2009 International Conference on Advances in Recent Technologies in Communication and Computing

Detecting and Preventing IP-spoofed DDoS Attacks by Encrypted Marking based Detection And Filtering (EMDAF)

M.Nagaratna
Asst. Professor &
Coordinator of Examination.
JNTU Hyderabad
mratnajntu@gmail.com

Dr. V.Kamakshi Prasad
Professor & Additional
Controller of Examinations
JNTU Hyderabad

S.Tanuz Kumar
Dept of CSE, JNTUCEH
s.tanuzkumar@gmail.com

Jawaharlal Nehru Technological University, Computer Science Dept., Kukatpally, Hyderabad, Andhra Pradesh, India.

***Abstract*—Distributed Denial of Service (DDoS) attacks are the major threat to the current internet world. Source IP Address spoofing in one of the approach to perform Distributed Denial of Service (DDoS) attacks. In this scenario the packet true origin is difficult to identify. Thus the defense against the Distributed Denial of Service (DDoS) attack is very complex to handle. We propose a novel scheme which is based on a firewall. This firewall can distinguish the attack packets from the packets sent by legitimate users based on the marking value on the packet, and thus filter out most of the attack packets. Compared to other packet-marking based solutions, our scheme is very effective and has a very low deployment cost. In the implementation of this scheme we would require the cooperation of only about 10% of the Internet routers in the marking process, and server to generate encrypted marking for secured transmission. The scheme allows the firewall to Detected and prevents the DDoS attacks from the first packet itself.**

***Key words*—Distributed denial-of-service attacks, firewall, IP address spoofing, packet filtering and encryption.**

1. Introduction

In today world, the Internet is an essential part of our everyday life. Many important and crucial services like banking, shopping, transport, health, and communication are partly or completely dependent on the Internet. According to recent sources [4] the number of hosts connected to the internet is almost 400 million and there are currently more than 1 billion users of the Internet. Thus, any disruption in the operation of the Internet can be very inconvenient for most of us. The Internet was originally designed for openness and scalability without much concern for security, malicious users can exploit the design weaknesses of the internet to wreak havoc in its operation. The incidents of DDoS attacks are on rise, the attacker's sole purpose is to reduce or eliminate the availability of a service provided over the Internet, to its legitimate users. This is achieved either by exploiting the vulnerabilities in the software, network protocols, or operation systems, or by exhausting the consumable resources such as the bandwidth, computational time and memory of the victim. The first kind of attacks can be avoided by patching-up vulnerable software and updating the host systems from time to time. In comparison, the second kind of DoS attacks is much more difficult to defend. This works by sending a large number of packets to the target, so that some critical resources of the victim are exhausted.

1.1 The different types of attack [5]:

ICMP attack- In this DDoS attack, the attacker flood large amount of ICMP_ECHOREQUEST packets in the network using target host IP Address, if the attacker does not forge the IP address then he will be affected because he will receive all the reply for the request sent. Since the IP address was forged now the target host will be affected.

SYN-ACK attack- **N**ormal TCP connection follows "three way handshake" i.e. destination receives a SYN packet from a source and sends back a SYN ACK. The destination must then hear an ACK of the SYNACK before the connection is established. While waiting for the ACK to the SYN ACK, a connection queue of finite size on the destination keeps track of connections waiting to be completed. By generating phony TCP SYN packets from random IP addresses at a rapid rate, it is possible to fill up the connection queue and deny TCP services such as email, file transfer, or WWW to legitimate users.

2. Approaches for Defending

Defenses for Distributed Denial of Service attack can be classified into three categories: preventive mechanisms, reactive mechanisms, and source-tracking mechanisms.

2.1 Preventive Defense

The preventive schemes aim at improving the security level of a computer system or network; thus preventing the attacks from happening, or enhancing the resistance to attacks. A proactive server roaming scheme belongs to this category. This system is composed of several distributed homogeneous servers and the location of active server changes among them using a secure roaming algorithm. Only the legitimate users will know the server's roaming time and the address of new server. All connections are dropped when the server roams, so that the legitimate users can get services at least in the beginning of each roaming epoch before the attacker finds the active server out again. Such solutions are generally costly and difficult to really prevent attacks.

978-0-7695-3845-7/09 $26.00 © 2009 IEEE
DOI 10.1109/ARTCom.2009.167

2.2 Source Tracking

The source-tracking schemes, on the other hand, aim to track-down the sources of attacks, so that punitive action can be taken against attacks. The existing solutions fall into four groups: packet marking, message traceback, logging, and traffic observation. Many different packet marking schemes have been proposed, for encoding path information inside IP packets, as they are routed through the internet. Probabilistic packet marking (PPM), in which the routers insert path information into the Identification field of IP header in each packet with certain probability, such that the victim can reconstruct the attack path using these markings and thus track down the sources of offending packets. Dean et al. [3] mention an algebraic approach based on reconstructing polynomial functions to track packets. Belenky and nsari [1] propose a deterministic marking approach (DPM), in which only the address of the first ingress interface a packet enters instead of the full path the packet passes (as used in PPM) is encoded into the packet. In the message traceback method [5], routers generate ICMP traceback messages for some of received packets and send with them. By combining the ICMP packets with their TTL differences, the attack path can be determined. Some factors are considered to evaluate the value of an ICMP message, such as how far is the router to the destination, how quick the packet is received after the beginning of attack, and whether the destination wishes to receive it. A common problem existing in these four solutions is that the reconstruction of attack path becomes quite complex and expensive when there are a large number of attackers (i.e. for highly distributed DoS attacks). Also, these types of solutions are designed to take corrective action after an attack has happened and cannot be used to stop an ongoing DDoS attack.

2.3 Reactive Solutions

The reactive measures for DDoS defense are designed to detect an ongoing attack and react to it by controlling the flow of attack packets to mitigate the effects of the attack. One of the proposed reactive schemes, given by Yaar et al. [2] uses the idea of packet marking for filtering out the attack packets instead of trying to find the source of such packets. This scheme uses a path identifier (called Pi) to mark the packets; the identification field in the packet is separated into several sections and each router inserts its marking to one of these. Once the victim has known the marking correponding to attack packets, it can filter out all such packets coming through the same path. The Pushback [6] method generates an attack signature after detecting congestion, and applies a rate limit on corresponding incoming traffic. This information is then propagated to upstream routers, and the routers help to drop such packets, so that the attack flow can be pushed back. In the Neighbor Stranger Discrimination (NSD) [7] approach, the network is divided into neighbors and strangers. If packet is from neighbor then NSD will accept the packet else it will reject. The success of the reactive schemes depends on a precise differentiation between good and attack packets.

3. PROPOSED CONTRIBUTION

With the help of encryption mechanism we can enhance the speed of detection and prevention of IP spoofed packed. The new scheme is Encrypted Marking based Detection And Filtering (EMDAF)

3.1 Proposed EMDAF system

EMDAF scheme has the following functions:

- Server receives packets from client which contain source IP address and marking value.
- Server send echo message to source IP address to verify the marking value.
- If both marking values are same, then server will generate a key. Else the packet is attacked packet. So, the server will discard the request.
- Now using the encryption mechanism the server will encrypt the generated key.
- Form now onwards in further communication the encrypted marking will be used for secure transmission.

3.1.1 The marking scheme

The complete marking scheme is shown in and the pseudo code is described below:

```
Marking procedure at router R (having IP address A):
k <- a 16-bit random number
M(R) <- k XOR h(A)
For each packet w
{ If W.ID = 0 Then
w.ID <- M(R)
Else
{ M_old <- w.ID
M_new <- M(R) XOR CSL(M_old)
w.ID <- M_new
}}
```

3.1.2 Generating Encrypted Marking

After verifying both the marking values, if they are same then the firewall will generate a random key. Then this random key will be encrypted using existing encryption mechanisms like Symmetric Cryptography like DES, AES or Asymmetric Cryptography like RSA, ECC etc. Then server will send the encrypted marking to the client. From now onwards both client and server will communicate with each other using the encrypted marking. Since the marking remains same through out the session, even if path changes it will not affect the system. In this proposal we will use Elliptical Curve Cryptography

because communication using this mechanism is more efficient and secured as compared to other mechanisms like.

- High cryptography strength relative to key size (150-250 bits).
- The smaller key size also makes possible much more compact implementations for a given level of security, which means faster cryptographic operations, running on smaller chips or more compact software.
- The one way function of ECC is very strong. i.e. 'Forward' operation which must be tractable and an 'inverse' operation which must be in practical terms intractable.
- One way function can be replaced by system based on elliptical curve.

3.1.3 Filtering Scheme

The EMDAF scheme employs a firewall at each of the perimeter routers of the network. This firewall scans the marking field of all incoming packets to selectively filter-out the attack packets. When a packet arrives at its destination, its marking depends only on the path it has traversed. If the source IP address of a packet is spoofed, this packet must have a marking that is different from that of a genuine packet coming from the same address. The spoofed packets can thus be easily identified and dropped by the filter, while the legitimate packets containing the correct markings are accepted and the packet IP address and its encrypted marking is updated in the filter table. Now in the further secure transactions the encrypted marking is verified. If the marking received by server for an existing IP address in the filter table is same then it will be accepted else it will be dropped

4. Conclusions

In this paper we have proposed a low-cost and efficient scheme called EMDAF, for defending against IP spoofed attacks, The EMDAF scheme is composed of three parts: marking process, filtering process, secure transmission. The marking process requires the participation of routers in the Internet to encode path information into packets. We suggest the use of a hash function and secret key to reduce collisions among packet markings. The time required to mark the each packet is saved because in this scheme once a secure transmission is established between source and destination then there is no requirement of marking and comparing process at participant routers and firewall router respectively. So we can say that following benefits can be achieved by proposed scheme.

- High speed filtering of spoofed packet.
- Enhancement in packet transmission.
- Once secure transmission is established no role of participating router in filtering process.
- After secured transmission even if path changes no remarking is required.
- There is no requirement to generate unnecessary echo messages to update filter table.
- From the beginning of creation of filter table all attack packets will be detected and dropped.

This scheme can be performs well even under massively IP spoofed attacks. In future work we can implement this mechanism for networks which does not require any infrastructure for communication like Mobile Ad-hoc NETworkS (MANETS)

References

[1] A. Belenky and N.Ansari, “IP traceback with deterministic packet marking” IEEE Communications Letters, vol. 7, no. 4, pp. 162-164, Apr. 2003.

[2] A. Yaar, A. Perrig, and D. Song, “Pi: A path identification mechanism to defend against DDoS attacks” in Proceedings of the IEEE Symposium on Security and Privacy, pp. 93-109, May 2003.

[3] D. Dean, M. Franklin, and A. Stubblefield, “An algebraic approach to IP trackback” in Proceedings of the 2001 Network and Distributed System Security Symposioum, pp.3-12, Feb. 2001.

[4] Internet World Stats, Internet User Statistics – The Big Picture: World Internet Users and Population Stats, http://www.internetworldstats.com/stats.htm

[5] S. Bellovin, “ICMP Traceback Messages, Internet draft”, work in progress, Mar. 2000.

[6] J. Ioannidis and S. M. Bellovin, “Implementing push-back: router-based defense against DDoS attacks” in Proceedings of the Network and Distributed System Security Symposium (NDSS’02), pp. 6-8, Feb.2002.

[7] N. Aaaraj, S. Itani, and D. Abdelahad, “Neighbor stranger discrimination (NSD)- A new defense mechanism against DDoS attacks,” in Proceedings of the 3rd FEA Student Conference, May 2004.