International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 1 Issue 2 July 2011

DETECTING AND PREVENTING IP SPOOFED ATTACK BY HASHED ENCRYPTION

Vimal Upadhyay (A.P St Margaret Engineering College Neemrana) , Rajeev kumar (Pursuing M-Tech Arya College)

ABSTRACT

Network introduces security problems, threats, risks and other type of attacks like internal and external attacks. Wireless networks are a new type of networked systems which comprise of motes with the physical environment and collaborate among each other to provide data to end –users. These motes are small devices that have limited processing, communication and memory. They are placed in the environment for long periods without any assistance. This technology has a lot of potential in the areas of military, health, environmental monitoring etc. As WNs are a classification of networks, therefore, most of attacks that are applicable on networks tend to apply on the WNs. Hence Security is a difficult problem in WN. And the resource- starved nature of wireless networks poses great challenges for security. The first challenges of security in sensor network lie in the conflicting interest between minimizing resource consumption and maximizing security. Secondly the capabilities and constraints of sensor node hardware will influence the type of security mechanisms that can be hosted on a sensor node platform. Energy in the security realm is key establishment. Attacks on a WN can come from all direction and target at any node. Damage can include leaking secret information, interfering messages and impersonating nodes, thus violating the above security goals. In this paper we have explored general security threats in wireless network and made an extensive study to categorize available data gathering protocols and analyze possible security threats on them.

Keywords: *Attack, Data Gathering threat mode, Routing, security, Wireless Network.*

Introduction

In this paper we explore a mechanisms for defending against ip spoofed packet attacks, have become one of the major

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 1 Issue 2 July 2011

threats to the operation of the Internet today. We 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. 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 have 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.*

Statement of Problem

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 di□cult 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

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 1 Issue 2 July 2011

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.

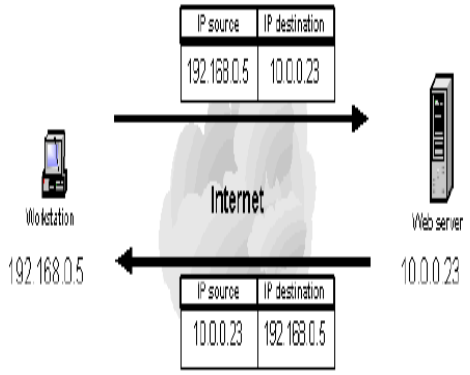


Figure 1: Valid source IP address

Figure 1: Valid source IP address

It 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.

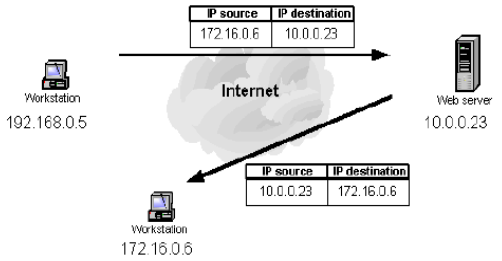


Figure 2: Spoofed source IP address

Figure 2: Spoofed source IP address

It 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

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 1 Issue 2 July 2011

web server that it will simply discard. 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.

Reactive Solutions :- Marking-based Detection and Filtering (MDADF)

The reactive measures for DDoS defence 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. 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 Pi 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 corresponding to attack packets, it can filter out all such packets coming through the same path. The Pushback method generates an attack signature after detecting a 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. D-WARD is designed to be deployed at the source network. It monitors the traffic between the internal net- work and outside and looks for the communication difficulties by comparing with predefined normal models. A rate-limit will be imposed on any suspicious outgoing flow according to its offensive. A Packet Score scheme estimates the legitimacy of packets and computes scores for them by comparing their attributes with the normal traffic. Packets are filtered at attack time basing on the score distribution and congestion level of the victim. In the Neighbor Stranger Discrimination (NSD) approach, NSD routers perform signing and filtering functions besides routing. It divides the whole network into neighbors and strangers. If the packets from a network reach the NSD router directly without passing through other NSD routers, this network is a neighbor network. Two NSD routers are neighbor routers to each other if the packets sending between them do not transit other NSD routers. Therefore, a packet received by an NSD router must either from a neighbor networks, or from a neighbor router. Each NSD router keeps an IP addresses list of its neighbor

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 1 Issue 2 July 2011

networks and a signatures list of its neighbor routers. If a packet satisfies neither of the two conditions, it is looked as illegitimate and dropped. The success of the reactive schemes depends on a precise differentiation between good and attack packets. Designing an Effective Protection Scheme Generalizing from the various defense mechanisms, a good protection scheme against DDoS attacks should be based on continuous monitoring, precise detection and timely reaction to attacks. The following characteristics are desirable: The scheme should be able to control or stop the flow of attack packets before it can overwhelm the victim. The timely detection and immediate reaction to an attack is essential, to prevent the depletion of resources at the victim location. The suitable place to deploy defense scheme are the perimeter routers or the firewall of a network. In stopping the flow of attack packets to the victim, the scheme must ensure that packets from legitimate users are successfully received so that the service to the legitimate users is not denied or degraded. Any degradation in service would signify a partial success for the denial of service attack. The implementation cost should be low. Unless most internet users fully recognize the threats posed by DoS/DDoS attacks, it is difficult to get cooperation from them in defending such attacks, especially when the investment required is costly. Therefore, any viable DDoS defence scheme should require minimal participation of third party networks or intermediate routers on the internet. A good defence mechanism should be able to precisely distinguish the attack packets from the legitimate packets. What makes it difficult to control or stop the DDoS attacks is the use of spoofed IP address. Spoofed packets are commonly used in DoS/DDoS attacks to hide the location of attackers and the compromised machines, so that the paths to them are concealed. Also, the success of the reflector attacks and many of the basic DoS attacks require the use of spoofed IP addresses in the attack packets . In the reflector attack, attackers flood the victim through some hosts called reflectors.They control the compromised hosts to send a large number of packets to many reflectors with spoofed source IP addresses of the victim. All the reflectors will send responds to the victim, so that the effect of the attack is amplified many times. Also, the attack path becomes unclear due to the participation of reflectors. Some of the DoS attacks, such as smurf, fraggle, land, and the flood attacks, need to spoof their packets, using the victim's or random IP address, to fulfill their attacks. If we can distinguish the packets which have spoofed IP addresses, then these packets can be selectively filtered out by a firewall to stop most attacks.

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 1 Issue 2 July 2011

Detecting and Preventing IP-spoofed Distributed DoS Attacks

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 all-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)_MR. In this way, the order of routers influences the final marking on a packet received by the firewall.

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 1 Issue 2 July 2011

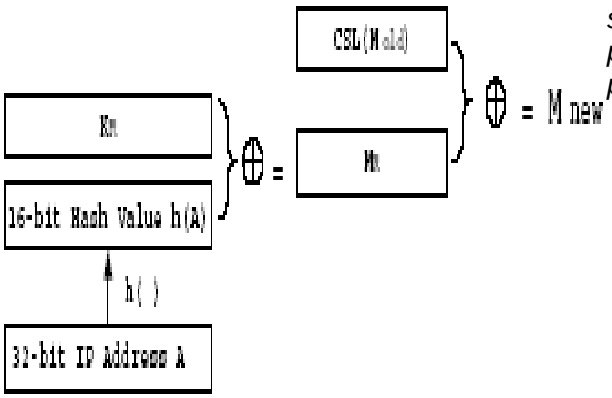


Figure 5: The marking scheme

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 <- 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
}
}

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).

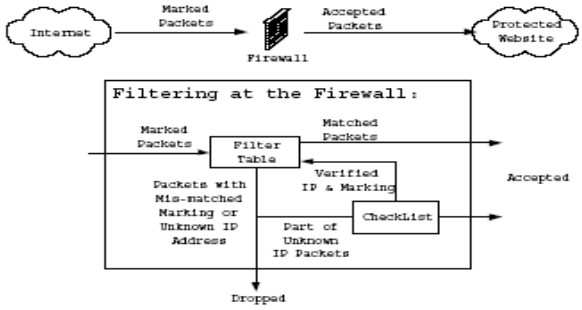


Figure 6: The system structure

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*

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 1 Issue 2 July 2011

Learning Phase

To distinguish the spoofed packets, the firewall needs to keep a record of the genuine markings. During normal time that no attacks are happening, the firewall can learn about the correct markings for packets sent from specific IP addresses. The (IP-address, Marking) pairs are stored in a Filter Table1, which are later used to verify each in coming packet and filter-out the spoofed ones. The learning phase continues for a sufficient time to allow most of the filter table to be filled up. If the Filter Table gets full, any new entry to be added replaces the oldest one. 1The filter table can be implemented as a content-addressable memory to speed up the filtering process.

Normal Filtering Procedure

After the learning phase, the firewall begins to perform its normal filtering operations. To the packet from an IP address recorded in the Filter Table, it is accepted if it has a consistent marking; otherwise, it is dropped. For the packet from a new IP address, we accept it with probability p and put the (IP-address, Marking) pair to a Check List, so that the marking can be verified. The value of p is set to high (close to 1) initially. When an attack is detected, the value of p is decreased according to the packet arrival rate and the victim's capability for handling the incoming traffic.

Marking Verification

To verify the markings in the Check-List, a random echo message is sent periodically to the source address for each (IP-address, Marking) pair in the Check-List, and a counter is used to record the number of echo messages have been sent for it. To avoid the reply being imitated by the attacker, the content of the echo message is recorded in the Check-List and compared with the content of reply received. On receiving an echo reply from the source, the marking can be verified and the (IP-address, Marking) pair is moved to the Filter Table; otherwise, it indicates the previously received packet was spoofed, then this pair is deleted from the Check List. If the counter in the Check List shows that more than d(= 10) echo messages have been sent to an IP address x, then the entry for this IP address is removed from the Check List and the pair (x,_) is added to the filter table, where _ is a special symbol denoting that all packets having source IP address x should be discarded. Since in this situation, this source IP must be either non-existent or inactive, so that the packets received with this source address are coming from the attacker and need to be rejected.

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 1 Issue 2 July 2011

Attack Detection

To detect the start of a DDoS attack, we use a counter called Total-Mismatches-Counter TMC), which counts the number of packets whose marking cannot be matched at the firewall. This includes both packets with incorrect markings as well as packets from unknown source addresses that are not recorded in the Filter Table. Whenthe TMC value becomes greater than a threshold _, it is considered as a signal of DoS/DDoS attack. The value of TMC is reset to zero after fixed intervals to ensure that the cumulative results over a long duration is not considered as the indication of attack by mistake.

Route Change Consideration

Though routes on the Internet are relatively stable, they are not invariable. Once the route between two hosts has changed, the packet received by the destination will have a different marking with the one stored in the Filter Table, so that it may be dropped according to our basic filtering scheme. Taking route changes into consideration, we introduce another counter called SMC, to count the number of mismatching packets for any IP address A. When the value of SMCA reaches a threshold _, the entry (A, Marking A) is copied to the Check List to test whether the route from this source has changed and SMCA is reset to zero. If the new marking is verified by the Check List verification process, the marking for this IP address is updated in the Filter Table. Otherwise, the original marking is preserved. Unless the route change has been verified, the original marking is still used to filter packets.

Complete Filtering Scheme

Using the techniques and criteria introduced above, a complete filtering procedure is described below. Any packet received by the firewall is judged by the filter according to the following rules:

1) If the (IP-address, Marking) pair is same with one of the records in the Filter Table, the packet is received.

2) If the source IP address of the packet exists in the Filter Table, but the marking does not match, this packet is considered to be a spoofed packet and is dropped. TMC is incremented.

3) If the source IP address does not appear in the Filter Table, then this packet is accepted with a probability p. TMC is incremented.

4) If the TMC value exceeds the threshold, an attack is signaled.

5) All echo reply messages that are received as responses to the firewall's requests are handled by the Check List verification process. They are not passed through the filter. In general, our MDADF scheme has the following functions:

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 1 Issue 2 July 2011

• 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.

Pushback Implementation

By employing the filtering scheme, the firewall can protect the victim Web site by filtering out attack packets. However, sometimes the attack flow may be too large and the firewall may not have enough resources to handle it. In that case, we may employ the method of pushback. In the Pushback method, the victim of a DDoS attack sends the signatures of attack to upstream routers and asks them to help filtering out these packets. Since one IP address can be used in the attack packets from many different sources, if we use the markings of spoofed packets as the attack signatures, large numbers of comparison need be done by the upstream routers. Instead, we create a list of IP addresses with their corresponding markings from the Filter Table and send this list (called the Push-back List) to the upstream routers. Whenever the firewall adds new entries or updates old entries in the Filter Table, these entries are sent as updates to the upstream routers, so that the Pushback List can be updated. The upstream routers compare each packet with the Pushback List after marking it and discard spoofed packets. Most of the attack packets are filtered before arriving at the victim, so that the victim Web site can continue with its normal operations. In some instances, the upstream routers of the victim still cannot deal with the attack flow, then they need to pushback further. To perform this function, each router R transforms all original markings Mi(i = 0, 1, · · · , n) in the Pushback List by computing M0 i = CSR(Mi _MR), where CSR (Cyclic Shift Right) is the inverse of the CSL operation. The router then sends the new generated markings M0 i (i = 0, 1, · · · , n) to its upstream routers. This process can be performed recursively until the attack flow is controlled.

Drawback 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.*

Proposed Framework and Design

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 1 Issue 2 July 2011

With the help of cryptosystem we can enhance the speed of detection and prevention of IP spoofed packed.

The new scheme is HASHED ENCRYPTION AND MARKING BASED DETECTION AND FILTERING SYSTEM (HEMDADF)

Which can be implemented as bellow.
Existing MDADF system

1. *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.*
2. *If marked packet is found then accepted.*
3. *Marking is done for each packet at participants routers.*

Proposed HEMDADF 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.

Research Methodology

For this any existing cryptosystem can be taken. Here I am using Hashed Encryption

Hashed Encryption:-

IPv4 Header

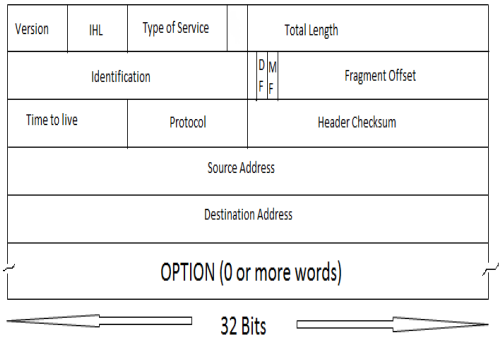


Figure 8: IPv4 Header

Encryption is done 32 bits source IP Address into fixed-length hash code using hash function and place this hash code into Identification field of IPv4 Header and send that packet into the network. On the other side, recipient received that packet and applies hash function to the source IP Address to produce hash code and compare this hash code to the hash code available in Identification field.
If both hash code are equal then packet is authenticated. If source IP Address of packet modified in network by an attacker than hash code will not be equal and recipient discard that packet.

IPv4 Packet at Sender side:

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 1 Issue 2 July 2011

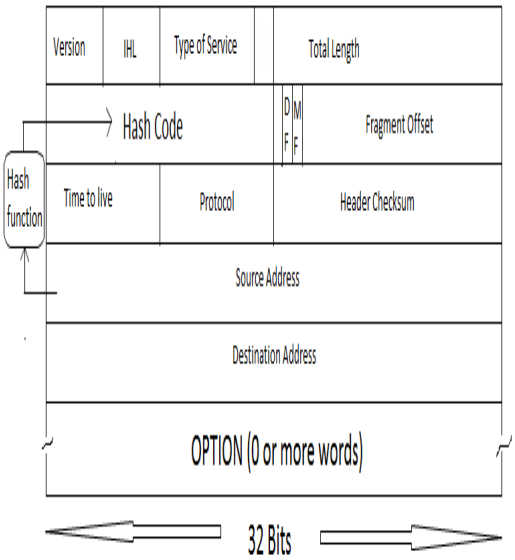
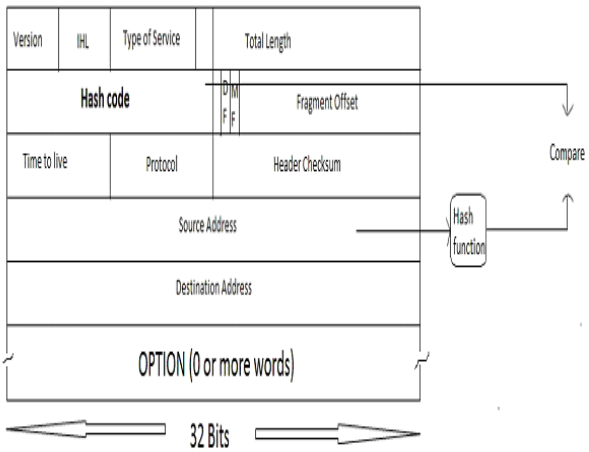


Figure 9: Packet at sender side

At sender side source address of sender inside generated packet is used to generate the hash code with the help of any known hashed algorithm. Now this hash code is written in to the identification field of the packet. Now IP packet is transferred by usual method



IPv4 Packet at Receiver side:

Figure 10: Packet at Receiver side

Whenever IP packet is received at receiver side if it is first time communication between sender and receiver then with the help of marking and detection schemes source is verified and packet is validated. Once packet and source address is validated then my given method is used to transfer the packet for better detection and prevention of IP spoofed attack.
Hashed Function can be used as follows(Fig 11)

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 1 Issue 2 July 2011

IP packet

RQST for marking confirmation

Next IP packet

RQST for Secure transmission

Secure source Address Transmission
(Using Hashed Function)

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 1 Issue 2 July 2011

(IP Spoofed attacker)

Figure 11: Secure source address Transmission using Hash function.

In our proposed system 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.

1. *High speed filtering of spoofed packet.*
2. *enhancement in packet transmission*
3. *Once secure transmission is established no role of participating router in filtering process.*

Conclusion

In this paper I have designed a low-cost and efficient scheme called HEMDADF, for defending against IP spoofed attacks, The HEMDADF 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 my 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 up to 5000 attackers. HEMDADF 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, Abdulmotaleb 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,"

International Journal of Enterprise Computing and Business Systems

ISSN (Online) : 2230-8849

http://www.ijecbs.com

Vol. 1 Issue 2 July 2011

---

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.

errig, dawnsong}@cmu.edu 2006.

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

7. StackPi: New Packet Marking and Filtering Mechanisms for DDoS and IP Spoofing Defense Abraham Yaar Adrian Perrig Dawn SongCarnegie Mellon University{ayaar, p