International Journal of Emerging Technology and Advanced Engineering
Website: www.ijetae.com (ISSN 2250-2459 (Online), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 1, January 2013)

International Conference on Information Systems and Computing (ICISC-2013), INDIA.

IHONEYCOL: A COLLABORATIVE TECHNIQUE FOR MITIGATION OF DDoS ATTACK

M.Buvaneswari[1], Ms.T.Subha[2]

[1]*PG Student ,Department of Information Technology, Sri Sairam engineering college, Chennai, India;*
[2]*Associate Professor,Department of Information Technology, Sri Sairam engineering college, Chennai, India.*
Email: address buvaneswarisanthi@gmail.com,subharajan1979@yahoo.co.in

Abstract

Distributed denial of service is flooding of network with unrelated information by malicious node. Thus causing the authorized service deny from user. This distributed denial of service poses a major security threat. The mitigation of distributed denial of service becomes hard when they it comes to distributed environment. In general denial of service intended to shut down for a period of time. The discovery of these attacks become challenging when we intend to use expensive network devices. In this paper we propose a technique called iHoneyCol which effectively mitigate distributed denial of service rather than present filtering approach. iHoney Col is integration of Firecol and Honey pot. The core of Firecol is composed cluster of intrusion prevention system IPS which form the mitigation shield around the user. Honey pot is a trap set to detect the malicious node and monitor the traffic for prevention of attacks in future.

***Keywords*-- IPS rule, DDoS, Honey pot, clone attack, Ping of death.**

I. INTRODUCTION

Distributed Denial of Service attack or more accurately packet flooding attack, in contrast to logical DoS attack that exploits OS or application vulnerabilities[1].Worms are also emerging threats and they are not unrelated to DDoS problem as they are being used to conquer attack agents.

The state of the art DDoS detection algorithm assumes that detection infrastructure is located near saturated link in vicinity of victim, where the detection is easy. The tradeoff in this case is that detection algorithm can be simplified but local response is ineffective as available bandwidth has already been consumed in upstream path.

To couple with this problem technique like “IP trace back”[2] or “IP pushback”[3] aim to find attack source and potentially move countermeasures near the source of attack. The proposed new framework named “Fire collaborator” to deal with this problem on ISP level based on collaborating IPS[4].It is distributed detection and alert information sharing system that allows several IPS’s to collaborate in order to stop distributed attack as far as possible from victim. Honeypot is tactic or trap set to detect an unauthorized user by recording the patterns of malicious traffic over network.

II. RELATED WORK

Fire collaborator is a hardware or software device that helps in mitigating the effect of distributed denial of service. Initially the customer register at ISP level. After registering the client is assigned with individual unique identifier.

If more than two users use the same identifier malicious node is detected. Firecol contains many IPS rules according to that the detection of any malicious traffic.

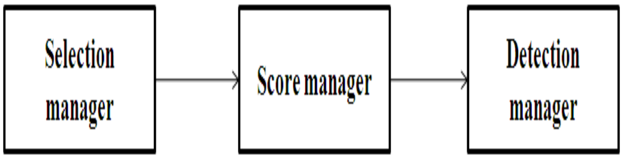

Fig1.Firecol functions.

Here the firecol contains many rules. These rules will be executed in the following manner. It contains a selection manager for determining the rules and any abnormal traffic observed. Score manager assigns the belief score according to the rules designed.

These scores can be exchanged as a worth of trust among the neighboring clients. Detection manager aims at detecting the authorized and unauthorized traffic among the incoming flow of data traffic. These are the existing solution to DDoS problems

1 Attack prevention and preemption, where the attack is prevented at client side itself so that the mitigation is done far from the destination. Pre-emption is when the attacker is authorized to send any malicious data. They get swapped by neighboring network devices.
2 Attack detection and filtering, where an attack is detected and they are filtered according to the traffic pattern registered at network devices. These filtering technique can be embedded into firewall through software or we can use separate hardware devices.

3 Attack source trace back and identification, once the attack has been identified the main source of attack is detected. Their individual IP address is added to black list by honeypot severs.

In general, DDoS solution has two phases,
1) *deployment phase*: deployed in one or more compromised node before attacks
2) *Attack phase:* where prevention of attack takes place.

Mitigation of Distributed Denial of Service include weapons like spoofing, prevention technique(Ingress and RPF filtering[5]),manually employed countermeasures (firewall filtering, rate limiting or route black holes[6]).

In multiple network domain[7] detect abrupt traffic changes over multiple domain. The main advantage is accuracy in detection .However it suffers from communication overhead. Distributed Denial of Service attack has been detected by group testing[8] basis, which is done at backend server. Here malicious request are indistinguishable. Distributed denial of service detection prevails as a detection of IP trace back[9], which quantify the network traffic. This also reduces the false alarm rate. In addition to this honey pot cannot be designed as sole source of network security. They can be incorporated with network firewall software or devices.

III. Proposed Work

The integration of “Firecol” and “Honeypot” helps in mitigating distributed denial of service to acceptable amount. The honeypot provides an organization information on their own security risk and vulnerabilities. It should consist of similar system and application that one used by organisation’s for its productive environment.

So to give the attacker a real world feeling and to be able to implement the learned lessons in productive environment. So we have planned to integrate the core concept of firecol and honeypot in order to achieve higher efficiency and provide better performance.

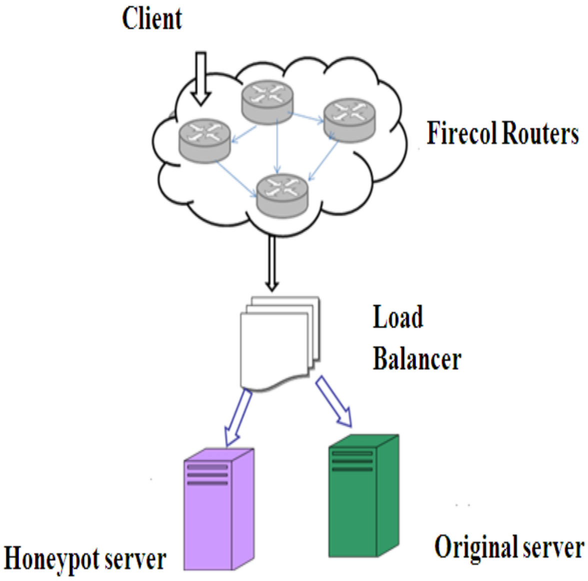

Fig2.System Architecture

The above system architecture proves the flow of traffic and identity of malicious traffic in an efficient way. In any network environment the client register themselves with their own ISP,s. After the registration is fulfilled, they are notified as an authorized client. Here two major problem of a network are addressed. They are clone attack and PoD attack.

CLONE ATTACK:

These attacks are nowadays called as “twin attack”. Its nothing but when an unauthorized client spoof the IP address of any authorized client to flood the network.

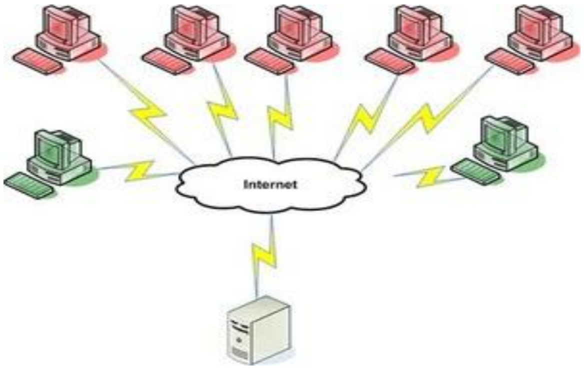

Fig3:Clone attack

It also has a special case when an authorized client himself spoof the IP address of any other authorized client. Here comes the function of firecol in a smart way.

The proposed solution is when all the client register themselves with ISP,s they also send their individual IP address, their location and time to the firecol router. The firecol router in turn response with the ACK packet and generate individual random number to all nodes. These random numbers are assigned to all nodes. The IP address, location and random number assigned to nodes. These information get stored in routing table of firecol router. The generation of random number is shown in figure4.

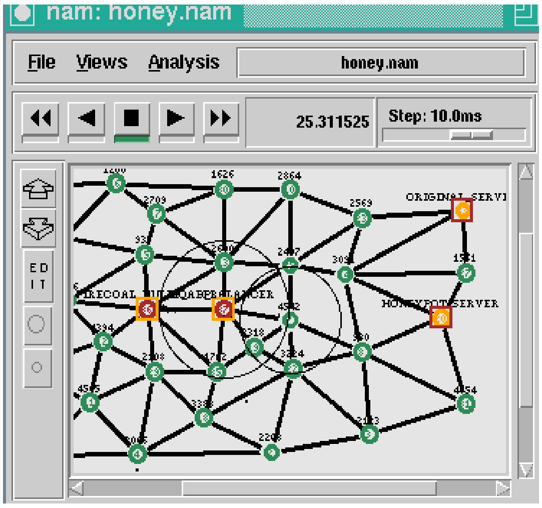

Fig4:Random number generation for clone attack.

Once if an authorized client spoof IP address of other node and tries to flood the network, the firecol checks the IP address and random number of that client. If any inconsistencies in that data occur then that client with unique random number is blacklisted as clone or malicious client. The information is immediately routed to honeypot server. The honeypot server add this particular client into black list and disconnects its TCP connection to all nodes.

PoD ATTACK:

PoD, in general known as ping of death. This attack can be defined as every data packet contains ICMP header which sends ECHO REQUEST and ECHO REPLY. If the ICMP data header exceeds 65,536 bytes crashes the entire system.

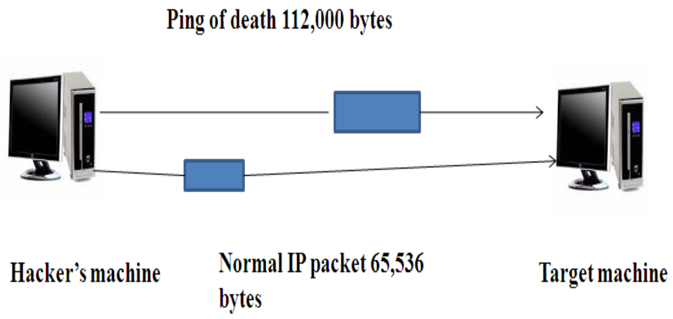

Fig5:PoD attack.

In existing system these can be overcome by fragmenting the data. The main drawback of this system is that the destination system cannot handle larger fragment of data, so they crashes. The proposed solution is disallowing the client themselves to send larger amount of data.

So that the traffic has been blocked away from the destination. The client attempt to send such a traffic flood will be recorded as black listing client by honeypot server. The other solution is "virtual fragmentation" of ICMP header packet.

That is, as soon as the client sends such a larger amount of ICMP data, they get fragmented at firecol and pass the original data to original server.

These activities are broadcasted to honeypot server by firecol. So at final honeypot server disconnects particular clients TCP connections. So that they are not eligible to transfer the data to any of the neighboring nodes.

So by virtual fragmenting the data the information loss can be reduced. The virtual fragmentation is done by firecol router without the knowledge of client. So the user thinks that they are going to crash the system(disguises themselves).

IV. CONCLUSION

Therefore iHoneycol, provides a collaborative solution for the early detection of flooding DDoS attacks by making use of "Firecol-IPS" system and "Honeypot-IDS" system. It prevent the attack as close to the source and as far from destination, providing a protection to subscribed customers and saving valuable network resources. Also, the study of iHoneyCol demonstrated its light computational as well as communication overhead.

Being offered as an added value service to customers, the accounting for iHoneyCol is therefore facilitated, which represents a good incentive for its deployment by ISPs. In general, iHoneycol which overcomes twin attack and ping of death attack in an efficient manner using a collaborative technique.

REFERENCES

[1] C.Siaterlis,B.Maglaris.”Detecting DDoS attacks with passive measurement based heuristics”,IEEE conference publication 2004.

[2] S.Savage, D.Wetherall, A.Karlin, T.Anderson.”Practical network support for IP traceback”, proceedings of 2000ACM SIGCOMM conference.

[3] J.Ioannidis and M.Bellovin. ”Implementing pushback,router based defense against DDoS attack”, proceeding of NDSS,Feb2002.The internet society.

[4] J.Francois,Adel,E.Atawy,E.Al-Shaee, R.Boutaba,”A collaborative approach for proactive detection of DDoS attack”,IEEE transaction 2012.

[5] CISCO.Remote triggered blackhole filtering.ftp//ftp_eng.cisco.com/cons/isp/security/.

[6] Kai Hwang and Wei-Shinn Ku,” A collaborative detection of DDoS attack over multiple domain”, IEEE journal 2007.

[7] Yin Xuan, Incheol Shin, My T.Thai,Taieb Znati, ”Detecting application Denial of Service attack: A group testing based approach”, IEEE publication 2009.

[8] Yan Xiang,Ke LI,Wanlei Zhou,”Low rate DDoS attackdetection and traceback by using new information metrics”,IEEE publication 2011.

[9] Nathalie Weiler,”Honeypots for DDoS attack”,IEEE conference publication 2002.