International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | Apr-2016 www.irjet.net p-ISSN: 2395-0072

Prevention of Distributed Denial of Service Attack using Web Referrals: A Review

Mrunali Desai[1], Sawan Patel[2], Parag Somaiya[3], Vishal Vishwanathan[4]

[1]*Professor, Computer Engineering, K.J. Somaiya Institute of Engineering And Information Technology, MH, India*
[2]*Student, Computer Engineering, K.J. Somaiya Institute of Engineering And Information Technology, MH, India*
[3] *Student, Computer Engineering, K.J. Somaiya Institute of Engineering And Information Technology, MH, India*
[4] *Student, Computer Engineering, K.J. Somaiya Institute of Engineering And Information Technology, MH, India*

Abstract - ***Distributed Denial of Service (DDoS) attacks are potent, new form of attack on the availability of Internet services and resources. A DDoS attack, by definition, is any attack intended to cause a service to become unavailable or unusable. In a DDoS attack, there are no inherent limitations in the number of machines that can be used to launch the attack. The distributed nature of the internet helps a DDoS attack with hosts owned by disparate entities around the world. We are making a java based filter which will have restriction on number of request in particular time, IP access permissions, alarm in case of heavy load on server, checking of extensions because .exe extension can be used for DoS attack, and size limit for data transfer from server. We are demonstrating how this DoS attack can be prevented and smooth services can be given to trusted clients even when the DoS attack is performed on server. During attack, the trusted clients will be provided with uninterrupted service. The access mechanism for trusted clients will be based on the token. We are implementing a filter at application layer which will monitor the request coming from clients, size of data, .exe extensions etc. There may be chances of DDoS attack from different clients within the network. So, DDoS prevention mechanism has been designed. There will be 5 modules in the system which will prevent DoS and DDoS attacks.***

Key Words: *DDoS attack, Filters, Security.*

1. INTRODUCTION

A Denial of Service (DoS) attack can be referred as an attack with the purpose of preventing legitimate users from using a victim machine/network resource. A Distributed Denial of Service (DDoS) attack is a large scale, coordinated and synchronized attack on the services available to the victim system or network resource, launched indirectly through many compromised machines on the Internet. The services under attack are those of the "primary victim", while the compromised machines used to launch the attack are often called the "secondary victims." The use of secondary victims in performing an attack provides the attacker with the ability to wage a much larger and more disruptive attack, while making it more complicated to track the original attacker. As defined by the World Wide Web Security FAQ: A Distributed Denial of Service (DDoS) attack uses many computer systems to launch a coordinated DoS attack against one or multiple targets. Using client/server technology, the attacker can easily multiply the effectiveness of the Denial of Service significantly by harnessing the resources of multiple unwitting compromised computers which serve as attack platforms.

2. EXISTING SYSTEM

The process of design comprises "conceiving and planning out in mind and making a drawing, pattern or a sketch". The system design shows a logical representation of what a given system is required to do into the physical reality at the time of development. Important design concepts such as reliability, response time, throughput of the system, etc., should be taken into consideration. Design constraints like cost, hardware limitations, standard consent etc. should also be handled. The task of system design is to take the description and associate it with a specific set of machines, accommodation, etc., to provide entire specifications of a working system. This system must provide all of the significant data processing and it may also do some of those tasks found during the analysis phase as optional extras. It must work within the enforced constraints and show better performance over the existing system. At the beginning of design a choice must be made between the main approaches. Preliminary design concerns with identification analysis and selections of the major design options are available for development and implementation of a system. These options are most prominent in terms of the physical facilities to be used for the processing who or what does the work.

Application Layer Attacks: These attacks targets on a weakness in a particular web application. They are the most sophisticated, stealthy type of DDOS attacks because

they can be very effective without generating abnormal amounts of traffic. This "low and slow" approach makes attack very complicated to detect using traditional volumetric detection mechanisms. Recently, Kevin Kennedy, Sr. Director of Product Management at Juniper Networks, noted in a blog post: "Forget armies of bots, just a single computer machine was enough to generate a small, well targeted attack that took down one of the E tailors in Europe within several minutes, And precisely just because it was not so severe, it was lost in the noise of legitimate user traffic, taking a full day to identify and remitted and putting $10M of sales at risk." 9 attacks, the scope of DDoS targets also remains broad. The challenge with application layer attacks is to distinguish human traffic from bot traffic, so DDoS mitigation providers usually follow browser fingerprinting techniques like cookie tests and JavaScript tests to check if requests actually come from legitimate browsers. Launching DDoS attacks from hidden, but real browser instances running on infected computers makes this type of detection very hard.

3. PROPOSED SYSTEM

The architecture of the proposed system is shown in the Fig.1.

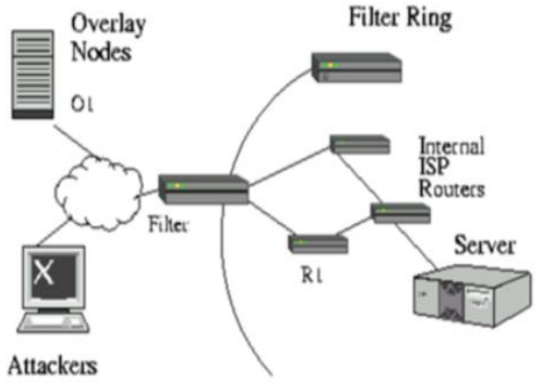

Fig -1: Proposed System

We distinguish between the terms byte pattern, flow pattern and traffic pattern. A byte pattern is a sequence of bytes within a packet. A flow pattern is a serial of packets that together forms a specific attack. A traffic pattern is an aggregation of multiple flow patterns that target the same site. We do attack detection by trying to observe traffic abnormalities. We argue that traffic -pattern need to be analyzed for this. For the identification of packets belonging to a specific attack, we determine its signatures. Attack signatures can be detected either by byte patterns or flow patterns. Once this has been done for a specific attack, a countermeasure can be selected and activated to deal with attacks.
The proposed system is based on a variety of filters which basically, keeps track on user activities, which led to a DDoS or a DoS attacks to occur, and also these filters can prevent attacks like flooding, phising, buffer overflow, syn flood attacks. These filters are designed and programmed in java using web referrals. The system can be used by organization on a small scale, prevent DDoS and Dos attacks.

Filters: Apart from host blocking, it is required to filter attack traffic out based on protocol and payload information. One reason is that the set of victim hosts may only sometimes be identified fully, for example if some infected hosts do not pass the worm in the system but wait silently after infection until they start to participate in a DDoS attack. In a filter, it may be desirable not to block all HTTP traffic to a site under attack, but just a specific query or query type as transmitted by some known infected hosts. In order for this to work, byte patterns have to be identified and then a filter for these patterns has to be designed and installed on the fly.

Types of filters will be used are:

A. Credential Filter: It check and evaluates credential details provided by the user at the login page and gives access to the legitimate users, denying the unauthorized user from accessing services.

B. Rate Attempt Filter: Sometimes attackers try to access the services by acquiring accounts of legitimate user, there are multiple tools available which lets attacker do this by guessing password automatically. Thus, to prevent such attacks, rate attempt filter has been designed which keeps a track on the count of wrong attempts and blocks the attacker for a specific count.

C. Size Limit Filter: Attacker may try to shut the server down by generating a load on server. This can be done by unnecessarily uploading heavy and large files on server. This situation needs to be avoided. For this, size limit filter has been designed, which keeps a limit on the files being uploaded even by the legitimate users. So the server runs smooth.

D. Load Limit Filter: Server may get overloaded because of some other reasons as well, for example: a large number of legitimate users accessing the services at the same time, may also led the server to shut down. This situation may account under DDoS attacks. So to prevent this, Load limit Filter is designed which allows only a specific number of users to access the services , at a time.

E. IP Filter: If some unusual activities are observed in the sending and receiving of packets, then that particular IP can be black listed. Black list is a list of IP addresses with a vague history.IP filter basically blocks all the IPs present in the black list and prevents them from accessing the services.

4. CONCLUSIONS

Detecting, preventing, and mitigating DDoS attacks is essential for national security. In the same manner that the Internet has become more user friendly in the past few years, and more individuals, businesses, and government agencies make use of it, so the hacking and disturbing network traffic has increased a lot. DDoS attacks are easy for attackers and script kiddies to obtain the authorised access and the potential for other attacks like the recent attack against the 13 root servers is quite high. Finding different ways for preventing and stopping DDoS attacks will be significant for national security. This mechanism can easily be implemented at small scale and DoS attack can be easily prevented. This Project focuses on prevention of DDOS Attacks with the help of various filters that work on application layer on the client as well as admin side web application. The filters are programmed in Java and the web services acts as an interface between client and admin. This system aims to ensure that no authorized user is ever denied access to the web server and an illegitimate user is blocked permanently.

REFERENCES

[1] Thomas Peltier, Justin Peltier, and John A. Blackley "Information Security Management Handbook,Fifth Edition"

[2] Cole, Eric. Hackers Beware. New Riders Publishing: Indiana, 2002.

[3] Harrison, Ann. "Denial of Service Aftermath." CNN. 14 Feb 2000. 10 Mar 2005.

http://archives.cnn.com/2000/TECH/computing/02/14/dos.aftermath.idg/

[4] Navratilova, Wiki. "A Brief History of Distributed Denial of Service Attacks." Uniform Chicago. 22 Aug 2000. 10 Mar 2005.

http://uniforum.chi.il.us/slides/DDoS/sld005.html

[5] Skoudis, Ed. Counter Hack A Step by Step Guide to Computer Attacks and Effective

Defenses. PrenticeHall: Canada, 2002.

[6] Lukas Ruf, Arno Wagner, K´aroly Farkas, Bernhard Plattner "A Detection and Filter System for UseAgainst LargescaleDDoS Attacks in the Internet Backbone"

http://www.hit.bme.hu/~farkask/publications/DDoSIWAN04.pdf

[7] J.Lemon, "Resisting SYN Flooding Dos Attacks with A SYN Cache", Proceeding of USENIX BSDCon'2002,February, 2002.

[8] Christos Douligeris and Aikaterini Mitrokotsa, "DDoS Attacks And Defence mechanisms: A Classification," in Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology, (ISSPIT'03), pp. 190-193, Dec 2003.

[9] C. K., and K. V. Viswanatha "Enhanced Ant Colony Based Algorithm for Routing in Mobile Ad Hoc Network" World Academy of Science, Engineering and Technology 46 2008.

[10] Yuji Waizumi , Tohru Sato and Yoshiaki Nemoto: A new Traffic Pattern Matchinng for DDoS trace back Using Independent Component Analysis in Procedding of World Academy of science ,Engineering and Technology 2009