International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Minimization of DDoS Attack using Firecol an Intrusion Prevention System

Bhagyashri Kotame[1], Shrinivas Sonkar[2]

[1, 2] Savitribai Phule Pune University, Amrutvahini College of Engineering, Sangamner

Abstract: ***The Distributed Denial of Service is Process of continuosly sending unrelated information to the targeted system by the malicious node. Which causes the authorized users to stay away from the required services. The DDoS is major security threat .For distributed environment the mitigation of DDoS attack is very difficult, but is neccessary to prevent the user and network resources from this attack. In this paper firstly we areaddressing the problem of DDoS attack and proposing a technique of fireol which effectively reduces the DDoS attacks rather than presently available filtering approaches. This paper also presented the architecture and algorithm for firecol. The main part of firecol is formedof clusters of intrusion prevention system(IPS), which forms the protection rings around the host. Firecol is intended to provide security at different layers (various layers of OSI Model). Also firecol support different rules which increases the intensity of identifying the attacks, and more flexibely and dynamically is notices the attacks and increasesthe efficiency.***

Keywords: Detection, mitigation, Distributed denial of service (DDoS), IPS, BOTNET.

1. Introduction

With the growth of internet the threats for the services over internet are also increasing. In such case it has became mandatory to provide security to the network for the survival of entities. Distributed Denial of Service attack are packet flooding attacks which continuously floods the victim node with irrelevant packages, which is contrast from logical DoS attack which harms the operating system or Application. It blocks the service to the valid node by continuously flooding the service providers. The DDoS attack victims consists of the targeted nodes and the machines that are used by the attacker in the DDoS attacks. In Distributed Denial of Service attack the victim is flooded from many different sources, around hundred of sources.

Due to this the detection of this attack is very difficult. It becomes difficult to differentiate the traffic from legitimate users from those of traffic from attacker. DDoS attacks evolved from some megabits in 2000 and have grown up to around 100Gbs, the mitigation of which is difficult from many ISPs today [2].

Much recent work aimed at finding the distributed denial of service attacks by fighting the underlining vector that is the use of botnet [5] .The network formed by many machines (bots) that is controlled by single machine (master) is termed as botnet network. The synchronized attacks as like DDoS can be launched by the master by sending orders to the bots via a command and control channel. The detection of botnet related attack is very difficult; because of this its mitigation is also delayed.

So as to avoid these issues, the major focus of this paper is detection of DDoS attacks and per second notes their underlying vectors. As highlighted in [2] the DDoS attacks are mostly used for flooding a particular victim machine with mega traffic, in contrast the non distributed DoS attacks mainly exploits the vulnerabilities by forwarding some carefully forged packets to disturb the services. The DDoS attacks gains popularity due to its high effectiveness against any type of service, since there is no need for any service specific flaws to be identified and exploited in victim. As such this paper focuses specifically on flooding DDoS attacks.

It is hardly possible for single Intrusion Prevention System (IPS) or Intrusion Detection System (IDS) to detect such DDoS attacks, until they are located close to the victim. However, further the IDS/IPS may crash because it may need to deal with huge volume of request. Allowing such huge amount of traffic to travel over the Internet and just detecting or blocking it at the host IPS or IDs can strain Internet resources. This paper presents new collaborative system for detection of DD0S attacks as close as possible to the attack sources and as far away as possible from the victim termed as Firecol... Firecol is a service where the customer who request protection can subscribe. The participating Intrusion Prevention systems along the way to subscribed customer communicate by calculating and exchanging belief scores on attacks. A virtual protection shield of IPS is formed around the host they protect. In addition to the detection of DDoS attacks, firecol helps in the detection of other flooding attacks like flash crowds and botnet based attacks.

2. Literature Survey

A. Networks, Arbor, Lexington, MA [2] in cooperation with the Internet Security operations community they have completed their fourth edition of an ongoing series of annual operational security surveys. This survey is designed for providing important data that is useful to the network operators in order to make the decision about their use of network security technology. So as to provide protection to their mission critical infrastructure, and also meant to serve as general resource for the engineering community. The major focus of the survey respondents are issues of operational network securities and the day-to-day aspects of security in commercial networks. The real world concerns are more accurately represented by the result provided in this

survey rather theoretical and emerging attack vectors addressed elsewhere. Since last three surveys the ISP security has expanded. ISP spent most of their resources against distributed denial of service (DDoS) attacks.

T. Peng, C. Leckie, and K. Ramamohanarao [3] in this paper described that the Internet was originally designed for openness and scalability. In order to support ease of attachment of host to network the IP (Internet Protocol) was designed but it provided less support for verifying the contents of IP packet header fields. Due to which it is possible to take the source address of packet and becomes difficult to identify the source of the traffic. The presented several bandwidths based attacks such as Distributed Reflector, Infrastructure attacks, Protocol based and application based attacks. They stated four categories for defending the DoS attacks firstly they mentioned how the DoS attacks can be prevented and how it can be stopped before it causes any harm. They assume attack traffics source address is spoofed and also includes packets filtering at the routers. It permits only the legitimate traffic to pass through it. Secondly after they mentioned the detection of attack. DoS attack detection is different from any intrusion detection. By deleting the file created by the attacker or by making changes in the system log the general intrusion detection is possible. The detection of Dos attack is difficult, and also the services of target machine become very poor. Thirdly they mentioned identifying the source of attack and fourthly the reaction of attack.

K. Xu, Z.-L Zhang, and S. Bhattacharyya [4] they presented general methodology for building comprehensive behavior profiles of Internet backbone traffic in terms of communication pattern of service and end-host. Their goal is profiling Internet backbone traffic by automatically discovering significant behaviors of interest from massive traffic data and also provides possible interpretation of this behavior that helps network operators in understanding and quickly identifying anomalous event with a significant amount of traffic. They use combination of data mining and entropy based techniques to automatically gather useful information from largely unstructured data. They adopted entropy based approach to extract clusters of significance instead of using a fixed threshold based on volume. Once the clusters are extracted in the second stage of their methodology they discover the "structures" among the clusters and then build common behavior models for profiling. They demonstrated that blocking the most offending sources is reasonably cost-effective.

E. Cook, F. Jahanian, and D. McPherson [5] in this paper they presented the origin and structure of bots and botnets. They presented IRC (Internet Relay Chat) system which provides one0to-one and one-to-many messaging over the internet and also studied the methods of detecting IRC-based bots. They identified three approaches for handling the botnets: 1) by preventing the system from getting infected.2) by detecting command and control communication between the bots and among bots and controllers.3) by detecting secondary features of bots infection. They described botnet detection approach by correlating secondary detection information to pinpoint bots and botnet communication.

S.M Bellovin[6] presented the need of firewall over the Internet .Some people feel firewall is not needed if cryptography is used, but Bellovin in this paper presented that firewall is still powerful protective mechanism. He presented Distributed Firewall and hybrid firewall. He presented that firewall and IPSEC are synergistic strong firewalls can be implemented with the help of IPSEC; this removes many limitations of today's firewalls. Complete implementation of the distributed firewall is most flexible and secured. While host are outside the traditional firewall, with other host live behind.

3. Problem Definition

In the existing system the user's who want the protection need to subscribe to the firecol security service through the trusted server. Some predefined set of rules are used for protection of subscribed user. As and when the packets are received from the sender, the pattern of these IP packets is matched by the rules. It corresponds to single IP or an IP sub network. The rule definition can include protocols port used or any other monitor able information. When the packets are received at the system their frequency is measured, that is number of packets matching the rules. If the frequency comes out to be high it is considered as an attack and that particular IP is blocked. The existing systems have some limitations such as they provide security only till the network layer, the current IDS has high rate of false alarm. Huge amount of traffic passes through the Internet and only block it at the host IPS this can result in loss of many network resources.

In the proposed system also the customer who needs protection is needed to subscribe to the firecol system. In proposed system we are providing protection at all layers of OSI form data link layer to application layer, this increases level of security. In Firecol system the intelligence of one IPS is shared with other this helps to maintain the attacker list at all the available IPS. A list of attacker who already tried to attack system (termed as blacklist) is maintained, which helps in providing protection in future from such attackers/attacks. In proposed system we are defining our own rules suitable for the bank application. By some rules we are directly blocking the attacker, while in rest cases we are blocking the IP. Here the rules are based on transactions carried out in bank.

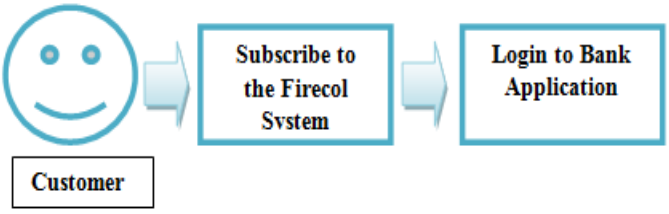

Figure 1: Customer Subscription

Our system consists of six different parts.
1. New Rule Metrics.
2. Selection Manager.
3. Score Manager.
4. Detection Manager.
5. Score List.
6. Bank System.

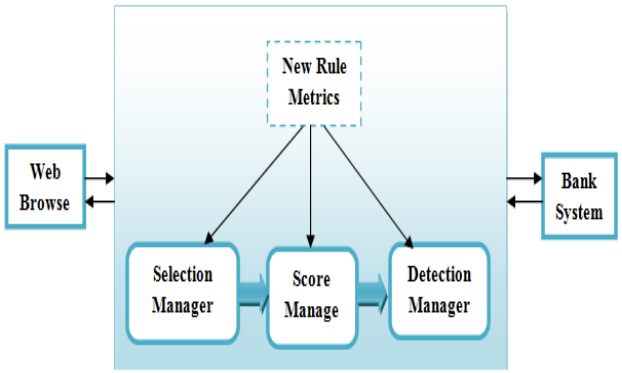

Figure 2: System Architecture

New Rule metrics defines new rules related to filtering of the customer request and attacks. Rules are to be selected by IPS for analysis. The selection is based on belief of the attack. Selection manager need to determine the rules for which some abnormal thing is observed. Selection manager checks the incoming traffic profile and selects the rule to be forwarded to the score manager. Score is allocated to the rule by the score manager. Score list is maintained, but even the score is high or low it is used to check the attack. There is final step that determines the attack. If the incoming request breaks the rule defined, the detection manager marks it as an attack and blocks that person/IP. Web browser is used by the customer to carry out their transaction of bank. Client sent their transaction request to the bank system via any web browser. And all the bank related activities i.e. maintain customer record is done in bank module.

4. Methodology

4.1 Algorithms

In the proposed system following algorithm is being used for the detection of attack.
Input= {number of customers, request by the customers}
Output= {attack detection}

1. if IP_ID== mID then
2. bv_j=false
3. return
4. else
5. $rate_j$=$rate_j$+Fq_j
6. if $rate_j$>cap_j then
7. bvj=false
8. raise alert
9. return
10. else
11. forward request to system
12. end if
13. end if

Here IP_ID holds the IP address, cap_i is the stored capacity for each rule. Bv_j is a Boolean variable. If the rule for particular request is greater than the defined capacity an alert is raised. Else the request is forwarded to the bank system. After the attack is detected it also needs to be prevented.

In the proposed system following algorithm is being used for the prevention of attack.

Mitigation(r [])
1. for i =1 to n
2. if r[i]== follow
3. Legitimate request
4. else
5. Temporary block
6. Provide opt
7. if otp==1
8. Legitimate user
9. else
10. Permanent block
11. end if
12. end if
13. end for

In above algorithm otp is one time password. In proposed system protection against attack is provided in two steps. Here if all the rules are followed the request is considered legitimate request and is forwarded. And if any of the rule is not followed that user or IP is temporarily blocked. The blocked user is then provided one time password if the password matches correctly that user is provided further provided access or is permanently blocked.

4.2 Math Model

System can be described mathematically through. S will describe whole system.
So S will be,
S= {Input, Process, Output}

Input:
Input = {Input dataset of IP packets including time}

Process
1. **Compute a Frequency:** It is the number of request that matches with rule.

$$FRQ_i = \frac{FRQ_i}{\sum_{j=1}^{n} FRQ_i} \quad \ldots (1)$$

Where, FRQ_i is the no. of request matched with rule r_i.

2. If there is a flooding attack, the traffic volume increases and so does the frequency of some rules. Thus, a request rule with some frequency or frequency higher than a certain threshold will be selected as a potential attack at time. To check whether the traffic follows the profile i.e. within the defined rules,

$K(fq, fq') \leq \omega$

Where, where fq is the current frequency of rule, fq' is the maximum traffic profile, and ω the maximum admitted deviation from it.

Output:
Output= {Attack detection and prevention}

5. Result Analysis

5.1 Hardware and Software used

Hardware Used
-Processor: Pentium IV ad above.
-RAM: 256 MB (min) and above.
- HDD: 20 GB and above.
-Key Board: Standard Windows Keyboard.
-Speed: 1.1 GHz.
-Nodes: Laptops as customer nodes
-LAN: Switches

Software Configuration

- Operating System: Windows XP and above.
- Tool: Net Beans
- Programming Language: Java.
- Database: SQL.

5.2 Result of Propose Work

Following snapshots are showing the result of the work done in proposed system.

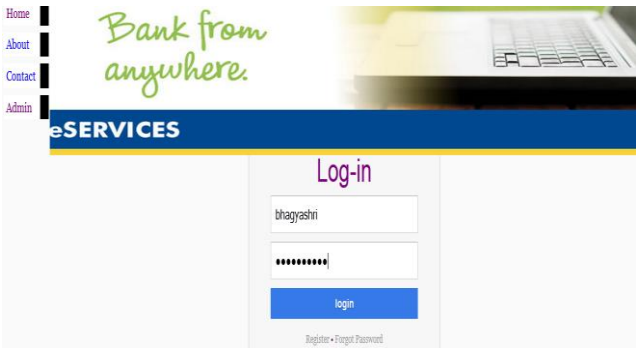

Figure 3: Customer login after they subscribe to Firecol System

Account No	Name	Signup Time	IP	Usertype
1	bhagyashri	2015-22-05 11:17 AM	192.168.1.5	Normal
4	nilam	2015-22-05 11:22 AM	192.168.1.5	Normal
4	nilam	2015-22-05 11:23 AM	192.168.1.5	Normal
1	bhagyashri	2015-22-05 11:29 AM	192.168.1.5	Attacker

Figure 4: The IP that is blocked after an attack is detected from that IP

6. Conclusion

This paper proposed Firecol system, which is useful for early detection of DDoS attacks at HTTP layer. Attack information is shared among all the IPS within the rings. It provides protection to the subscribed customer and saves lot of network resources by detecting the attacks close to the source of attack. In this paper we are providing the security at all the layers. Irrespective of whether the score is high or low we block all the attacks when they occur. By IPS multiple level of protection is applied among the source and destination. It shares intelligence of one LIDS with other so that maximum blacklist is shared among the IPS. The proposed system defines the new rule metrics suitable for the application for filtering the attacks.

References

[1] J. François, I. Aib, and R. Boutab,"FireCol: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks," IEEE 2013 Trans on Netw, Volume: PP, Issue: 99
[2] A. Networks, Arbor, Lexington, MA, "Worldwide ISP security report," Tech. Rep., 2010.
[3] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the DoS and DDoS problems," Comput. Surv. vol. 39, Apr. 2007, Article 3.
[4] K. Xu, Z.-L .Zhang, and S. Bhattacharyya, "Internet traffic behavior profiling for network security monitoring," IEEE/ACM Trans. Netw., vol. 16, no. 6, pp. 1241–1252, Dec. 2008.
[5] E. Cooke, F. Jahanian, and D. Mcpherson, "The zombie roundup: Un- derstanding, detecting, and disrupting botnets," in Proc. SRUTI, Jun.2005, pp. 39–44.
[6] S. M. Bellovin, "Distributed Firewall," Login Mag., vol. 24, no. 5, pp. 37–39, Nov. 1999.
[7] Y. Kim, W. C. Lau, M. C. Chuah, and H. J. Chao, "Packet Score: A statistics-based packet filtering scheme against distributed denial-of-service attacks," IEEE Trans. Depend. Secure Comput. , vol. 3, no. 2, pp. 141–155, Apr.–Jun. 2006.
[8] J. Françcois, A. El Atawy, E. Al Shaer, and R. Boutaba, "A collaborative approach for proactive detection of distributed denial of service attacks," in Proc. IEEE MonAM, Toulouse, France, 2007, vol. 11.
[9] Paxson ,"End-to-end routing behavior in the Internet," IEEE/ACM Trans. Netw., vol. 5, no. 5, pp. 601–615, Oct. 1997
[10] Y. Zhang, Z. M. Mao, and M. Zhang, "Detecting traffic differentiation in backbone ISPs with NetPolice," in Proc. ACM SIGCOMM Conf.Internet Meas., 2009, pp. 103–115.
[11] L. Feinstein, D. Schnackenberg, R. Balupari, and D. Kindred, "Statistical approaches to DDoS attack detection and response," in Proc.DARPA Inf. Survivability Conf. Expos., 2003, pp. 303–314.

Author Profile

Bhagyashri B. Kotame received B.E (CSE) from Pune University College of Engineering, Kopargaon and pursuing M.E (CSE) in Savitribai Phule Pune University University College of Engineering Sangamner. My area of research includes Computer Networks, Network Security.

Shrinivas Sonkar received the ME (CSE) from SRTMU Nanded and registered Ph.D in Computer Science & Engineering from Pune University. He is currently working as Professor in the Department of Computer Engineering at **Savitribai Phule Pune University College of Engineering Sangamner.** He has ten years of teaching experience and has guided many projects in the area of Network Security and Cloud Computing for CSE Departments. His research interests are in the areas of Network Security and Cloud Computing.