IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

An Efficient mechanism to identify DDoS attacks by using Mark on Demand Server and Deterministic Packet Marking

A. Ravi[1], Karthik Shankar P S[2], J. N Sudhir[3], K. Karuna[4], Chandan Kumar[5]

Associate Professor, Computer Science & Engineering, Guru Nanak Institution Technical Campus, Hyderabad, India[1]

B.Tech Student, Computer Science & Engineering, Guru Nanak Institution Technical Campus, Hyderabad, India[2,3,4,5]

Abstract: In the present age of technology where the Internet is the foremost necessity, the able working of Internet is the key concern. The main disadvantage faced on the Internet is the security of the data and other security constraints. One of the most known threats is Dynamic Denial of Service (DDoS) where the server is burdened with data which causes it to not respond to other user's requests. This key issue is tackled till present day with the help of various techniques, one of the most prominent among being the Packet Marking. Deterministic Parking Marking (DPM) is the method which is used to mark the packets which are transmitted through the Internet. DPM, when used along with the Mark on Demand Servers, increases the possibility of easy and efficient detection of the DDoS attacks faced on the servers. We discuss the methods using .NET framework to identify the traffic sources and identify the physical address of the attacker for prevention and safety.

Keywords: DDoS attack, Denial of Service, Detectors, Deterministic Packet Marking, DPM, IP header marking, Mark on Demand, Packet Marking.

I. INTRODUCTION

Dynamic Denial of Service (DDoS) [7],[8] attacks are one of the key issues faced in huge distributed systems across the internet. DDoS is a type of DOS attack where multiple compromised systems, which are often infected with a trojan, are used to target a single system causing a Denial of Service (DoS) attack. The DDoS attack uses multiple computers and Internet connections to flood the targeted resource. DDoS attacks are often global attacks, distributed via botnets. Victims of a DDoS attack consist of both the end targeted system and all systems maliciously used and controlled by the hacker in the distributed attack.

IP traceback is the method which is used to triangulate the exact physical location of the attacker causing the DDoS attacks. Traceback involves method using which the IP address of the malicious attacker is brought into notice using which the perpetrator identified. The most common IP traceback method involves packet marking which, where the packets sent or received from the servers are marked for future reference to identify the attacker and their physical system. The packet marking methods uses a specific kind of method to identify suspicious IP addresses which may soon be a threat.

In the method of Probabilistic Packet Marking, which is one of the methods of packet marking, the markers are placed on generally all the packets which are being transmitted through the network by the server or through the server. The strings used are called as tags. These tags are used to determine the packet physical location.

In this paper, we discuss the method which overcomes the Probabilistic Packet Marking, that is Deterministic Packet Marking with the aid of one of a kind of servers called as Mark on Demand(MOD) Servers. This server works along with 3 detectors which when notified about the huge traffic of packets being sent or received, transmits these packets to the detectors which will check the request's source. If the requests are sent from the same source the detectors request the MOD server for marking these packets. All these methods will be clearly explained in the paper in a very justifiable and understandable format.

The rest of the paper is organized as below, Section II holds all the existing methods already in use. The procedures and the drawbacks of the methods in current will be discussed. In Section III the proposed method will be spoken about and explained, followed by Section IV which presents the System Architecture. Finally, Section V presents Results and Section VI presents the Conclusion.

II. EXISTING SYSTEM

A. Probabilistic Packet Marking

Probabilistic Packet Marking [1], [5] is the most initial method used for packet marking. In the method of PPM, the markers are placed on generally all the packets which are being transmitted through the network by the server or through the server. In PPM, there are two different procedures followed, Fragment Marking [1] and Hash-based Advanced Marking scheme [1].

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

In the method of Fragment Marking [1], a threshold value is fixed by the server called Pm, whenever a packet passes through a router a random number is assigned to the packet which is then compared with the pre-fixed threshold value which helps it decide if the packet is to be marked or not. But the method has a major flaw when it comes to a huge number of systems are used by the attacker. The computational overhead used to reconstruct the attacker's path was very high [1]. When the attacker used many different systems for the attack the rate of finding the original source had a more false positive.

Song and Perrig [1] advocated a new method of PPM where the hash-based techniques were to be used for marking the packets in the network. This method was named as the Advanced Marking Scheme(AMS) [1]. This system overcame all the drawbacks of the FMS [1]. It used a hash-based method where the hash value of the IP address is used for marking the packets rather than using the IP address itself. Compared to the FMS, it has a low computational overhead and low false positive.

Considering the overall method of PPM, the main drawbacks [9] associated with this method is that the process of marking each and every packet of the system becomes a very challenging and hard task to keep up with. All the marked packets are difficult to be checked every time, as in real-time environment the ability of the maintenance and supervising these many marked packets is not viable.

III.PROPOSED SYSTEM

A. Deterministic Packet Marking

Deterministic Packet Marking(DPM) is the key method used to overcome this flaw. In DPM [6], [9], the method uses the unfilled bits of the IPv4 head to identify the source of the packets [2]. The method of DPM is very simple, scalable and the inherent security is intact without any flaws. The only problem with DPM is when the maximum number of systems to be checked affects the whole procedure of finding the original attack source. The burden of so many packets throughout the system makes it quite hard for it to check and identify the perpetrator.

To overthrow this disadvantage of DPM, a new method [4] is proposed where the DPM is used along with a MOD (Mark on Demand) server. The working of these MOD servers depends on Traffic Detectors installed to monitor the data traffic and detectors installed in the servers, which are used to mark the packets. It conquers the main flaw faced by DPM by allowing the ability to easily check multiple systems. The method also enables the ability to conduct a global search and easily pinpoints the single source of the attack than isolating every possible router and terminal combinations. This system provides a more understandable traceback mechanism to isolate the attacker from the normal clients without giving the attacker a chance to mask or retaliate.

In this method [4], there are four different sections which perform separate operations which in total help to provide the marking of packets effective.

1) **Client:** The client refers to any terminal which requests for information to be accessed from the server. The client can connect to the internal network of the server only after authentication. Only after which, they are to request for any file or any information. The client sends a request for any specific action to take place.
2) **Traffic Routers:** The traffic routers are the through points which facilitate the data transfers in the network. Along with this function of theirs, an additional subprogram runs which help it to monitor the flow of the data through it. When the packets marked by the MOD server goes through the routers, they make sure to trace the path and report back to the MOD server, to reconstruct the attack route and trace the IP address of the attacker.
3) **Detectors:** The Traffic Routers request the detectors to process the packets which are being pulled out in the huge quantity. The detectors carry a huge set of functions [4]. The whole detection process uses 3 detectors.
   a) The first detector stands for checking the origin of the requests. Each terminal has got its own session code, so if at all multiple requests are made from one, the detector filters these aside. There may be more than one terminal which has demanded multiple packets. The packets are sent in the same sorted manner to the next detector.
   b) The second detector checks for the marked packets and rechecks the origin of the requests. It segregates according to individual terminal session ID. The marked packets which are suspicious are sent to the MOD server [4]. The unmarked packets are forwarded to the next detector. This is where the threat is initially being noted.
   c) The third detector is the one which confirms that it is a threat. It takes in the marked packets which are outputted from the MOD server after marking their IP header for identifying their physical address. The third detector then combines these both set of packets and only processes the unmarked packets which are not any threat to the system.
4) **MOD Server:** The MOD Server is also part of the detection, the packets which are suspicious are sent from the second detector to the MOD Server which checks for the IP address of the packets which are marked with the help of the packet marking algorithm. The packets which are marked by the MOD stand as a bait for finding out the physical location of the attacker. It helps to trace out multiple locations at the same time due to the marking is done by the method in the IP header. These unique mark helps the routers to know the exact location of these packets.

The MOD server uses the method of packet marking in the IP header as shown in Fig 1. The packet marking method

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

was first stated by Y. Gong [2] as a hybrid marking method. The mark is stamped on packets through overloading the 16-bit identification field in IP header. The leftmost bit is a flag termed logging flag bit. It is set to 1 if the current router commits logging operation on the packet, otherwise set to 0. The remaining 15 bits is used to represent router identification. Using this packet marking method in the MOD Server, the packets are a market for the supervision of the packets through the network with the help of the Traffic monitor routers, tracing them back to the IP address of the attacker trying for a DDoS attack on the server. Compared to the usual DPM methods where only a section of the IP header was marked, MOD method uses the whole header for the marking purpose to increase the traceability of the packets whose header is marked.

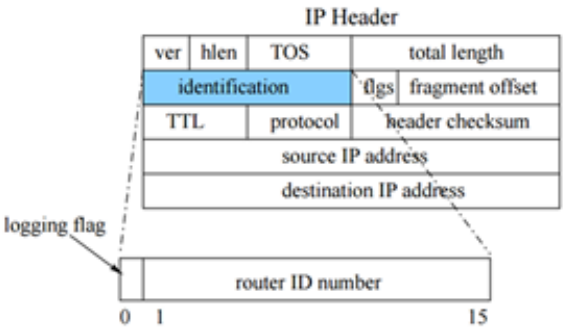

Fig. 1 The Packet Marking in the IP header.

IV. SYSTEM ARCHITECTURE

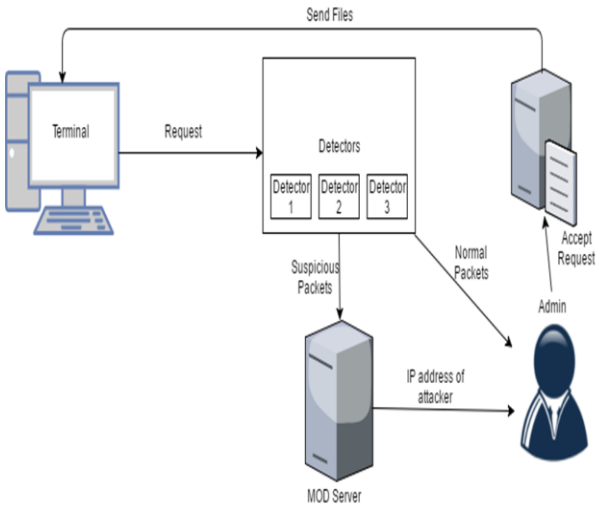

Fig. 2. System Architecture of the MOD-DPM system

The System Architecture of the MOD-DPM system consists of the 4 modules as stated earlier.

1) Terminal: It is the usual user end communication device which is used by the users to connect to the network and thus access the functions.
2) Detectors: The array of the 3 detectors which are used to detect the suspicious inflow of packets through the network.
3) MOD Server: The MOD server which marks the unmarked packet to trace the physical address of the user sending the spoof packets.
4) Admin: The main supervisor looking over the whole file request acceptance and security issues.

V. RESULTS

The DPM method proposed helps in the triangulation of the physical IP address of the attacker, who uses a huge surge of data to burden the server. The MOD server uses the principle of constant data governance through the traffic router and when the packets are found suspicious calls them using the detectors and mark the packets. The marked packets help to bring out their physical address. Each time an anomaly is reported about in the packet flow, the detectors report it to the MOD server which marks the packet and through the Traffic routers, they monitor these packets. The packets are checked due to which the exact IP address of the attacker is being traced. We use .NET framework to execute the above method to show the working of the system.

B. User Login

Fig. 3 User login Screen for authentication

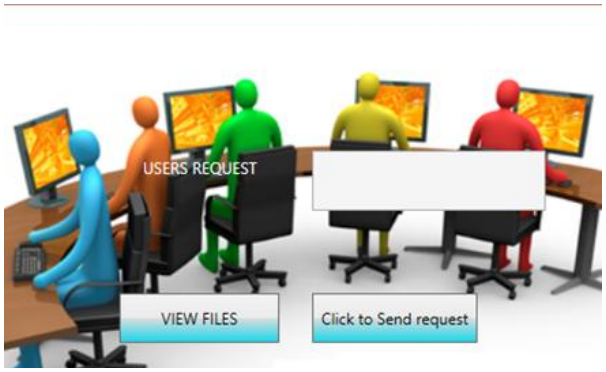

Fig. 4. The File Request for Users

C. Detectors and MOD Server

These are the combination of the detectors which identify the single source of the packets and the MOD server which puts a unique mark on these packets for being identified by the routers which will track the attack route back to the origin of the DDoS attack if it is confirmed.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 3, March 2017

Fig. 5 Detector 1 forwarding packets to Detector 2

1) When an anomaly is detected:

Fig. 6(a) Detector 2 detects suspicious entry

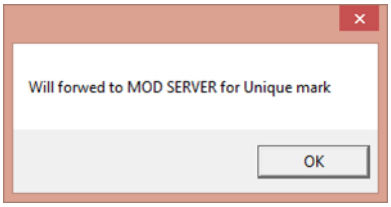

Fig. 6(b) Forwarding it to MOD Server for Mark

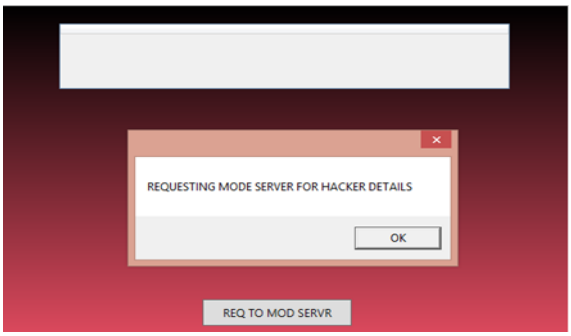

Fig. 6(c) Detector 3 requesting Server for Hacker's details

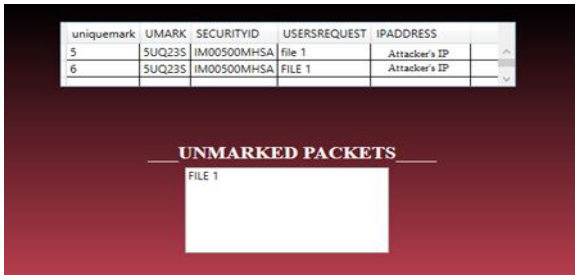

Fig. 6(d) MOD Server Displaying the Attacker's IP

2) When an anomaly is not detected**:**

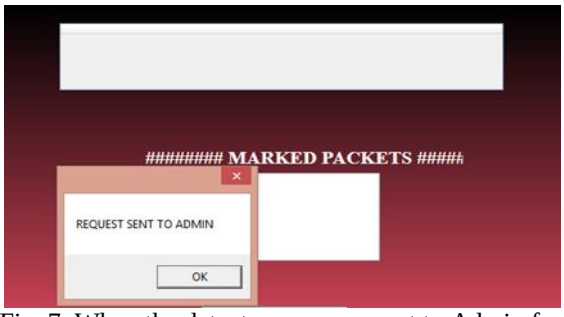

Fig. 7. When the detectors pass request to Admin for request response.

VI. CONCLUSION

The Dynamic approach of DPM along with the functionality of the MOD server enhances the backdrops faced by the PPM method, where all the packets are marked. It overcomes the DPM method wherein the packet marking scheme used could be a flaw in the case of multiple terminals being used for causing the DDoS attacks. The MOD Server method along with the principle function of DPM, the overall chances of prevention of the DDoS increases manifold. The method of using detectors to identify the similarly sourced requests provide a high ground for the administrator to monitor and prevent the attacks. The usage of the traffic router monitors which govern the flow of the packets throughout the network helps to bring out a lead in the case of the identifying spoofing packets which in-turn cause the DOS attacks on the server.

REFERENCES

[1] Liming Lu, Mun Choon Chan, Ee-Chien Chang, "A General Model of Probabilistic Packet Marking for IP Traceback", ASIACCS '08, March 18-20, Tokyo, Japan.

[2] Chao Gong, Kamil Sarac, "IP Traceback based on Packet Marking and Logging", IEEE International Conference on Communication (ICC), May 16-20, 2005., Seoul, Korea.

[3] Turgay Korkmaz, Chao Gong, Kamil Sarac, Sandra G. Dykes, "Single packet IP traceback in AS-level partial deployment scenario", Int. J. Security and Networks, Vol. 2, Nos. 1/2, 2007

[4] Shui Yu, Wanlei Zhou, Song Guo, Minyi Guo, "A Feasible IP Traceback Framework through Dynamic Deterministic Packet Marking", DOI 10.1109/TC.2015.2439287, IEEE Transactions on Computers

[5] T. K. T. Law, J. C. S. Lui, and D. K. Y. Yau, "You can run, but you can't hide: An effective statistical methodology to trace back DDoS attackers," IEEE Transactions on Parallel and Distributed Systems, vol. 16, no. 9, pp. 799–813, 2005.

[6] S. Yu, W. Zhou, S. Guo, and M. Guo, "A dynamical deterministic packet marking scheme for DDoS traceback," in IEEE International Conference on Global Communication, 2013.

[7] Darshan Lal Meena, Dr. R. S. Jadon, "Distributed Denial of Service Attacks and Their Suggested Defense Remedial Approaches ", Volume 2, Issue 4, April 2014

[8] Akash Mittal, Prof. Ajit Kumar Shrivastava, Dr. Manish Manoria, "A Review of DDOS Attack and its Countermeasures in TCP-Based Networks", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.2, No.4, November 2011

[9] Andrey Belenky, Nirwan Ansari, "IP Traceback With Deterministic Packet Marking", IEEE COMMUNICATIONS LETTERS, VOL. 7, NO. 4, APRIL 2003