of identifying the machine that directly generates attack traffic is called IP trace back problem. IP trace back is a subtle scheme to tackle DoS attacks. If it can provide the exact attack origin, then we may apply some proper actions such as packet filtering to stop attacks completely. The mechanism must be incrementally deployable which means, it should function even when not all of the routers across the Internet use this mechanism. A trace back mechanism should not require major changes on the current infrastructure. The number of packets required to identify the attack path should be as low as possible. Also, a trace back mechanism should scale to a large number of attackers while maintaining accuracy.

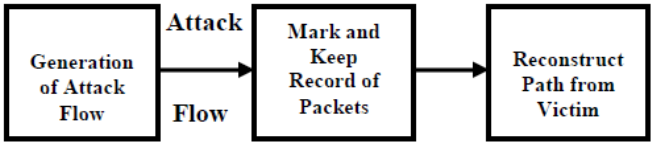

Figure 7: Block Schematic of Proposed approach for trace back

A. Packet Marking

Our proposed scheme uses dynamic probabilities for marking packets. The reason for this is to provide a uniform probability distribution for each router to send its information to the victim. The probability of a packet has lastly been marked at router ri (i=1,2,…,D) and nowhere further down the path is called the leftover probability [13] and can be shown as

$$p\,(1-p)^{D-i} \text{ for } 1 \leq i \leq D.$$

(1)According to equation (1), when fixed probabilities are used, leftover probabilities will be in the order of

```
for each packet P
    identification = get 16-bits identification value
    counter = (identification >>11) & 31
    fragment-id = (identification >>8) & 7
    fragment = identification & 255
    for each router r in router map
        hash = calculate SHA1 of router r's address
        if (hash[fragment-id] == fragment)&&(r.distance
                                              ==counter)
            add router r to the path
        else
          counter++
```

$$r1 < r2 < \ldots < rD$$

Therefore, routers that are closer to the victim have bigger chance to pass their marking since the probability of the marking to be rewritten is lower. In order to provide a uniform leftover probability, each router can mark packets with a probability which is determined by an inverse function of the distance it has travelled [13]. If p = 1/i, where i is the distance from its source to the marking router, the leftover probability can be computed by equation (1) as:

$$1/I\,(1 - 1/i+1)\,(1 - 1/i+2)\ldots\,(1 - 1/i+D) = 1 / D \qquad (2)$$

By equation (2), each router has the same leftover probability which means each router has the same chance to send its marking to the victim.

```
for each packet P
      find initial TTL value of P
      distance = initialTTL - TTL
      p = 1 / distance
      rv = select a random number from interval [0,1)
      if (rv<p)
            hash = calculate SHA1 of router address
            fragment-id = select a random integer from
            interval [0,7]
            fragment = hash [fragment-id]
            counter = 0
    else
            counter++
```

Figure 8: Algorithm for Packet Marking.

The distance from the packet source can be determined from the current TTL value of the packet. Since most initial TTL values fall in the set of {32, 64, 126, and 255} and recent Studies [5] show that about 99% of path lengths on Internet are less than 25 hops, the distance of a packet from its source can be deduced from its current TTL value.

B . Path Reconstruction

In path reconstruction phase, the victim uses markings it has received and its router map. We will not focus on map construction phase, since it is explained in FIT [18] briefly. It

is assumed that, the victim has the correct information of its upstream routers (IP address and their distance from the victim). Using a router map is a key feature in an IP trace back scheme in order to reduce the number of false positives.

Path reconstruction procedure is very important, since the design of this procedure affects the performance of the scheme directly. Most of the schemes, including FIT, avoid revealing the details of their path reconstruction procedures. In the proposed scheme we perform path reconstruction by using the algorithm shown in Fig.9

Figure 9: Algorithm for Path Reconstruction.

IV.SIMULATION ENVIRONMENT

Simulation is an important method in network research, which can analyses the new protocol created at different network topology and cross traffic quickly and low-costly. ns2 [24] is a kind of simulator, which is widely used and with multiple protocol. It also presents multi layer abstract to simulate with large-scale.

NS2 (Network Simulation 2) is an object-oriented and discrete-event network simulator. And it is an authoritative simulation tool in network researches [24] [25]. In common, NS2 defines a file format (*. tr) to track and record simulation processes and results.Ns2 is an object-oriented simulator, which is written in two programming languages: C++ is used to implement the specifics of the underlying simulated protocols and process vast amount of data efficiently.OTcl is used as the front end interpreter of the simulator and can establish the desired environment. The objects in these two languages are closely related and corresponding to one another. We can create Terrestrial, satellite and wireless networks with various routing algorithms (DV, LS, PIM-DM, PIM-SM, AODV, DSR), Traffic sources like web, ftp, telnet, cbr, stochastic traffic, Failures, including deterministic, probabilistic loss, link failure, etc and Various queuing disciplines (drop-tail, RED, FQ, SFQ, DRR, etc.) and QoS (e.g., IntServ and Diffserv). In our view, nodes in the simulation scenarios can be classified into four different roles: attacking nodes, legitimate traffic nodes, intermediate routers and the victim. With these benefits of ns2, we set up a simulation environment that can be used to evaluate the effectiveness of different PPM schemes.

V.CONCLUSION

In this paper, we presented a approach for defending and trace back technique against spoofed DoS traffic. For instance, the integrated solution combines filtering and traces back mechanisms to deal with Denial of Service attacks.

In this paper, a simulation environment is constructing via ns2, setting attacking topology and traffic, which can be used to simulate and compare the effectiveness of different PPM schemes. The simulation approach also can be to test different performing effect of PPM schemes in DoS attacks.

REFERENCES

Journal Papers:

[1] S.Gavaskar, R.Surendiran, Dr.E.Ramaraj *"Three Counter Defense Mechanism for TCP SYN Flooding Attacks", International Journal of Computer Applications (0975 – 8887) Volume 6– No.6*, September 2010.

[2] J.Manikandan, S.Vijayaragavan ,R.Madhavi,"*A Survey of DDoS Service Attacks in Collaborative Intrusion Detection System."2010 International Journal of Computer Applications (Vol .1 – No. 25).*

[3] A.John ,T.Shivkumar,*''DDoS Survey of Trace back Method " International Journal of recent Trends in Engineering,Vol .1.*

Theses:

[4] Tao Peng , "*Defending Against Distributed Denial of Service Attacks*". doctoral diss. Department of Electrical and Electronic Engineering, University of Melbourne.

Proceedings Papers:

[5] Chung-Hsin Liu ,Yong- Zhi Huang ,"The Analysis for DoS and DDoS attacks of WLAN " *2010 Second International Conference on Multimedia and Information Technology.*

[6] Iustin Priescu, Sebastian Nicolaescu," Design of Traceback Methods for Tracking DoS Attacks" *IEEE , 2009.*

[7] WANG Xiao – Jing , XAIO You – lin ," IP Traceback based on Deterministic Packet Marking and Logging ." *International Conference on Scalable Computing and communication,2009.*

[8] Turker Akyuz , Ibrahim Sogukpinar, "Packet Marking With Distance Based Probabilities for IP Traceback*." IEEE, First Intern,ational Conference on Networks & Communications 09 .*

[9] Cheol-Joo Chae, Seoung-Hyeon Lee, Jae-Seung Lee, Jae-Kwang Lee," A Study of Defense DDoS Attacks using IP Traceback" *International Conference on Intelligent Pervasive Computing 2007.*

[10] V. Murali Bhaskarant, A. M. Natarajan,S. N. Sivanandam3," Analysis of IP Traceback Systems*." IEEE 2006.*

[11] Mudhalkar Srivastsa,Arun Iyangar ,Jian Yin ang Ling Liu, A Client- Transperant Approach to Defend against Denial of Service Attacks.*5th IEEE SRDS'06.*

[12]Wei Chen Dit-Yan Yeung,"Defending Against TCP SYN Flooding Attacks Under Different Types of IP Spoofing", *International Conference on Systems andInternational Conference on Mobile Communications and Learning Technologies IEEE 2006.*

[13] Mohamad Chouman, Haidar Safa, Hassan Artail," A Novel Defense Mechanism against SYN Flooding Attacks in IP Networks", *CCECE/CCGEI, Saskatoon, May 2005.*

[14] Qiang Li , Hongzi Zhu , Meng Zhang , Jiubin Ju," Simulating and Improving Probabilistic Packet Marking Schemes Using Ns2." *IEEE Sixth International Conference on Parallel and Distributed Computing, Applications and Technologies 05.*

[15]Masahito Yamana, Katsuhiro Hirata, Hiroshi Shimizu Simulation of IP traceback for the Denial of Service attacks. " *Symposium on Applications and the Internet Workshops 05.*

[16]Yuichi Ohsita Shingo Ata Masayuki Murata ," Detecting Distributed Denial-of-Service Attacks byanalyzing TCP SYN packets statistically". *IEEE Communications Society Globecom 2004.*

[17] J. Haggerty, T. Berry, Q. Shi and M. Merabti," DiDDeM: A System for Early Detection of TCP SYN Flood Attacks" *IEEE Communications Society Globecom 2004.*

[18] Zhaole Chen, Moon-Chuen Lee," An IP Traceback Technique against Denial-of-Service Attacks" *19th Annual ComputerSecurity Applications Conference (ACSAC 2003).*

[19] Kihong Park Heejo Lee,"On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack" *IEEE , 2001*.

[20] Stefan Savage, David Wetherall, Anna Karlin and Tom Anderson," Practical Network Support for IP Traceback",*ACM SIGCOMM'00, Stockholm, Sweden.2000* .

[21] Sirikarn Pukkawanna, Vasaka Visoottiviseth, Panita Pong

http://www.cert.org/archive/pdf/DoS_trends.pdf.

[22] CERT Coordination Center, "TCP SYN flooding and IPspoofing attacks,"CERT Coordination Center, "Trends in Denial of Service Attack Technology," October 2001.

[23] Christoph L. Schuba, Ivan V. Krsul, Markus G. Kuhn, Eugene H. Spafford , Aurobindo Sundaram, Dieg Zamboni," Analysis of a Denial of Service Attack on TCP". No.2 IEEE May 2009. paibool," Lightweight Detection of DoS Attacks" .

[24] Flashget http://www.flashget.com

[25] The Network Simulator - ns-2, http://www.isi.edu/nsnam/ns.

[26] Nam: Network Animator. http://isi.edu./nsam/nam/.