

Detecting and Preventing IP Spoofed Attack by Cryptography

Mr. Gopal Bhati, Mr. Ashish Kr. Chakraverti, Mr. Dhanna Ram
St. Margret Engineering College Neemrana Alwar Rajasthan

Abstract - In this paper We explore a mechanisms for defending against ip spoofed packet attacks, have become one of the major threats to the operation of the Internet today. I propose a novel scheme for detecting and preventing the most harmful and difficult to detect DDoS Attacks—those that use IP address spoofing to disguise the attack flow. Our scheme is based on a firewall that can distinguish the attack packets (containing spoofed source addresses) from the packets sent by legitimate users, and thus filters out most of the attack packets before they reach the victim. Unlike the other packet marking based solutions, our scheme has a very low deployment cost; It can be estimated that an implementation of this scheme would require the cooperation of only about 20% of the Internet routers in the marking process. The scheme allows the firewall system to configure itself based on the normal traffic of a Web server, so that the occurrence of an attack can be quickly and precisely detected.

Keywords:- Distributed denial-of-service attacks, firewall, IP address spoofing, packet filtering.

I. INTRODUCTION

Today, the Internet is an essential part of our everyday life and many important and crucial services like banking, shopping, transport, health, and communication are partly or completely dependent on the Internet. According to recent sources the number of hosts connected to the internet has increased to 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 As 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. Incidents of disruptive activities like e-mail viruses, computer worms and denial-of service attacks have been on the rise reports an increase of such incidents from 252 in 1990 to 137,529 in 2003). The incidents which has raised the most concern in recent years are the denial-of-service(DoS) attacks whose 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 are 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 and the victim can no longer communicate with other users. For second type of attack ip spoofing is most popular tool.Packets sent using the IP protocol include the IP address of the sending host. The recipient directs replies to the sender using this source address. However, the correctness of this address is not verified by the protocol. The IP protocol specifies no method for validating the authenticity of the packet's source. This implies that an attacker could forge the source address to be any he desires. This is a well-known problem and has been well described In all but a few rare cases, sending spoofed packets is done for illegitimate purposes.

Figure 1: Valid source IP address, illustrates a typical interaction between a workstation with a valid source IP address requesting web pages and the web server executing the requests. When the workstation requests a page from the web server the request contains both the workstation's IP address (i.e. source IP address 192.168.0.5) and the address of the web server executing the request (i.e. destination IP address 10.0.0.23). The web server returns the web page using the source IP address specified in the request as the destination IP address, 192.168.0.5 and its own IP address as the source IP address, 10.0.0.23.

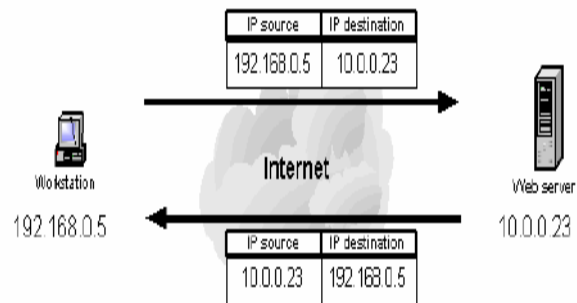


Figure 1: Valid source IP address

Figure 2: Spoofed source IP address, illustrates the interaction between a workstation requesting web pages using a spoofed source IP address and the web server executing the requests. If a spoofed source IP address (i.e. 172.16.0.6) is used by the workstation, the web server executing the web page request will attempt to execute the request by sending information to the IP address of what it believes to be the originating system (i.e. the workstation at 172.16.0.6). The system at the spoofed IP address will receive unsolicited connection attempts from the web server that it will simply discard.

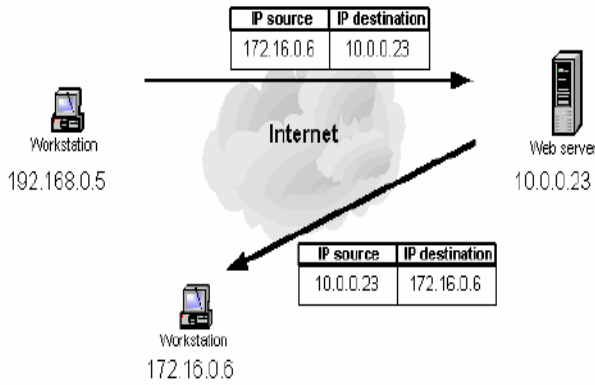


Figure 2: Spoofed source IP address

Sending IP packets with forged source addresses is known as *packet spoofing* and is used by attackers for several purposes. These include obscuring the true source of the attack, implicating another site as the attack origin, pretending to be a trusted host, hijacking or intercepting network traffic, or causing replies to target another system. In this paper, we present and analyze a Marking-based Detection and Filtering (MDADF) scheme to defend massively distributed DoS attacks.

II. EXISTING APPROACHES FOR DETECTING AND PREVENTING IP SPOOFED ATTACKS

Recent scheme for this purpose are based on packet marking scheme some popular schemes are as follows. For marking purpose ID field is used. The 16-bit Identification field in IP header has been commonly employed as the marking space). The Identification (ID) field is currently used to indicate IP fragments belonging to different packets, but only less than 0.25% of the packets on the Internet actually use this feature. Therefore, employment of ID-field as the marking space will not much affect the normal transmission of IP packets.

2.1 Stack Pi: New Packet Marking and Filtering:-

Fig. 3. The basic Stack Marking Scheme. This figure shows how the Pi mark evolves as the packet traverses routers R1 through R9. Initially, the marking field contains arbitrary data. In this example, each router marks with $n = 2$ bits and the field has space for four router markings.

Fig. 4. The stack marking scheme with write-ahead. The new scheme allows the inclusion of markings from router R3, despite the fact that it is a legacy router. Each router along the path first (a) checks the topmost marking in the stack to see if it equals the marking that would have been generated by the

Fig-3

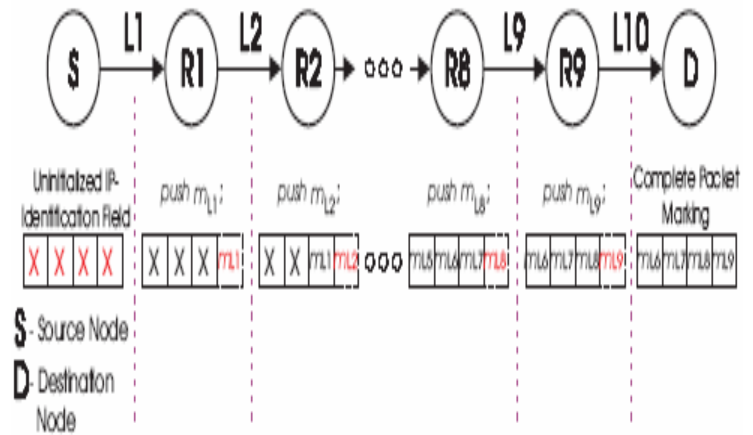
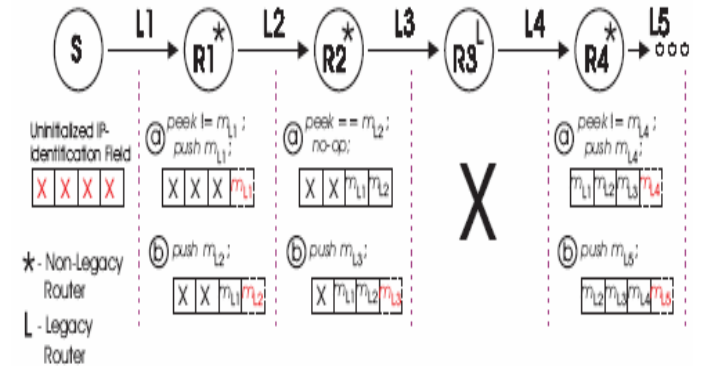


Fig-4



router connected to the current router's incoming link, and if the topmost marking is not equal to that, the router adds that marking to the packet; and then (b) adds the marking for the incoming link of the next-hop router to the stack.

Draw backs of stack pi is given as bellows

- ID field of IP packet used as stack and overwritten after over flow.
- No of router and No of packet required to detect and prevent spoofing is more.
- Slow speed.

A. *Marking-based Detection and Filtering (MDADF):-*

Though source IP addresses can be spoofed by attackers, the paths packets take to the destination are totally decided by the network topology and routers in the Internet, which are not controllable by the attackers. Therefore, the path of a packet has taken can really show the source of it. By recording the path information, the packets from different sources can be precisely differentiated, no matter what the IP addresses appeared in the packets. Packet marking, which is firstly proposed by Savage et al. in the PPM scheme, is a good method to record path information into packets. To indicate the path a packet traverses, the simplest way is to add all the routers' IP addresses into the packet. The number of hops a packet passes through in the Internet is about 15 on average and mostly less than 31. Since the length of a path is uncertain,

it is difficult to reserve enough space in the packet to put all the addresses, and the packet size increases as the length of the path increases. In order to avoid the increase in packet size, a possible method is to put all information into a fixed space. A router puts its IP address into the marking space of each packet it receives; if there is already a number in that space, it calculates the exclusive-or (XOR) of its address with the previous value in the marking space and puts the new value back. This method ensures that the marking does not change its length when a packet travels over the Internet, so the packet size remains constant.

MDADF scheme has the following functions:

- Distinguish and filter out spoofed packets by checking the marking of each packet using the Filter Table.
- Detect the occurrence of DDoS attack, so that appropriate defensive measures can be taken before serious damage is caused.
- Ensure that not many legitimate packets are dropped mistakenly, due to route changes on the Internet.

Marking scheme:-

To make the marking scheme more effective, we let each router perform a Cyclic Shift Left (CSL) operation on the old marking Mold and compute the new marking as $M = CSL(Mold) \oplus MR$. In this way, the order of routers influences the final marking on a packet received by the firewall.

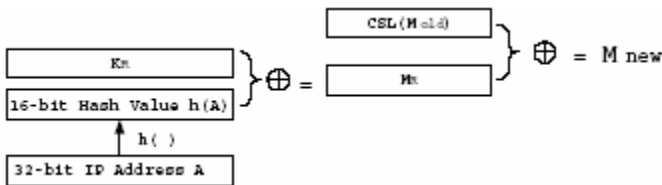


Figure 5: The marking scheme

The complete marking scheme is shown in Figure 5 and the pseudo code is described below:

Marking procedure at router R (having IP address A):

$k \leftarrow$ a 16-bit random number

$M(R) \leftarrow k \text{ XOR } h(A)$

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
  }
}

```

Filtering Scheme

The MDADF scheme employs a firewall at each of the perimeter routers of the network to be protected and the firewall scans the marking field of all incoming packets to selectively filter-out the attack packets (see Figure 6).

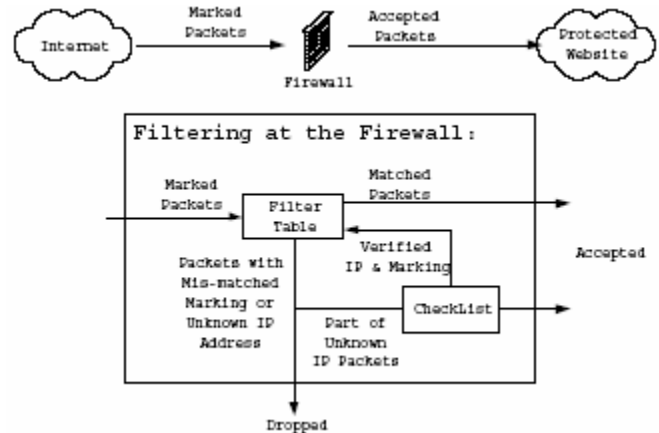


Figure 6: The system structure

On employing this marking scheme, 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.

Filtering scheme has following steps:

- Learning Phase
- Normal Filtering Procedure
- Marking Verification
- Attack Detection
- Route Change Consideration

Draw back of this scheme:-

1. At each participant router It is required to mark all the packets and at each step due to this more time is required to detection and prevention.
2. Marking scheme is changed for same source packet when route is changed.

III. PROPOSED CONTRIBUTION

With the help of cryptosystem we can enhance the speed of detection and prevention of IP spoofed packet. The new scheme is CRYPTOGRAPHY AND MARKING BASED DETECTION AND FILTERING SYSTEM (CMDADF)

Which can be implemented as bellow.

Existing MDADF system

- a. If unidentified marked packet is found at destination then marking is done and filter table is updated if it is not possible then packet is filtered out.

- b. If marked packet is found then accepted.
- c. Marking is done for each packet at participants routers.

Proposed CMDADF system

Rather than doing the marking for each packet after confirmation of source validity, if further packet transmission is required put it in secure transmission with cryptosystem. It would be more reliable that Source address of IP packet should be Encrypted.

IV. RESEARCH METHODOLOGY

For this any existing cryptosystem can be taken. For e.g. RSA cryptosystem..

RSA cryptosystem:-

The RSA cryptosystem was invented in 1977 by Rivest, Shamir and adleman and was the first realization of Diffie-Hellman’s abstract model for public key cryptography.

To set up this system each user picks two large primes p and q and computes Their product $n=pq$. The group used is $G=Z_n^*$. It is well Known that the order of G is

$$\Phi(n)=p-1)(q-1).$$

The public key is the pair of integer (n,e) and the private key is d . The problem of computing $\Phi(n)$ using only n is computationally equivalent to the problem of factoring n , which is believed to be hard)but not proven). Thus the security of RSA is based on the factoring problem.

RSA cryptosystem can be used as follows (Fig

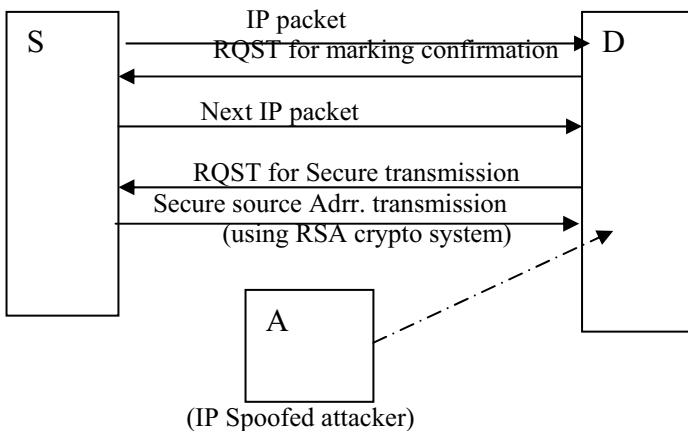


Fig 7: Secure source adrr. Transmission using RSA cryptosystem

V. MOTIVATION

In my proposed system the time required to marked 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.

- a. High speed filtering of spoofed packet.
- b. enhancement in packet transmission
- c. once secure transmission is established no role of participating router in filtering process.

VI. CONCLUSIONS AND DISCUSSION

In this paper We have proposed a low-cost and efficient scheme called CMDADF, for defending against IP spoofed attacks, The CMDADF 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 scheme also includes mechanisms for detecting and reporting spoofing in a timely manner.The evaluation of the scheme under simulations, would be shown that our scheme can effectively and efficiently differentiate between good and bad packets under spoofed attack. Most good packets are accepted even under the most severe attack, whose traffic is about 10 times of normal traffic. At the same time, the bad packet acceptance ratio is maintained at a low level. This scheme can be performs well even under massively ip spoofed attacks involving upto 5000 attackers. CMDADF scheme detected the occurrence of attack precisely within 3 - 4 seconds. The quick detection is valuable to the victim so that appropriate actions can be taken to minimize the damage caused by a IP spoofed attack.

REFERENCES

- 1.International Journal of Network Security, Vol.7, No.1, PP.70–81, July 2008(Received Aug. 9, 2006; revised and accepted Nov. 8, 2006) Yao Chen1, Shantanu Das1, Pulak Dhar2, Abdulmotaieb El Saddik1, and Amiya Nayak1
2. Y. Chen, S. Das, P. Dhar, A. E. Saddik, and A. Nayak, “An effective defence mechanism against massively distributed denial of service attacks,” inthe 9th World Conference on Integrated Design & Process Technology (IDPT’06), San Diego, June2006.
3. Y. Chen, A Novel Marking-based Detection and Filtering Scheme Against Distributed Denial of Service Attack, Masters Paper, University of Ottawa, 2006.
- 4.Y. Kim, W. C. Lau, M. C. Chuah, and H. J.Chao, “PacketScore: statistics-based overload control against distributed denial-of-service attacks,” inProceedings of IEEE INFOCOM’04, pp. 2594-2604, Mar. 2004.
- 5.A. Belenky and N. Ansari, “Tracing multiple attackers with deterministic packet marking (DPM),”in 2003 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing(PACRIM’03), pp. 49-52, Aug. 2003.
6. Network security and cryptography by William stalling