V.Priyadharshini, Dr.K. Kuppusamy / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 3, May-Jun 2012, pp.2263-2267

Prevention of DDOS Attacks using New Cracking Algorithm

V.Priyadharshini[1] , Dr.K.Kuppusamy[2]
Dept of Computer Science & Engg
Alagappa University, Karaikudi,Tamilnadu,India

Abstract

In the modern computer world, maintaining the information is very difficult. Some interrupts may occur on the local system (attack) or network based systems (network attack) [4]. Without security measures and controls in place, our data might be subjected to an attack. Now a day's several attacks are evolved [4]. One common method of attack involves sending enormous amount of request to server or site and server will be unable to handle the requests and site will be offline for some days or some years depends upon the attack [1]. This is most critical attack for network called distributed denial of service attack [3]. In this paper a new cracking algorithm is implemented to stop that DDOS attacks. In our algorithmic design a practical DDOS defense system that can protect the availability of web services during severe DDOS attacks. The proposed system identifies whether the number of entries of client exceeds more than five times to the same sever, then the client will be saved as a attacker in blocked list and the service could not be provided. So our algorithm protects legitimate traffic from a huge volume of DDOS traffic when an attack occurs.

Keywords: *DDoS, Traffic, Attack, cracking algorithm.*

1. Introduction

Denial of Service (DOS) attacks are intended to shut down the servers for a period of time. To make site nonfunctional for a time, the main part of attack is DOS attack. DOS attacks are usually doing by following methods: 1. Send unlimited amount of packets to the server 2. Executing malwares 3.Teardrop attack 4.Application level flood [2]. In the existing system to stop the above problem to implement some protect a network against DDoS attacks. First limit the number of ICMP and SYN packets on router interfaces. Second Filter private IP addresses using router access control lists. Finally apply ingress and egress filtering on all edge routers.The proposed system gets affected by the denial of service because an intruder finds one or more systems on the Internet that can be compromised and exploited. This is generally accomplished using a stolen account on a system with a large number of users and/or inattentive administrators, preferably with a high-bandwidth connection to the Internet.

The compromised system is loaded with any number of hacking and cracking tools such as scanners, exploit tools, operating system detectors, root kits, and DoS/Distributed DoS(DDoS) programs [5]. This system becomes the DDoS master. The master software allows it to find a number of other systems that can themselves be compromised and exploited. The attacker scans large ranges of IP network address blocks to find systems running services known to have security vulnerabilities. This initial mass-intrusion phase employs automated tools to remotely compromise several hundred to several thousand hosts, and installs DDoS agents on those systems. The automated tools to perform this compromise is not part of the DDoS toolkit but is exchanged within groups of criminal hackers. These compromised systems are the initial victims of the DDoS attack. These subsequently exploited systems will be loaded with the DDoS daemons that carry out the actual attack.

The goal of this application is to maximize a system utility function. When a DDoS attack occurs, the proposed defense system ensures that, in a web transaction, which typically consists of hundreds or even thousands of packets from client to server, only the very first SYN packet may get delayed due to packet losses and transmissions. Once this packet gets through, all later packets will receive service that is close to normal level. This clearly will lead to significant performance improvement.

2. Related Work

S.Malathi and Dr.K.Kuppusamy have proposed DDoS attacks to prevent our files, the concept of file watcher, IP watcher and firewall are used. File watcher is responsible to monitor the file stored in the home directory and analyze the modifications made in the file. In addition, the IP address that modifies the file can be detected by IP watcher. When the client sends request to modify the file, the file watcher deny the service provided to the user and thus prevent the file from attack. The IP Address of the client who sends attack on the file is blocked by adding its address to the blocked list of the firewall. The clients whose IP Address are in the blocked list can't have permission to access the file further. Thus the file is prevented from the attacks. In this paper, a new method has been proposed to watch the activities taken in the file and to prevent the file from modifications by other users [1].

Vyas Sekar, Nick Duffield, Oliver Spatscheck, Kobus van der Merwe **and** Hui Zhang have proposed the design space for in-network DDoS detection and propose a triggered, multi-stage approach that addresses both scalability and accuracy. Our contribution is the design and implementation of LADS (Large-scale Automated DDoS detection System). The attractiveness of this system lies in the fact that it makes use of data that is readily available to

an ISP, namely, SNMP and Net flow feeds from routers, without dependence on proprietary Hardware solutions. We report our experiences using LADS to detect DDoS attacks in a tier-1 ISP [6].

3. Methodology

3.1. New Cracking Algorithm

Due to increase in number of users on internet, many people want to attack other system resources. Competitors also want to make their web site more popular than others. So they want to attack the service of other's web site. They keep on logon to a particular web site more times, and then service provided by the web server performance keeps degraded. To avoid that one, this application maintains a status table. In that it keeps the IP addresses of current users and their status. If the particular IP address has been signed on for a first time, it makes the status as genuine user. For 2, 3, 4 it marks as Normal user. For the fifth time it makes the particular IP address status as Attacker. In the time calculations we are only consider 5 times. User wish to server increase the time depends up on the application. After that, the user cannot allow get the service of that particular web site. The service is denied to that particular IP address.

3.2. Algorithmic steps

3.2.1 Packet Filter

Packet filters act by inspecting the "packets" which transfer between computers on the Internet. If a packet matches the packet filter's set of rules,
the packet filter will drop (silently discard) the packet, or reject it (discard it, and send "error responses" to the source). It is observed that a web transaction typically consists of hundreds or even thousands of packets sent from a client to a server. During a DDos attack, since the packets will be randomly dropped at high probability, each of these packets will go through a long delay due to TCP timeouts and retransmissions. Consequently, that total page download time in a transaction can take hours. Such service quality is of little or no use to clients. In contrast, our defense system ensures that, throughout a web transaction, only very first packet from a client may get delayed. All later packets will be protected and served. We show that this allow a decent percentage of legitimate clients to receive a reasonable level of service.

3.2.2 MAC Generator

MAC Generator distinguishes the packets that contain genuine source IP addresses from those that contain spoofed address. Once the very first TCP SYN packet of a client gets through, the proposed system immediately redirects the client to a pseudo-IP address (still belonging to the website) and port number pair, through a standard HTTP URL redirect message. Certain bits from this IP address and the port number pair will serve as the Message Authentication code (MAC) for the client's IP address.

MAC is a symmetric authentication scheme that allows a party A, which shares a secret key k with another party A, which shares a secret key k with another party B, to authenticate a message M sent to B with a signature MAC (M, k) has the property that, with overwhelming probability, no one can forge it without knowing the secret key k. Next we are verifying the secret key to prevent attackers who are using genuine address or spoofed address. Since a legitimate client uses its real IP address to communicate with the server, it will receive the HTTP redirect message (hence the MAC). So, all its future packets will have the correct MACs inside their destination IP addresses and thus be protected. The DDoS traffic with spoofed IP addresses, on the other hand, will be filtered because the attackers will not receive the MAC sent to them. So, this technique effectively separates legitimate traffic from DDoS traffic with spoofed IP addresses.

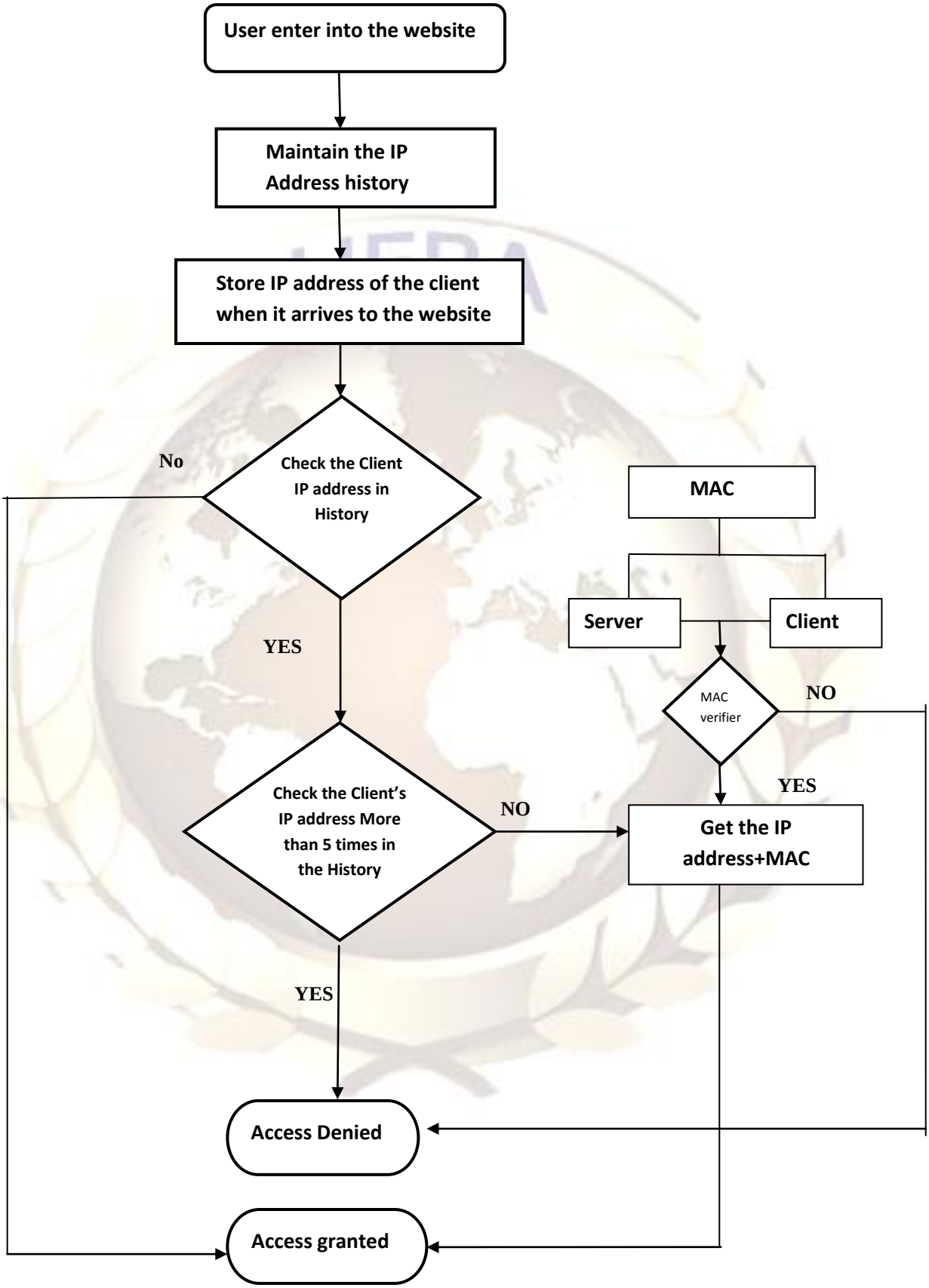
3.2.3 IP Handler

When an attackers using genuine address, the proxy server uses the Deficit Round Robin algorithm to collect the address of the client request. if an attacker sends packets much faster than its fair share, the scheduling policy will drop its excess traffic. More Over, for each genuine IP address, the system will perform accounting on the number of packets that reach the firewall but are dropped by the scheduler; its IP address will be blacklisted.

New Cracking algorithm

```
Start the Process
H=Maintain the IP address History;
U=User enter into the website;
I=Store the Each Client IP address;
Check each time U in server, If (I==H)
{
Else If(I<5)
{
IP=Get the IP address;
MAC 1=IP+MAC // Read Previous MAC Algorithm
Server=MAC1;
Client=MAC1;
If (Server=Client)
{
Accept the request from the client
Send the response for the request.
}
Else
{
Add the User.IP to the Attacker List,
Print : "Access Denied"
}
}
}
Else
{
Accept the request from the IP
Send the response for the request.
}
End
```

4. Implementation: New cracking algorithm basic functions as follows.



5. Results and Discussion

The experimental results of this paper are carried out by several attackers list and the website. The browser updates each time the history of the user and at the same time the information of the history are provided with the information such as Mac address, Time, and IP Address. Based on the IP Address, each time the user arrived at the website is analyzed. When the new user enters into the site continuously, the new cracking algorithm to determine whether the user is DDoS attacker. At the same time our experimental result obtains without any attacker or any DDoS prevention. In that situation what is sate of web server is calculated. And also when the attacker is allowed to access the website, the status of the web server also calculated. And also the attacker list is maintained and checked the user with the list. If the attacker is found, the access is denied by New cracking Algorithm. In this situation, the web server status also calculated. This is very useful for the users to determine the efficiency of our proposed algorithm named as New Cracking Algorithm**.** So in this algorithm to use the DDoS to prevent the server from accessing the server and interruption of the performance in server is distribute successfully in this system

6. Conclusion

In this paper we have proposed the Procedure made to tackle the continuous Problems occur in the internet services. In the proposed cracking algorithm for user friendly in domain and the capacity to store user profiles and profiles and sending them to the server component aided by computer speed high memory capacity and accuracy. This have the advantage of differentiating the clients from the attackers those who tries to affect the server function by posting requests in a large amount for unwanted reasons. This can be used for creating defenses for attacks require monitoring dynamic network activities. The basic idea behind the proposed system is to isolate and protect the web server from huge volumes of DDoS request when an attack occurs. In particular, we propose a DDoS defense system for protecting the web services. When a DDoS attack occurs, the proposed defense system ensures that, in a web related server information are managed without corruption. This newly designed system that effectively gives the availability of web services even during severe DDoS attacks. Our system is practical and easily deployable because it is transparent to both web servers and clients and is fully compatible with all existing network protocols.

7. References

[1] An effective prevention of attacks using giTime frequency algorithm under ddos by Dr.K.Kuppusamy,S.Malathi, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011.

[2] BARFORD, P., KLINE, J., PLONKA, D., AND RON, A. A Signal Analysis of Network Traffic Anomalies. In Proc. Of ACM/USENIX IMW (2002).

[3] BRUTLAG, J. D. Aberrant Behavior Detection in Time Series for Network Monitoring. In Proc. of USENIX LISA (2000).

[4]. Exploiting P2P Systems for DDoS Attacks by Naoum Naoumov and Keith Ross, Department of Computer and Information Science Polytechnic University, Brooklyn, NY 11201.

[5] Trends in Denial of Service Attack Technology CERT® Coordination Center Kevin J. Houle, CERT/CC George M. Weaver, CERT/CC In collaboration with: Neil Long Rob Thomas v1.0 - October 2001.

[6]. Large-scale Automated DDoS detection System by Vyas Sekar Carnegie Mellon University Nick Duffield AT&T Labs-Research Oliver Spatscheck AT&T Labs-Research-Annual Tech '06: 2006 USENIX Annual Technical Conference

[7] J. Li, J. Mirkovic, M. Wang, P. Reiher, and L. Zhang. SAVE: source address validity enforcement protocol. In INFOCOM, June 2002.

[8] Bremler-Barr and H. Levy. Spooling prevention method. In Proc. IEEE INFOCOM, Miami, FL, March 2005.

[9] K. Park and H. Lee. On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets. In Proc. ACM SIGCOMM, San Diego, CA, August2001.

[10] F. Baker. Requirements for IP version 4 routers. RFC 1812, June 1995.

[11] C. Jin, H. Wang, and K. Shin. Hop-count filtering: an effective defense against spoofed ddos traffic. In Proceedings of the 10th ACM conference on Computer and communications security,October 2003.

[12] Team Cymru. The team cymru bogon route server project. http: //www.cymru.com/BGP/bogonrs. html.

BIOGRAPHY

Ms. V.Priyadharshini

Ms.V.Priyadharshini is a Research scholar in the Department of Computer Science and Engineering, Alagappa University, Karaikudi, Tamilnadu, India. She has received her M.Sc in Information Technology from Annamalai University, Chidambaram, Tamilnadu in the year of 2011. She has presented her work in national level conferences. Her areas of research interests include Network information security, Networks.

Dr.K.Kuppusamy

Prof. Dr K.KUPPUSAMY is working as an Associate Professor in the Department of Computer Science and Engineering, Alagappa University, Karaikukdi, Tamilnadu He has received his Ph.D in Computer Science and Engineering from Alagappa University, Karaikudi, Tamilnadu in the year 2007. He has 22 years of teaching experience at PG level in the field of Computer Science. He has published many papers in International Journals and presented in the National and International conferences. His areas of research interests include Information/Network Security, Algorithms, Neural Networks, Fault Tolerant Computing, Software Engineering, Software Testing and Optimization Techniques.