# IP Spoofing Prevention Methods using RPF and SPM

Irene Getzi S
Asst. Professor, Dept. of MCA
Jyoti Nivas College
Autonomous
Bangalore, India

Shilpa Vijayan
Department of MCA
Jyoti Nivas College
(Autonomous)
Bangalore, India

SitaMahalakshmi R
Department of MCA
Jyoti Nivas College
(Autonomous)
Bangalore, India

## ABSTRACT
The Internet Protocol (IP) is a main protocol using for route information across the Internet. The role of IP is to provide best-effort services for the delivery of information to its destination.

IP spoofing is a technique used to gain unauthorized access to host computers, so that the intruder can sends messages to another computer with an IP address indicating that the message is coming from a trusted host. IP address spoofing or IP spoofing is the creation of Internet Protocol (IP) packets with a source IP address, with the intention of hiding the identity of the sender or impersonating another computing system.

In non-blind spoofing the hacker requires information about the sending host like OS, Sequence Number of packets, etc. But in blind spoofing attacker might not care about the source.

A good network should have some strong Detection and Prevention methods against IP spoofing. The prevention methods can be classified as Host Based solutions, Router-Based Solutions and Solutions requiring the use of both Routers and End-Hosts.

This paper contains an overview of two prevention methods, namely RPF (Reverse Path Forward) and SPM (Spoofing Prevention Method) and its analysis. And it also shortly describes some other methods like ACL, Packet filtering, etc. As both methods have its own advantages and disadvantages, this paper is about the promotion of SPM rather than RPF. We hope that our comparative study will be helpful for researcher to merge the advantages of both methods and propose a new technique so that a secured communication system can be built.

## Keywords
IP Header, Acces control list, Filtering, FIB, CEF, &AS.

## 1. INTRODUCTION
An IP address is a binary number that uniquely identifies computers and other devices on a TCP/IP network.[5] It is a protocol for transferring information over the Internet, network and many other networks. An IP packet normally divided into two portions, namely header and body. In certain cases, hackers make some changes in the IP header so that it seems to the destination machine that the message is sent from a trusted host. This is known as IP spoofing. Hackers usually replace the source address in the header with some other IP, which may be selected randomly or intentionally.

There are many methods using to detect as well as to prevent the IP spoofing, like Packet filtering, Access control list, Compression, Cryptography, etc. Also, there are some software used for this purpose like StopCut, Find Mac Address pro, Security Gateway for Exchange/SMTP, Packer Creator, Responder Pro, etc.

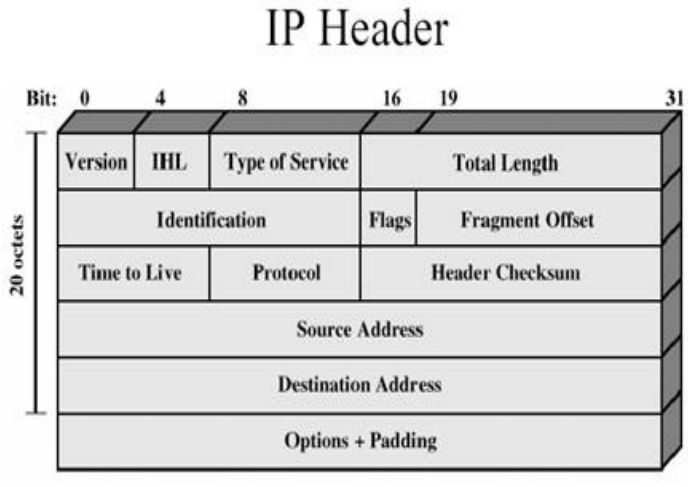
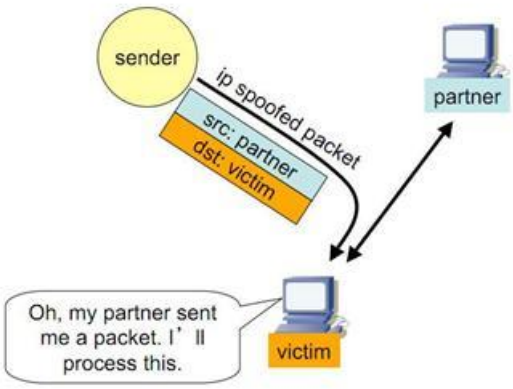



**Figure1. Header format of an IP**




Here we are concentrating on the RPF (unicast traffic) and SMP. Reverse Path Forwarding is a Cisco IOS tool for preventing IP spoofing. It checks each IP packet's source address with the routing information in the routing table as well as with the incoming interface. If the source interface different from the routing table it will drop the packet, otherwise it accepts. In the Spoofing Prevention Method, a unique key is associated with each pair of source destination networks, once a packet is received at the destination machine it will verify the key and removed.

## 2. RELATED WORKS
The internet is probably one of the greatest inventions of the century. The internet is really useful and has a lot of advantages, like the transformation of resources, files and even applications also, but it is not ensuring 100% security to the user. One needs to be very alert when using the internet. IP spoofing is one of the

main threats to internet. There are many prevention methods available.

Access Control List is a sequential series of commands or filters, which tells the router what types of packets to accept or deny based on some special conditions.[3] ACL's are applied to the interface of the routers. The Router will take the decision about packets based on the conditions specified in the ACL's. It checks source address, destination address, TCP/UDP protocols and ports to make decision. ACL also controls traffic on the interface. We need to create a separate ACL for both directions, inbound and outbound traffic. Specifically ACL is a set of commands that determines whether packets need to be accepted or dropped while coming into an interface or leaving an interface. Router checks the ACL from top to bottom and when it finds a match then the packet can accepted or dropped according to the ACL permit or deny statement.

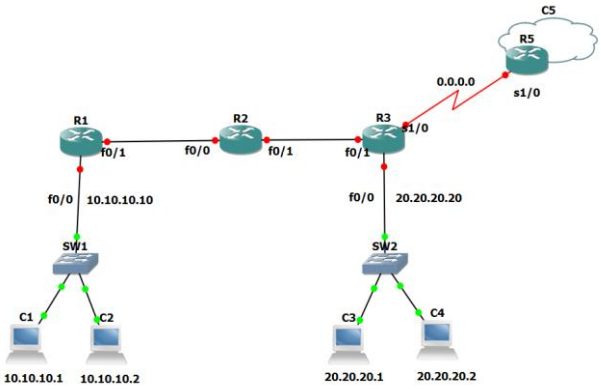
Packet filtering is another simple method of spoofing prevention. In software firewall, packet filtering is done by a program called a packet filter. Packet filter verify the header of each packet based on a particular set of rules, and based on that, come to a conclusion to prevent it from passing (called DROP) or to allow it to enter (called ACCEPT). Ingress filtering refers to the filtering of internet traffic coming into a private network. The Ingress filtering is interested in inbound traffic from a lesser trusted or untrusted network such as the internet [7] [8]. Egress filtering is a process in which outbound data is monitored or restricted, with the help of a firewall which blocks packets that fail to meet certain security requirements. The main purpose of egress filtering is to ensure that unwanted or destructive traffic (such as unauthorized e-mail messages, malware, or requests to Web sites) does not leave a particular network. [7] [8] Egress filtering can also be used to allow only certain servers or computers within an organization's network to send data out of that network.

## 3. TWO MAIN METHODS

### 3.1 Reverse Path Forwarding

RPF is a Cisco IOS tool to prevent IP spoofing. It can be used for both unicast and multicast. With RPF a router checks if a packet is acceptable or not. RPF checks the source address of a packet as well as the interface it used. If the source address is present in the routing table, then the packet is accepted by the Cisco machine, if not it will drop the packet. This method is mainly useful for DoS attacks. [2]

In RPF configured routing, if host C2 wants to send a packet to C4, it first moves to the router R1 through the interface f0/0. Router R1 will check its routing table, that the information about 20.20.20.2 is present or not, and the interface to go out. If there is a match in the routing table it will sent the packet to router R2. R2 also repeat the process of lookup and finally sent the pack to the R3. Router R3 again check that the information about 10.10.10.2 (source C2) is present or not and interface to come in. If there is a match, then R3 accept the packet and forward to 20.20.20.2 (destination C4) through the interface f0/0. If a packet with destination address other than for these networks 10.10.10.10 and 20.20.20.20, it will send through the default interface to ISP.



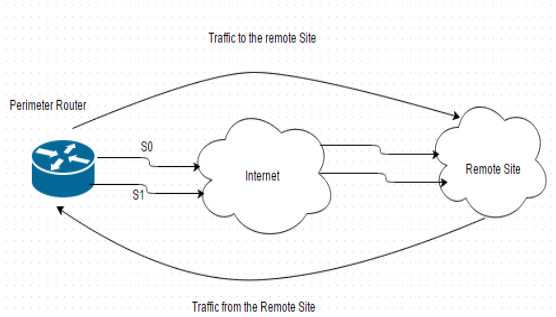

For RPF to function, CEF must be enabled on the router, because in RPF the router will use the Forwarding Information Base (FIB) which is build using CEF to perform lookup process in the routing table. FIB is a table which is created from the router's routing table, for increasing the performance of routing. Instead of checking the entire routing table each time, in CEF (Cisco Express Forwarding) FIB is pre build with IP addresses and outgoing interfaces. In real time RPF will never check directly the router's routing table; it checks the FIB to determine packet forwarding.

In case of RPF, the router not only checks the outgoing interface and destination IP, it also checks the incoming interface and source IP. The source IP should be coming from the same interface which is already updated in the FIB, if the source IP is coming from a different interface than the specified one in FIB, the packet will be dropped. Packet is encapsulated in GRE, IPSec etc, RPF will not be able to detect its spoofing.

ACL is a way of blocking some specified IP addresses, so that a host can prevent receiving a spoofed mail. We can improve the performance of RPF by enhancing with ACL. We can associate ACL with RPF so that the protection mechanism can improve. Normal RPF will drop packets that it believes to be spoofed. Cisco IOS uses the ACL to determine what action to be performed on the spoofed packet, which is detected by RPF. For this first a router should configure RPF and then ACL. In ACL, there are two statements to help in decision making; Permit statement allows the spoofed packets, and Deny statement which drops the spoofed packet.

The main attraction in ACL association is that Cisco IOS can keep track of spoofed packets. ACL provides a log file which keeps records of spoofed packets. If ACL is using Permit statement then in log file it gives the information about permitted packets. Since storing consumes more memory, it is difficult to store log file for some attacks like DoS Spoofing [10] [11].

RPF works best at perimeter router of your network, if you have single connection to entire web [12]. It is difficult to work with multiple paths in RPF. Which means that if multiple paths are exists into or from a source it is difficult for the RPF to create a summarized routing table. RPF is entirely relay on the routing table so that if there are more than one route from a same source, router will face some difficulties to create router's routing table. If we use RPF for multiple connections, it won't provide the optimal solution in detecting spoofed packet.




**RPF and Dual-Connection Problems.**

A network as shown in the figure, the perimeter router will sends packet to a remote host using the interface f0/0 with BGP; the internet will return the packet through interface f0/1 considering that as the best path. In this case if perimeter router is using RPF, It drops the packet because it was excepting, packet from interface f0/0. This is the problem when multiple paths occur.

## 3.2 Spoofing Prevention Method

Spoofing prevention method is a new approach to prevent IP spoofing, in asynchronous systems. This allows to the router at source to create a key for the packet and at the destination the key is verified and removed. In this each packet leaving from source S is tagged with a key K(S, D), where D is the destination network. Once the packet is received at destination D the key K is verified and removed by destination router. In this the overload of router is reduced. SPM is an efficient and defensive method where destination router can detect and filter the spoofed packets.

SPM is an enhanced method of both ingress/egress filtering. So it overcomes the drawback of ingress/egress filtering, i.e. SPM reduces the significant cost on ISP implementation. An ISP that joins SPM will mark all the packets that originate from it with some special keys, which is known only to the participants of SPM. Checking for the key matching in both source and destination requires the lookup operation. The key is periodically changing for each few hours to ensure more security. Key is usually a 32 bit string. The matching of key operation does not include any cryptography or any other calculations so that it reduces overhead in the router. The information of key which is generated by the source should be distributed all over to the SPM participants, for that some efficient distribution protocols are used.

AS's which required working on SPM should enable two things; 1) Mark outgoing packets with some special key, and 2) verify the authenticity of the incoming packets. An AS chooses a set of keys to mark its traffic, and which will be distributed by a specially created distributed protocol or by passive label distribution protocol. In passive label protocol key is derived from the traffic.

In SPM source AS router will place the key on packet and their authenticity is checked in destination AS router, if it is not a spoofed packet then it will be accepted by the destination after removing the key. Since the attackers have only access to low level devices, they could not be able to see the keys or the method. The main building blocks of SPM architecture are the key, Key distribution protocol and the tasks of routers.

## 3.3 Key

The main issues regarding key is, what is a key? Where the key is to be placed in a packet? And in which layer?

The key should be light weighted, Should not use any heavy calculations in creation and verification. A key is a unique string of 32 bit size, which is renewed periodically.

IP layer (networking layer) is the main layer in internet where the packets are created. This is the suitable layer to add key with header.
The effective place to add the key is in the header of the packet because header only is verified by the destination router, but in header where to add is another issue. So normally there are two options to add the key in packet header, one is to add in the IP option field and another option is to add in ID field (identification ).Option field is of 32 bit size which contains information like timestamp , record route, source route etc, But usually the routers will not process this field. This is the main disadvantage of adding the key in option field. ID field contains information of fragmented datagram, i.e. all fragments of a single datagram have the same identification number. Nowadays all packets are not fragmented. Another disadvantage of adding the key in ID field is that it is of 16 bit size, so it puts constrain for the key to be 16 bit long.

## 3.4 Key Distribution Protocol

In SPM, routers will keep key label information in two tables called AS-out table& AS-in table. In AS-out table, it maintain keys for marking flows that originate in this AS, and destined to another AS in the SPM. Whereas, AS-in table maintains keys for verification of flows that are destined to networks attached to the local AS. In SPM two methods are using for key distribution;

Passive key information distribution method: In this passive learning is used to add values in verification key table i.e. AS-in Table. Table values are being derived from the tagged keys in the traffic that comes from non-spoofed address. We can identify that a packet is non-spoofed, if it uses TCP where in the connection should be completed only with a 3-way handshake.

Active Distribution protocol: Active distribution protocol is using the normal BGP in the distribution of keys. In this it is impossible to use cryptographic keys suggested in secure BGP because keys require a light function in order to validate the actual traffic.

As it mentioned AS uses SPM so that the AS server should perform following tasks;

- Choosing the keys for the AS-out table.
- Distributing the AS-out table to the routers in this AS.
- Announcing the corresponding keys from the AS-out table to each of the other AS servers that participating in SPM.
- Building AS-in tables from announcements from other AS servers.
- Updating the AS-in table in the routers in it's AS.

## 3.5 SPM Routers

The routers should tag outgoing packets with a key and which routers should perform the authentication on AS incoming packets. SPM places the tagging task to the edge routers at the ISP. The packet authentication must do on the peering routers this way packet verification can make easy. The two main tasks of routers in SPM are;

Tagging outgoing packets with keys: To tag a packet the source is required to lookup on the destination, so we can combine this lookup process with the regular IP lookup. Two additional fields in FIB are using to store network-out table and network-in table

information in SPM. Since it requires a detailed forwarding table with entries from different AS, BGP router are best suitable for SPM.

Dynamic authentication process: Always the cost of authentication is higher than the coast of tagging the key, because it requires an additional IP lookup process for the source address (same as in uRPF).

## 4. ANALYSIS

After analyzing these two methods we find out the following things;

RPF is a router based solution, which can only be used for Cisco IOS. RPF emphasis on interface using rather than the source address to verify. It is a best suitable method for unicast traffic, like ISP directly connecting to its customer. RPF can improve its performance, if it is enhanced with ACL. RPF will function better if it is configured in the perimeter router. If asymmetric routes are using for transformation then RPF result false positive for spoofing. CEF should be enabled to function RPF. RPF faces some difficulties in multicasting like doping the replay which came through different interface. This method is not suitable for the encapsulated packets. In RPF only destination is responsible to check for spoofing. If BGP is using and giving importance for local preference and weight etc it could affect the performance of RPF. An attacker can easily hack a host which is mentioned in default gateway through other networks. RPF is fully depending on the routing table.

SPM is also a router based solution which is applicable for asynchronous systems. A strong authentication mechanism is present, using key for source and destination pair. Here both source and destination are responsible for protesting a host from spoofing. This method is not depending on routing table, but other two table kind data structures are using like AS-in table & AS-out table. Router overhead is reduced and the most of tasks are assigned to AS server. SPM can use with or without ingress/egress filtering. The key is renewing periodically, like each hour helps to prevent steeling the Key.

**Table of comparison between RPF & SPM**

| | RPF | SPM |
|---|---|---|
| Advantages | • RPF is a router based solution<br>• RPF emphasis on interface using rather than the source address to verify.<br>• It is a best suitable method for unicast traffic, like ISP directly connecting to its customer.<br>• RPF can improve its performance, if it is enhanced with ACL.<br>• RPF will function better if it is configured in the perimeter router. | • SPM is a router based solution which is applicable for autonomous systems.<br>• A strong authentication mechanism is present, using key for source and destination pair.<br>• Router overhead is reduced and the most of tasks are assigned to AS server.<br>• The key is renewing periodically, like each hour helps to prevent steeling the Key. |
| Disadvantages | • If asymmetric routes are using for transformation then RPF result false positive for spoofing.<br>• CEF should be enabled to function RPF.<br>• RPF is difficult to implement for multicasting.<br>• This method is not suitable for the encapsulated packets.<br>• In RPF only destination is responsible to check for spoofing.<br>• If BGP is using and giving importance for local preference and weight, it could affect the performance of RPF.<br>• RPF is fully depending on the routing table. | • Here both source and destination are responsible for protesting a host from spoofing.<br>• This method is not depending on routing table, but other two table kind data structures are using like AS-in table & AS-out table.<br>• Router overhead is more at both source and destination |

## 5. CONCLUSION

In this paper we are trying to make a comparative study among two spoofing prevention methods namely Reverse Path Forwarding and Spoofing Prevention Method. After studying and analysis these two, we are concluding that the SPM is a good method compared to RPF. In analysis we can find out that SPM uses some strong mechanism for prevention and it is suitable for any OS, network etc. And most important is, it have the benefit of stepwise deployment.

## 6. REFERENCES

[1] The Internet Protocol Journal, Volume 10, No. 4. By Farha Ali, Lander University.

[2] On the State of IP Spoofing Defense TOBY EHRENKRANZ and JUN LI University of Oregon

[3] Cisco Access Control Lists (ACL) By Joshua Erdman Digital Foundation

[4] IP SPOOFING By Christoph Hofer, 01-115-682 Rafael Wampfler, 01-132-034

[5] TCP/IP Protocol Suite, 4/e Behrouz Forouzan

[6] Proposed Methods of IP Spoofing Detection & Prevention. By Sharmin Rashid, Subhra Prosun Paul. World University of Bangladesh.

[7] TECHNICAL NOTE 01/2006: ENGRESS AND INGRESS FILTERING. By National Infrastructure Security Co-ordination Centre (NISCC) APRIL 2006

[8] A Comprehensive Analysis of Spoofing By

[9] P. Ramesh Babu Dept of Information Technology Rajamahendri Inst. of Engg & Technology Rajahmundry-533103, INDIA

[10] D.Lalitha Bhaskari Dept of C.S & S.E AU College of Engineering (A) Visakhapatnam-530003, INDIA

[11] CH.Satyanarayana Dept of C.S.E JNTUK College of Engineering Kakinada – 533003, INDIA

[12] IP Spoofing Attack Detection using Route Based Information By

[13] Sneha S. Rana, Department of Computer Technology, VJTI Mumbai

[14] T. M. Bansod Department of Computer Technology, VJTI Mumbai

[15] Detecting and Preventing IP-spoofed Distributed DoS Attacks By

[16] PYao Chen, Shantanu Das, Pulak Dhar, Abdulmotaleb El Saddik, and Amiya Nayak Published in International Journal of Network Security, Vol.7, No.1, PP.70–81, July 2008

[17] Understanding the Various Types of Denial of Service Attack by Raja Azrina Raja Othman

[18] Unicast Reverse Path Forwarding in CISCO IOS Release 11.1(17) CC