International Conference on "Emerging Trends in Computer Engineering, Science and Information Technology "-2015
Special Issue of International Journal of Electronics, Communication & Soft Computing Science and Engineering, ISSN: 2277-9477

Firecol: An Intrusion Prevention System for Minimization of DDoS attacks

Bhagyashri B. Kotame **Prof. S. K. Sonkar**

Abstract — **Distributed denial off service attacks (DDoS) are big threats to the Internet and detection of such attacks away from the victim and close to the attack source is a big challenge. But is necessary for protection of end-users and expensive network resources. We propose a new framework in order to overcome this problem of DDoS attack named Firecol. The victims who need protection can subscribe to Firecol system. The Firecol system is based on some routing rules depending on which the request from the customer is filtered. An alert is raised and the information is stored in backend for further analysis.**

Key Words — **Distributed Denial of Service (DDoS), Intrusion prevention system (IPS), Botnets, Detection, Mitigation.**

I. INTRODUCTION

Providing security to the network has become necessary for the existence of many entities that completely or partially depends on their internet presence. In order to stay competitive in today's global market it is necessary to provide protection against network attacks. DoS attack is considered as one major threat for Computer network. Distributed denial-of-service attack is packet/request flooding attack, which constitute major concern even though many works are done to protect the end user's from this attack.

Large set of machines known as zombies are used to launch DDoS attacks over some server or machine. DDoS attack has grown around 100 GB / s the mitigation off which is difficult. The main focus of this paper is detection of DDoS attacks and to note their vector. In non distributed DoS attack few carefully forged packets / request are used to interrupt a service where as Distribute DoS attack is used for flooding the victim by sending the traffic more than its predefined threshold. The DDoS attacks are heavily effective against any type of attacks.

In case of distributed database it is very difficult for single intrusion prevention system or intrusion detection system to detect the DDoS attack. Provided they need to be located near to the victim. Further the IDS/IPS may crash because huge volume of traffic/request is flowing through it. The internet resource can get strain by allowing massive traffic to pass through Internet and just blocking it at host IDS/IPS.

We are providing firecol system in Tier 3 networks, here the clients who needs protection can get this optional service from Internet providers and will be charged for it. The IPS and subscribed customer communicate by computing and exchanging belief scores on attacks. The IPS is placed in between the attacker and the bank application. Along with detection of DDoS attack firecol also detects other attacks such as flash crowds and botnet based DDoS attacks.

Objective

- To increase the accuracy as well as robustness of the system.
- To gain efficiency by using different HTTP layers.
- Introduce new rules for better analysis of traffic.
- When Firecol application finds n/w system under attack that time system automatically blocks unwanted messages from particular system and block that particular IP from n/w so that without manual change in system this software automatically change the system setting and prohibit system from attack.

II. LITERATURE SURVEY

J. Francois, A. EI Atway, E. A Shaer and R. Boutaba [2]. In this paper they presented a FireCollaborator system which is distributed detection and information sharing system where several IPS (Intrusion Prevention System's) collaborate to prevent the distributed attack close to the source of attacker. In contrary to solution those are applied at low level in the network, the solutions at ISP level save lot of resources as attacker's location with it is easy to determine more precision. They proposed a framework in order to improve the security at higher level. Here in order to share valuable information the IPS communicates with one another. They proposed a system where the client need to subscribe to the protection service with less communication overhead and unsubscribed customers are not provided the service. Selecting the rule for which attack is severe is responsibility of IPS. They presented their system had no false positives due to alert information technique.

A. Networks, Arbor, Lexington, MA carried out various annual operational security surveys. The survey was carried out in order to provide valuable data that the network operators can use so as to make their decisions related to use of network security technology in order to provide security to their mission critical infrastructure. The main focus of this survey is the issues related to the day-to-day aspects of security in commercial networks and operational network securities. The major focus of this survey is to present the real world concern and the emerging attacks those are addressed elsewhere. Over the last two three surveys the ISP security has grown. For protection against distributed denial of service attacks; the ISP spend many of their resources.

T. Peng, C. Leckie, and K. Ramamanoharao [3] in the paper they presented the aim why internet was designed was for scalability and openness. IP (Internet Protocol) was designed so as to make the attachment of host and network easy, but did not provide complete support. So as to verify the contents of header

field of IP packets. As a result of which it becomes easy to take source address of a packet. The described various bandwidth based attacks like Infrastructure attacks, Distributed Reflector attack, Protocol and application based attacks. They presented four different types for preventing the Dos attacks. 1) They stated how the Dos attack can be protected and how they can be stopped before causing any severe harm. They assume that the source address of the traffic is spoofed. But also includes filtering of the packets at the router, where only the legitimate traffic is allowed to pass through it. 2) After they presented the detection of DDoS attack is different from other intrusion detection. General intrusion detection is possible by the dropping the files those are created by the attacker or by making modifications in system logs. Detecting the DoS attacks is very difficult as well as the services provided by the target machine gets poor. 3) They presented identification of source attack. 4) Reaction of attack.

E. Cooke, F. Jahanian, D. McPherson [4] they mentioned the base (origin) and the structure of botnets. They described the messaging scheme over the Internet in form of one-to-one or one-to-many by the system of Internet Relay Chat (IRC) channel. They also mentioned the methods for detecting bots based on IRC. They stated three different approaches for overcoming the bots problem. 1) By detection of command and control communication among bots and controller and bots. 2) System is being prevented from getting infected. 3) By detection of secondary features of the bots infections. By the correlation of secondary detection of information to the pinpoint bots and botnet communication they describe the botnet detection approach.

K. Xu, Z.-L Zhang, and S. Bhattacharyya [5] they described simple method for building comprehensive behavior profiles of Internet backbone traffic in terms of communication pattern of service and end-host. Their main aim is profiling of the Internet backbone traffic by automatically discovering the behaviors of interest from huge traffic of data and also providing possible interpretation of this behavior that helps the network operators in understanding and quickly identifying abnormal event with a huge amount of traffic. They combinedly used data mining and entropy based techniques so as to automatically gather valuable information from largely unstructured data. Entropy based approach was adopted to extract clusters of significance, instead of using a fixed threshold based on volume. After the cluster extraction in the second stage of their methodology they discovered the "structures" among the clusters and from that they build common behavior models for profiling. They demonstrated, blocking the most offending sources is cost-effective.

S.M Bellovin [6] he described what is firewall and the requirement of firewall over Internet. Some people think if cryptography is used there is no need of firewall, but Bellovin stated the firewall is a powerful protection mechanism. He described what hybrid firewall is and distributed firewall. IPSEC and the firewall are synergistic and with the help of IPSEC a strong firewall can be implemented. Due to which the limitations of today's firewall are removed. Complete implementation of distributed firewall is flexible and secured. They retained the centralized policy control and protection they eliminated the dependency on the topology and IP addresses.

III. PROPOSED WORK

A. *Proposed System*

The exponential growth of network attacks is becoming more and more difficult to identify, so the need for better and more efficient Intrusion Detection system increases in step. The main problem with the current intrusion detection system is high rate of false alarm. In the existing system the customer who needs to protect their transmissions must subscribe to the firecol service via the trusted server. The subscribed customer is provided protection based on some predefined set of rules. The packets send from the sender passes through the system, here the predefined rules match the pattern of IP packets coming from the sender. These can include ports, protocols or any other monitor able informational. Whenever the packets are received their frequencies are counted (frequency= number of packets matching some predefined rule). If this count for particular rule is found high it is considered as an attack and that IP is blocked. But there are some limitations with the existing system, they provide security only till the network layer, the rate of false alarms is high. Also in case of distributed database huge traffic flows over internet and by just blocking it at host IPS can result in loss of network resources.

In proposed system the customers of bank are provided the value added protection service in build by the bank. We are defining new rule set for the bank application based on which the request from the customer will be filtered. We are also providing the security at all the layers, due to which the level of security increases. In case of distributed database firecol allows sharing of intelligence between one LIDS with other. The proposed algorithm performs in deep http analysis due to which security is provided to great extend. Here we are maintaining two blacklists were one blacklist contains the list of attackers by their name while the other contains the IP addresses, these lists are maintained based on different parameters (i.e. different rules). Due to which that user or IP from where the attack took place is permanently blocked. Here the concept of temporary block and permanent block is used. Once the customer is temporarily blocked he/she is provided one time password (OTP) if at all the OTP is found wrong that customer is permanently blocked.

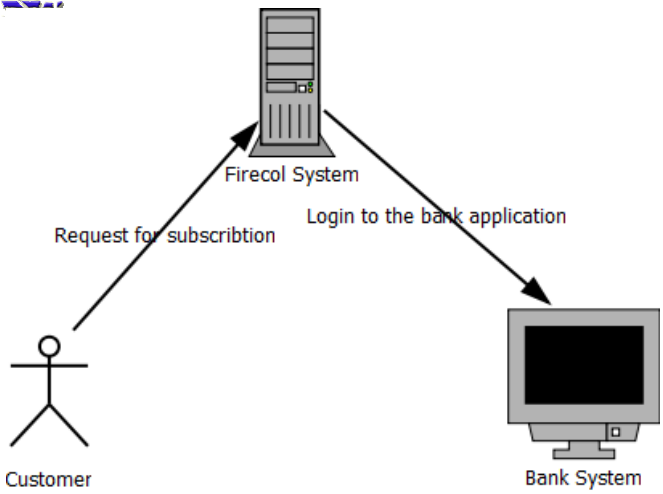

Fig.1. Subscribe to Firecol System

The proposed system consists of following six major parts:

1. Bank Rule Metric.
2. Selection Manager.
3. Score Manager.
4. Detection Manager.
5. List of Score.
6. Bank_System.

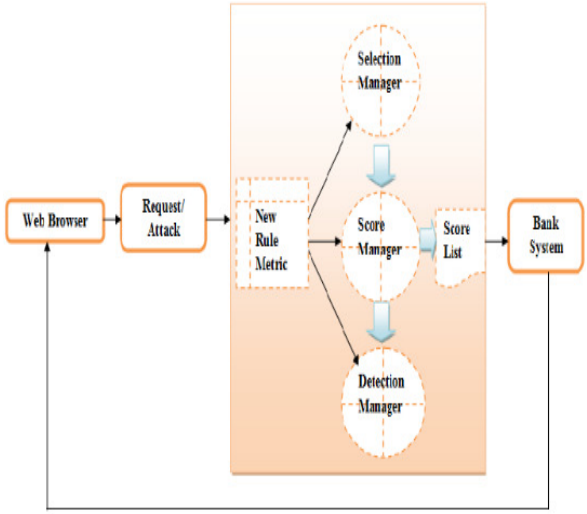

Fig.2.System Architecture

Firecol system is formed by Bank Rule Metric, Score Manager, Selection Manager, Detection Manager, and List of Score. The Bank rule metrics defines bank related transaction rules based on which the filtering of customer request can be done. For analysis the IPS selects the rules on the basis of belief score of the attack. It is responsibility of selection manager to determine the rules for which the abnormal behavior is observed. It checks the profile of incoming traffic and chooses the rules to be forwarded to the score manager. Score for the rule is allocated by the score manager. A separate score list is maintained and whether the score for particular rule is low or high is used to check an attack. Finally if any incoming request breaks some rule, the detection manager marks it as an attack and blocks the customer IP. All the bank transactions are carried out by the customer through the web browser. All the customer details related to bank are maintained by the bank application.

B. Algorithms

In this system the algorithm used for attack detection is as follows:

Input= {request for transactions by the customer}

Output= {detection of attack}

1. If ID_IPS== ID_My then
2. bv_k=false
3. return
4. else
5. $rate_k=rate_k+Fq_k$
6. if $rate_k>cap_k$ then
7. bv_k=false
8. raise alert
9. return
10. else
11. forward customer request to application
12. end if
13. end if

Here ID_IPS holds the IP address, cap_k is the stored capacity for each rule, bv_k is a Boolean variable. If number of request for any rule is more than the predefined capacity an alert is raised. Else the request is forwarded to the bank system. After the detection of attack it also needed to prevent that attack.
For one rule we are using the classification algorithm of naive based so that the average transaction of a customer can be found out for a day. So if the attacker is using the account of the legitimate customer he/she will be unaware of the amount that is regularly with drown by the legitimate customer. And hence can be caught.

In this system the algorithm used for the mitigation of attacks after its detection is as follows.

Mitigate(rule [])

1. for j =1 to n
2. if rule[j]== follow
3. Legitimate request
4. else
5. Block temporary
6. Provide customer with OTP
7. if OTP==1
8. Legitimate customer
9. else
10. Block permanently
11. end if
12. end if

13.end for

In this algorithm OTP variable is one time password. In this system protection against attack is provided in two steps. 1) If all the rules are followed the request is considered legitimate request and is forwarded to the application. And if any of the rules are not followed that user or IP is temporarily blocked. The blocked user is then give one time password if the password found correct that user is provided further provided access or is permanently blocked.

C. Mathematical Model

The entire system can be mathematically described; here FS presents the entire system.
So,
FS= {Input to the system, Process, Output of the system}

Input:
Input= {input is request for transaction from customer along with time}.
Process:

1. Frequency Computation:
It is number of customer request matching the rule R_i.

$$FRi = \frac{FRi}{\sum_{i=1}^{n} FRi} \quad \ldots. (1)$$

Here FR_i is the number of incoming request those match with rule.

2. In case of flooding attacks the volume of the incoming traffic increases and thus the frequency of few matching rules. Thus for the incoming request, if the frequency for some rule is set or the frequency for some rule crosses the threshold value it is considered as a potential attack. In order to check that whether or not the traffic follows the profile i.e. within the predefined rule.

$$K (frq, frq') \leq \alpha$$

Here frq is the current frequency of some rule R and frq'is the maximum traffic profile and α deviance from it.

Output = {the attack from the request is detected and prevented}

IV. Result Analysis

The result obtained as the output of the proposed system is as follows:

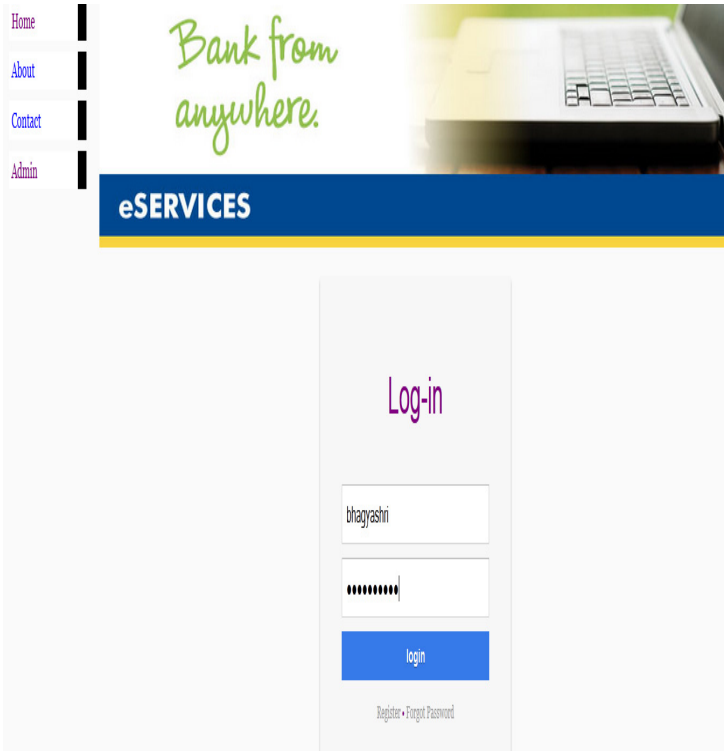

Fig.3. Login for customer of bank
Fig.4. Found as an attack if some rule is broken.

Fig.5. SQL injection attack
Fig.6. Session hijack attack

Conclusion

We propose Firecol system which is helpful in selection of DDoS attack before expected time at the HTTP layer and also its mitigation. This is scalable solution for detection of DDoS attacks. In case of distributed database multiple IPS are used and the attack information is shared among these IPS. Many network resources are being saved by detection and mitigation of attack close to the source of attacker and also the subscribed customer are provided protection. Whether the score for any rule is high or low we are blocking any customer who breaks the rule as a result of which the security is provided to great extent. Also we are providing security at all the layers. Due to Intrusion Prevention system high level of security is applied between the source and destination of request. It is sharing protocol, shares the intelligence of one LID with other. So much more blacklist is shared among the IPS. The system defines bank rule metrics which is suitable for bank application for the filtering of attacks.

Acknowledgment

My sincere thanks go to Amrutvahini College of Engineering for providing us a platform where we can develop our skills and capabilities. I would like to thank our guide for their constant support and motivation. Also I would like to thanks HOD of computer department and PG Coordinator who helped me in presenting this paper.

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] 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

[3] A. Networks, Arbor, Lexington, MA, "Worldwide ISP security report," Tech. Rep., 2010.

[4] 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.

[5] E. Cooke, F. Jahanian, and D. Mcpherson, "The zombie roundup: Understanding, detecting, and disrupting botnets," in Proc. SRUTI, Jun.2005, pp. 39–44.

[6] 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.

[7] S. M. Bellovin, "Distributed Firewall," Login Mag., vol. 24, no. 5, pp. 37–39, Nov. 1999.

[8] Paxson ,"End-to-end routing behavior in the Internet," IEEE/ACM Trans. Netw., vol. 5, no. 5, pp. 601–615, Oct. 1997

[9] 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.

[10] 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.

[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

[12] A. Feldmann, O. Maennel, Z. M. Mao, A. Berger, and B. Maggs, "Locating Internet routing instabilities," *Comput. Commun. Rev.*, vol. 34, no. 4, pp. 205–218, 2004.

[13] A. Basu and J. Riecke, "Stability issues in OSPF routing," in *Proc. ACM SIGCOMM* , 2001, pp. 225–236.

[14] M. Dischinger, A. Mislove, A. Haeberlen, and K. P. Gummadi, Detecting bittorrent blocking," in *Proc. ACM SIGCOMM Conf. Internet Meas.*, 2008, pp. 3–8.

[15] 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.

AUTHOR'S PROFILE

Passport Size Latest Color Photo	**Bhagyashri B. Kotame** Completed 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.
	**Prof. S. K. Sonkar** Completed 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.