THE FIGHT AGAINST IP SPOOFING ATTACKS: NETWORK INGRESS FILTERING VERSUS FIRSTCOME, FIRST-SERVED SOURCE ADDRESS VALIDATION IMPROVEMENT (FCFS SAVI)

Mohamed Lotfi Abderrahim and Mona Gharib

University of Dammam, Collage of Arts and Science, Department of Computer Science,Naiyria, Kingdom of Saudi Arabia

ABSTRACT

The IP(Internet Protocol) spoofing is a technique that consists in replacing the IP address of the sender by another sender's address. This technique allows the attacker to send a message without being intercepted by the firewall. The most used method to deal with such attacks is the technique called "Network Ingress Filtering". This technique has been used, initially, forIPv4 networks, but its principles, are currently extended toIPv6 networks.Unfortunately, it has some limitations, the main is its accuracy. To improve safety conditions, we applied the "First-Come First-Serve (FCFS)" technique, applied for IPV6 networks, and developed by the "Internet Engineering Task Force (IETF)" within its working group "Source Address Validation Improvements (SAVI)", which is currently being standardization. In this paper, we remember the course of an attack by IP Spoofing and expose the threats it entails.Then, we explain the "Network Ingress Filtering" technique. Next, We present the FCFS SAVI method and methodology that we have adopted for its implementation.Finally, we, followingthe results, discuss and compare the advantages, disadvantages andlimitations of the FCFSSAVI methodto thoseknown in the "Network Ingress Filtering" technique. FCFS SAVI method is more effective than the technique of "Network Ingress Filtering", but requires some improvements, for dealing with limitations it presents.

KEYWORDS

IP Spoofing attack, Network Ingress Filtering, SAVI solutions, FCFS SAVI method.

1. INTRODUCTION

The firewall operates according to certain rules that allow the access of authorized connections to the internal network. The Transmission Control Protocol TCP (which permits the transfer of information across the Internet) depends on the methods of identification and authentication between the computers of the network. The establishment phase of a TCP connection is done in three steps (Figure 1). If host A wants to establish a TCP connection to host B, it sends a packet with SYN flag(Synchronize). Host B responds with a SYN and ACK (Acknowledgement) packet. Host A sends a packet with an ACK flag. Then A and B can communicate [1,5].

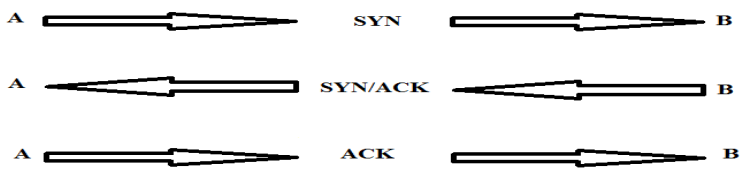

Figure 1: The phases of the establishment of a TCP connection.

DOI : 10.5121/ijsptm.2016.5101

To be able to pass through the firewall, the attacker gives his correspondence the address of one of the computers which are located in the internal network. The correspondence of the attacker appears as a normal internal correspondence between two computers in the same organization..The steps of IP Spoofing attack can be described as follows[1,7] It is considered :

S: The Target Server,
C : Client (Trusted Computer),
X : Attacker.

Find a client machine that's off. Guess the ISN of the server. Usually in regular increments. Use rsh to log in (rsh is a program that allow you to login from a remote site without a password) :

- X(as C) → S: SYN_flag, ISN=a [spoofs C]
- S → C: SYN_flag, ISN=b, ACK=a+1
- X(as C) → S: ACK=b+1 [spoofs C]
- X(as C) → S: [echo "* *" >> ~/.rhosts] [spoofs C]
- X(as C) → S: RESET [spoofs C]
- X now rlogins from anywhere in the world.

Figure 2 describes the stages of an attack by IP Spoofing.

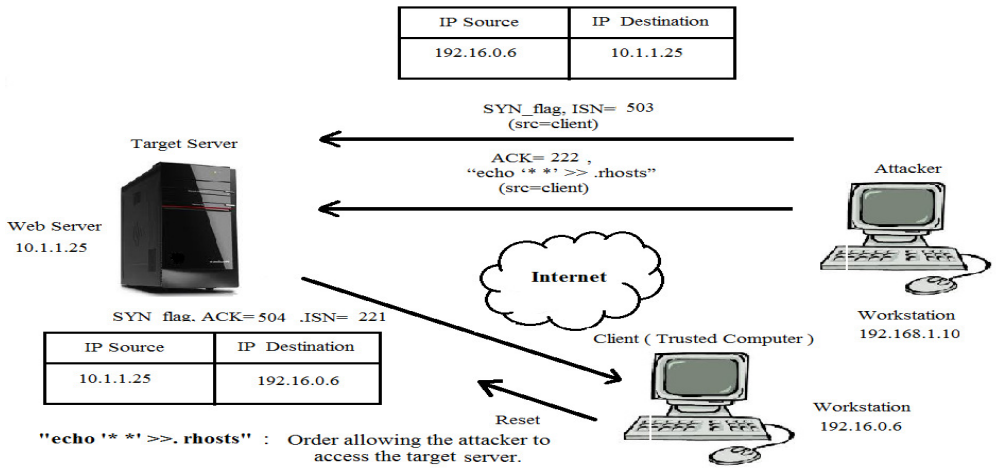

Figure 2 : Stages of the IP Spoofing attack.

This article is a contribution to the study of threats and ways to fight against IP spoofingattacks. For this, we have, in paragraph 2, established a classification ofthreats related to IP spoofingattacks. Then we described in paragraph 3, the technique of "Network Ingress Filtering" and we have given its limits.In paragraph 4, we presented the"Source Address Validation Improvements (SAVI)"solutions.These solutions are still being standardized. We chose the solution"First-Come First-Serve (Known FCFSSAVI)",and we presented in paragraph5. Paragraph6focuses on the description of the methodology we have adopted for the implementation of the FCFSSAVI solution . Paragraph 7 is devoted to presentation of results and comparisons to the imits of both techniques. The discussion of the advantages and disadvantages of solutions, is disclosed in paragraph 8. At the conclusion (paragraph 9), we described our recommendations for improving the FCFSSAVI technique.

2. THREATS SPOOFING SOURCE IP ADDRESSES

The attacks that may use the source IP address spoofing canbe classified according to their effects [8,9,10]:

- Attacks known by the technical term "Poisoning" whose objective is to corrupt databases. These attacks can continue with another attack. These attacks include: The Address Resolution Protocol (ARP) Poisoning, The Neighbor Discovery Protocol mechanism (NDP), The Domain Name System (DNS) Poisoning.

- Attacks that aim at blocking access to a service. Theyare known as the Denial of Service (DoS), such as the Denial Local Area Network (LAND)attack, The "User Datagram Protocol(UDP) Flooding"attack, The "TCP SYN Flooding"attack.

- Attacks aiming at recognition and infiltrationinto systems. For example, the "nmap"application is a well-known network recognitiontool. It allows the attacker to hide its location.

3. NETWORKINGRESS FILTERING" TECHNIQUE

This technique is static variant: "BCP 38" [11,12], or dynamic variant : "BCP 84" [4] (also known as unicast Reverse Path Forwarding (uRPF)).

3.1 BCP38

This consists in setting up filtering rules at the level of border routers of the client network and Internet Service Providers [2]. These rules will check if the source IP address of each packet passing through the router is legitimate or not [2]. Any IP packet that does not respect these rules is rejected. We considerthe architecture ofFigure 3,in which usethe techniques"NetworkIngress Filtering".

- Prefix A is allocated to Client A by the ISP.
- Prefix B is allocated to Client B by the ISP.
- The ISP uses a filtering "Network Ingress Filtering" at routers A and B.

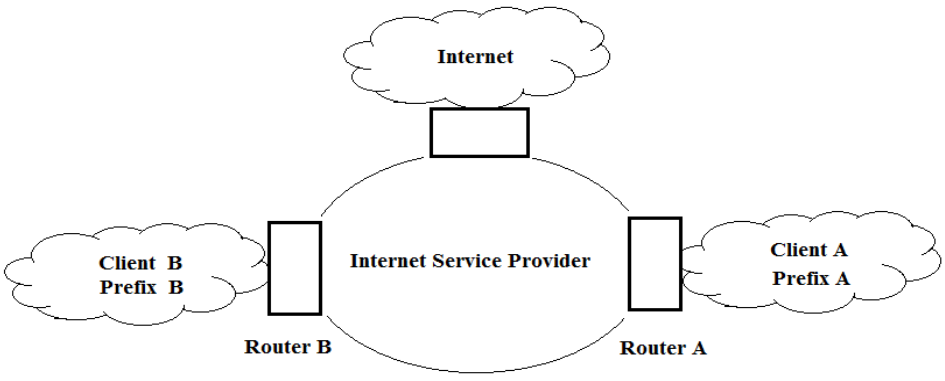

Figure 3 : Architectureusing the technique"NetworkIngress Filtering".

In this case, Router A will not let any packet get out of client A's network except those which have an IP address source that is included in prefix A. Similarly, Router B will not let any packet get out of client B's network except those which have an IP address source that is included in prefix B.

3.2 BCP 84

This technique is known as unicast Reverse Path Forwarding (uRPF) [4]. It allows you to dynamically configure filtering rules and uses the routing database (routing information base (RIB)) or information transfer bases (forwarding information base (FIB))[3]. A packet with a specific IP address source, which arrives at the filter unit is only legitimate if the filter unit verifies, thanks to its FIB, that it would have received a packet with the same IP address, but this time in destination IP address. If this condition is satisfied, the packet can be allowed [4]. The router knows thanks to its FIB, that it must transmit any packet with a destination IP address included in the prefix of a client to the that client's network and that any packet with another destination IP address should be sent to the Internet access provider network. Moreover, according to the FIB, any packet coming from the client network, will only be legitimate if its source IP address is included in the prefix of the client. Any other source IP will cause the illegitimacy and the rejection of the packet.

3.2 Limits of Network Ingress Filtering Technique

These techniques do not provideperfect protectionin the following three casesin whichlegitimatepackets can beconsideredillegitimate[4]:

(i) Asymmetric Routing.
(ii) Low granularity in the filtering rules.
(iii) Network with several ISPs (Multihoming Network).

The asymmetric routing

Asymmetric routing means that incoming and outgoing packets pass through separate routers. If the routing information is not appropriately shared between Routers, legitimate packets will be considered illegitimate and therefore rejected.

Granularity

The principle of filtering "Network Ingress Filtering" is based on the use of rules based on prefixes in order to know whether an IP packet which a specific IP address source is legitimate or not. This means that an attacker can forge his source IP address using an address that is "topologically" correct: the attacker uses an address that is related to the IP prefix allocated to the network where it is located.

Network with multiple ISPs (Multihoming Network)

In this network, each Internet Service Provider(ISP) gives a different network prefix to the client. An IP packet with a IP address source based on the prefix of an ISP may be taken to the network of another ISP. If it uses the "Network Ingress Filtering" on the router which is connected to the client, the packet can be considered illegitimate and rejected.

4. SOURCEADDRESS VALIDATIONIMPROVEMENTS (SAVI)

This method specifies mechanisms that prevent devices that are connected on the same IP link to spoof IP addresses of the same link [15].

4.1 Principle

A SAVI solution identifies which IP address is legitimate for an IP terminal. For thisreason, a SAVI instance is placed in the path of packets sent by hosts (see figure 4) and requires the use of legitimate source IP addresses by those hosts according to thefollowing three stages[15] :

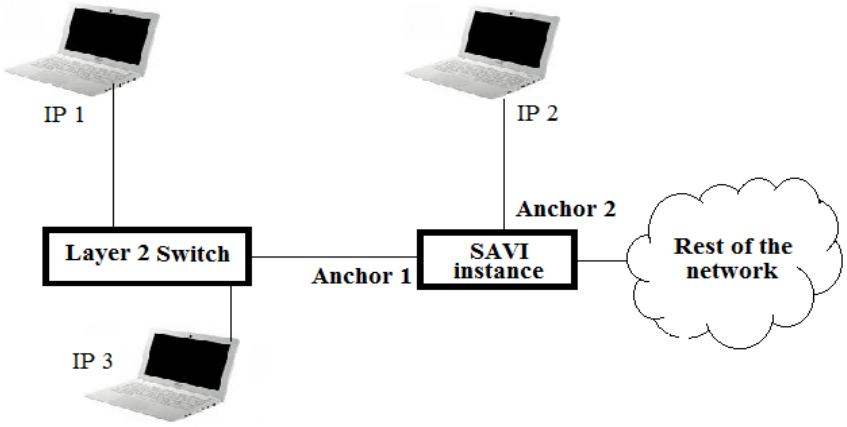

Figure 4 : SAVIarchitecture

1 - Identify which source IP addresses are legitimate for a host,relying on the observation of the packets exchanged by the host,
2 - Link a legitimate IP address to a property of the link layer where is the host network operates, This property, called binding anchor(BAnchor) must be checked in each packet sent by the host and should be more difficult to spoof than the host's the source IP address,
3 - Require that the source IP addresses included in the packets match the binding anchors to which they were linked.

A SAVI binding (SAVI-B) is an association between an IP address and a binding anchor (BAnchor). The binding anchor must be verifiable and hard to spoof[13].The BAnchor security level determines the level of reliability of SAVI solutions. Generally, they are anchorage points of SAVI instance which are chosen as BAnchor. For example [14]:

- If the SAVI instance is a layer 2 switch, the BAnchor is a switch port,
-IftheSAVIinstance is anIP router,theBAnchoris eitheranetworkinterfaceoftherouter orthe MAC address ofthenetworkinterface,
- If the SAVI instance is an 802.11 access point, the BAnchor is a "Security Association" 802.1x [19].

In the SAVI solution, a packet is considered legitimate, if there is a SAVI-B that associates the source IP address of the packet and Banch or through which the packet transits . Otherwise, the packet is considered illegitimate and it will be rejected.

The SAVI solutions are based on the observationof IP packets traffic and the use of assignment and IP address allocation protocols. These solutions are [15]:

- First-Come First-Serve, for locallyassigned addresses (FCFS-SAVI).
- SAVI Solutions for Dynamic Host Configuration Protocol (DHCP).
- Secure Neighbor Discovery (SEND).

4.2 Optimizations

In order not to suffer the scale factor and thus reduce memory requirements for SAVI instances, we define a perimeter of protection SAVI (Figure 5). The protected area is bounded by the SAVI instances [15]. It allows toclassify IP stream into two categories: one is from inside the perimeter, which will be considered trustworthy and therefore legitimate, and the other from outside the

perimeter, and will not be considered trustworthy. The SAVI solutions will be only apply to this category of flows. The validation of the source IP address is activated on all ports along the perimeter protection and inactivated on other ports.

The integrated legacy switch in the scope of protection should be unique and not partitioned [15]; the memory requirements for SAVI instances are then minimized because each link is stored only once by the SAVI instance connected to the host which is being validated. The topology of the link level ensures that packets cannot penetrate the protective perimetervia the legacy switch.

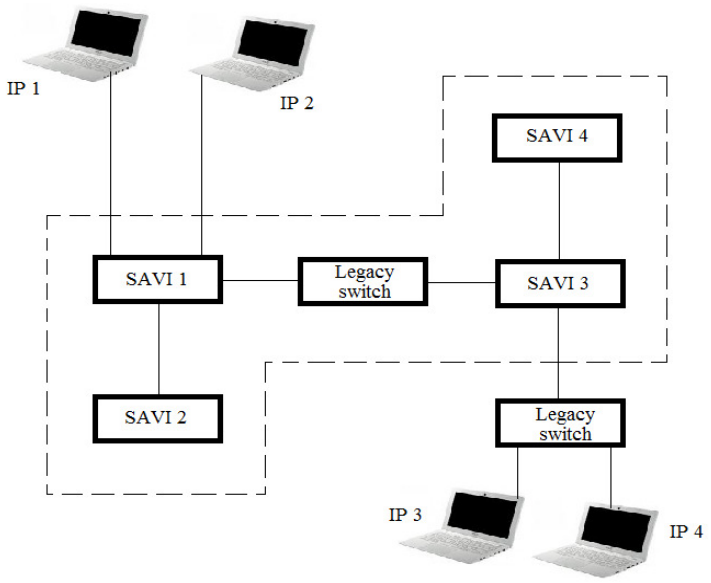

Figure 5 : Protection Perimeter.

5. FIRST-COME FIRST-SERVE (FCFS) SAVI SOLUTION

FCFS SAVI (First-Come First-Serve) solution uses SLAAC mechanisms (Stateless Address Autoconfiguration) to generate the SAVI-B [14]. It describes a method to validate the source address in an IPV6 network. The IPV6 address autoconfiguration mechanism Stateless Address Autoconfiguration (SLAAC) allows a node to generate and assign an IPV6 address [16]. This mechanism is based on the Neighbor Discovery Protocol (NDP) [17] which, itself, is based on the use of ICMPv6 messages [18] which are:

- Router Solicitation (RS) request sent by an IPV6 terminal to obtain information of a router.
- Router Advertisement (RA) message sent by an IPV6 router that contains information about the router and the network link.
- Neighbor Solicitation (NS): request sent by an IPV6 node to obtain information about another IPV6node.
- Neighbor Advertisement (NA): message sent by an IPV6 nodecontaining information about the node.

The main function performed by FCFS SAVI is to verify that the source address used in the data packets really belongs to the sender of the packet. During a SLAAC, an IPV6 node generates an IPV6 address and in order to verify that no other node on the same network link was used, it performs a procedure called Duplicate Address Detection (DAD) [16].The DAD procedure is performed on unicast addresses before assigning them to an interface.This procedurechecksthe

existence of theassigned address. Ifaduplicate addressisdiscovered duringthe procedure, thiscannotbe attributed tothe interface.Note that theDADprocedure is nottotally reliable, and it is possiblethat two identicaladdresseswill always exist [16].

According to Figure 6, the scope of application is formed by SAVI instances SAVI 1, SAVI 2, SAVI 3and SAVI 4 that check and filter information related the source address in the data packets and ND packets (Neighbor Discovery). The SAVI instances have two types of ports [14]:

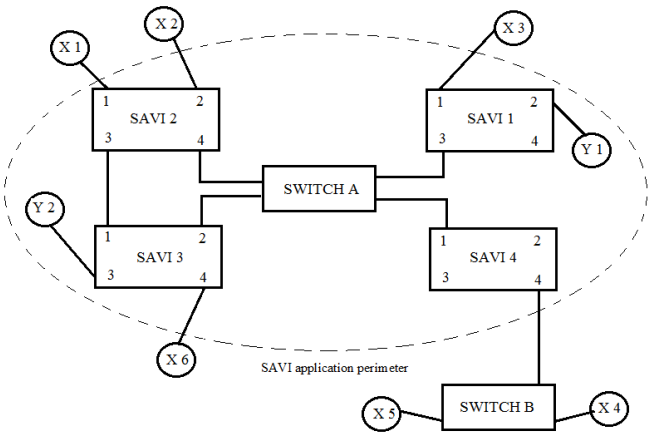

Figure 6 : FCFS SAVI application perimeter.

- Validating Ports (VP) in which treatment and SAVI filtering is performed; ports 1 SAVI 1, 1 and 2 of SAVI 2, 4 SAVI 3, 4 SAVI 4 are VP ports,
- Trustworthy Ports (TP) in which the SAVI processing is not performed: the ports 2 and 3 of SAVI 1, 3 and 4 of SAVI 2, 1, 2 and 3 of SAVI 3 1 SAVI 4 are TP ports.

6. IMPLEMENTATION OF FCFS SAVI METHOD

6.1 Data Structures FCFS SAVI

The FCFS SAVI solution uses two databases [14] :

- The first, called FCFS SAVI Data Base (FCFS SAVI DB) stores SAVI-B. Each entry of the database consists of the following information, which are given in Table 1.

Data	Description
IP ADDRESS	Specifies a source IP address.
BINDING ANCHOR	Indicates the BAnchor associated with this source IP address.
LIFETIME	Indicates the life of SAVI-B.
STATUS	Indicates the status of SAVI-B (TENTATIVE, VALID, TESTING_VP or TESTING_TP-LT).
CREATION TIME	Indicates when the entry was first created.

Table 1 : Information in the database FCFS SAVI DB.

-The second database is the FCFS SAVI Prefix List (FCFS SAVI PL). It can store the IP prefixes used in the networks links which ministrator of the SAVI instance or dynamically thanks to the A

messages received on TPs. Each entry in the FCFS SAVI PL contains the following information, which are given in Table 2.

Data	Description
PREFIX	Indicates an IP prefix.
PORT	Indicates the port on which IP prefix is observed.

Table 2: Informationinthe database FCFS SAVI PL

6.2 Ports configuration

Table 3 describes the port configurationof the SAV Iinstance.

Portsconfigured asTP	Portsconfigured asVP
Ports connectedtoanotherdeviceSAVI.	Ports connectedto hosts.
Ports connected torouters.	Ports connectedto a seriesof one or many switches(notSAVI) havingconnected hosts.
Ports connectedto a seriesof one or many switches(notSAVI) havingSAVIdevices or connectedrouters, but not to hosts.	Ports connectedto a seriesof one or manyswitches(notSAVI) havingSAVIdevices orrouters connectedto hosts.

Table3: Ports configuration on a SAVI instance.

6.3 Conduct of FCFS SAVI

The FCFSSAVI solution applies only to the local link [15]. A link consists of hosts and routers attached. Hosts generatepackets withtheir ownaddress as the sourceaddress.Thisis calledlocal traffic.Routerssend packetscontaining differentsource IPaddresses andgenerated by otherhosts(usuallylocated in anotherlink).This iscalled transit traffic.To distinguish between local traffic and transit traffic, SAVI device is based on FCFS SAVI prefix list and must take into account the two methods of assignment of prefixes which are manual setup and Router Advertisement configuration [17].

6.4 Treatment of transit traffic

This traffic is described in the following short form:

- If the data packet is received by a TP, no SAVI processing is performed on the package if no message NS is involved in the DAD procedure.
- If the data packet is received by a VP, SAVI function must check whether the data packet belongs to the local or transit traffic by searching the FCFS SAVI Prefix List:
- If the source IP address does not belong to any prefix (transit traffic), the packet must be destroyed,
- If the source address of the packet belongs to a prefix, the SAVI validation process for local traffic is run.

To implement this traffic, we developed the algorithmof Figure 7.

6.5 Local traffic Treatment

The description of the processing of data packets and of control by SAVI instance will be performed by a finite state machine system [14]. The different possible states of this machine are listed in Table 4.The Figure 8 describes the finite state machine of the FCFS SAVI method.

State	Description
NO_BIND	Input IP address does not contain BAnchor.
TENTATIVE	A data packet or DAD_NS message about IP address has just been received, the DAD procedure runs.
VALID	The link to IP address has been verified, it is valid and useful to filter traffic.
TESTING_TP-LT	Either a DAD_NS message was received on IP address by a TP or Lifetime IP address is about to expire.
TESTING_VP	DAD_NS message or data packet is received by a VP other than P.

Table 4: States of the finite state machine.

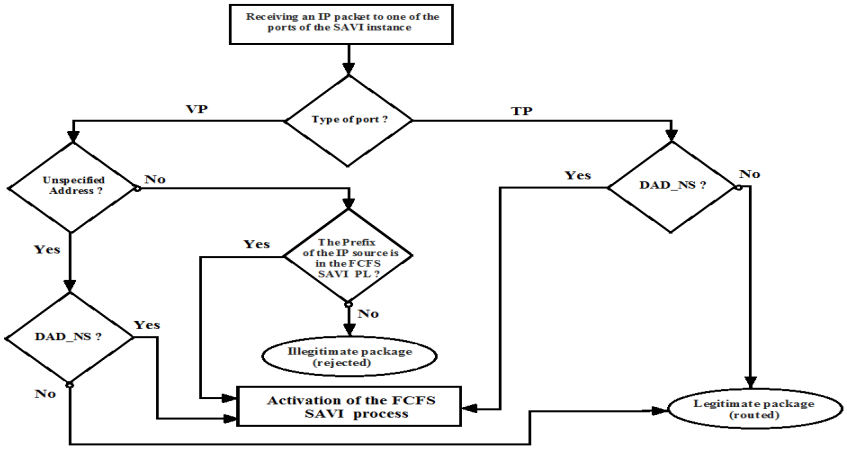

Figure 7: Algorithmof transit traffic.

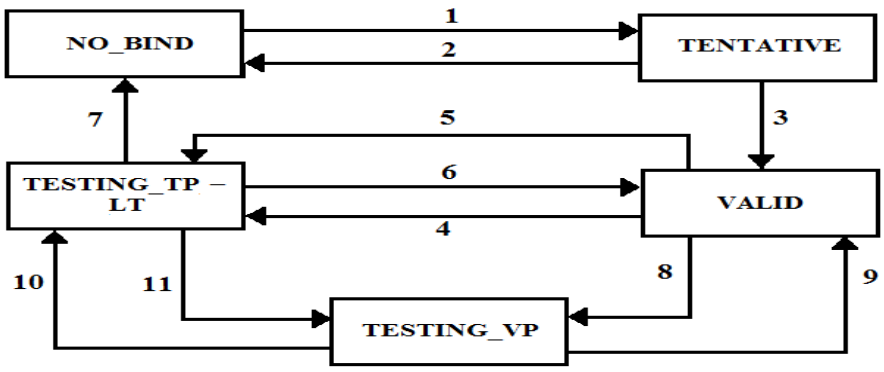

Figure 8: The finite state machine of the FCFS SAVI method.

By default, a packet with a source IP address, which has no entry in the FCFSSAVIDB, passes automatically in NO_BIND state. The SAVI instance will be activated and checks whether a SAVI-B exists for the IP address of the packet. Then, the finite state machine of the FCFSSAVI solution works are explained in Table5.

Table 5: Functioning of the finite state machine of the FCFSSAVI method.

Passing	Initial state	Final state	Pass condition	Comment
1	NO_BIND	TENTATIVE	Ifthe source IP addresswas notaSAVI-B, while creating aSAVI-B tothis address	
2	TENTATIVE	NO_BIND	FailedDADprocedure performedat theTENTATIVEstate.	
3	TENTATIVE	VALID	Success of theDADprocedure performedat theTENTATIVEstate.	
4	VALID	TESTING_TP-LT	Receiving aDAD_NSon a TP.	TheIPnode can beconnectedelsewhere.
5	VALID	TESTING_TP-LT	Expiry of thelifetime of theSAVI-B.	EachSAVI-Bhasa lifetime.
6	TESTING_TP-LT	VALID	FailedDADprocedure runat theLT-TESTING_TP stateandthe answerinaDADisNAreceived on portP.	
7	TESTING_TP-LT	NO_BIND	Success of theDADprocedure performedat thestateTESTING_TP-LT	
8	VALID	TESTING_VP	Packet receivedon a different portP '.	
9	TESTING_VP	VALID	Success of theDADprocedure performedat theTESTING_VPstate,andthe packet is aDAD_NS OR FailedDADprocedure performedat theTESTING_VPstatedue toNAmessage received on thePortP.	The portP 'will be likeBAnchorin theSAVI-B. Ifthe DADprocedurefails,because ofDAD_NSreceivedon portP ", different from P andP ' then the stateremains toTESTING_VP.
10	TESTING_VP	TESTING_TP-LT	FailedDADprocedureperformedat theTESTING_VPstatedue toDAD_NSreceived via aTP.	

11	TESTING_TP-LT	TESTING_VP	FailedDADprocedure performedat theTESTING_TP-LT stateandthe response is receivedon a different portP'.	

7. RESULTS

In the simulations we have done, we have unusualon thecomparisonof the limitsof the "Network Ingress Filtering" Technique, mentioned in paragraph3 - 3,to those foundin the FCFSSAVI solution . The tables 6summarizes the results of this comparison.

Table 6 : Comparison between FCFSSAVI solution and Network Ingress Filtering Technique.

	Network Ingress Filtering Technique	**FCFSSAVI Solution**
Address Family	**IPV4, IPV6**	**IPV6**
Application Area	**Transit Traffic**	**Local Traffic**
Limits	- Asymmetric Routing. - Low granularity in the filtering rules. - Network with several ISPs (Multihoming Network).	- Asymmetric Routing. - Network with several ISPs (Multihoming Network). - Fragmentation. - Effects ofoDADprocedure. - Invasion of privacy.
Security Considerations	Filtering canbeineffective ifthespoofed IP addressis inthe range ofvalid internaladdresses.	SAVIasolution cannotbemore secure thantheanchorlower levelit uses.Thus, if theanchor canbefalsifiedthe solution will befragile.

Granularity problem does not occur in the FCFSSAVI solution, but other problems arise: Fragmentation, Effects of oDAD procedure, Invasion of privacy. We have found in the literature description of these problems.

Fragmentation

When the FCFS SAVI solution is integrated into a material having little computing resource (layer 2 switch), the signaling becomes complex to treat. If the message is fragmented [20], its interpretation by the SAVI instance becomes difficult. In addition, the SAVI instance will be unable to generate B-SAVI. Consequently a legitimate traffic will be considered illegitimate.

Effects ofoDAD procedure

In some cases, it may be necessary, anIPv6node uses quickly address, generated or allocated. The procedure Optimistic Duplicate Address Detection (oDAD) [21]allows anIPV6nodeto useIPV6 addressbefore the DAD procedureis finalized.Compared to the DAD procedure, the advantage of oDAD procedureis to minimize address configuration delays in the successful case, and reduce disruption as much as possible in the case of failure.But in some cases, if the oDAD procedure is

used in anarchitecture based onSAVIsolutions, IPV6flowwill be consideredillegitimatebecause noSAVI-B exists.

Invasion of privacy

The FCFS SAVI solution allows to associate an IP node to an IP address.This technique can help administrators to control and monitor their networks [22]. An administrator can monitor all the messages sent and received by an IP node, identified by BAnchor. This monitoring is against user privacy.

8. DISCUSSION

8.1 Network Ingress Filtering Technique

The techniques of" Network Ingress Filtering" (BCP 38 andBCP84)can block the majority of IP packets with spoofedsource IP address. These techniques, easy to implement, are used to validate thesource IP addresses because they are simple to implement[15]: the decision to acceptor reject a packet is made solely on the basis of information available from routing protocols.The strength of BCP 38and BCP 84 depends on the position of the filter in the network. To be effective, these filters should not be deployed on a limited portion of the network, but rather on the entire network, either at the level of access to the network for BCP 38ordistributed manner throughout the network for theBCP84 [26]. In case of control of the network, the BCP 38hasa method seems both more efficient and requires less resources than theBCP84. Moreover, it does not require a complex distribution as is the case for theBCP84. Finally, from a technical point of view,this method appears to be feasible. It also indicates that depending on the position of the filter,the"ingress filtering" techniques can cause problems with DHCP(Dynamic Host Configuration Protocol) or BOOTP (Bootstrap Protocol) [25].

The disadvantage of BCP 38 is that the filtering rules are configured manually [12] : this can lead to the release of legitimate packets in case of a human error, which may occur while setting the rules[2]. In addition, the updating of filtering rules is not easy to perform , in case of allocation of a new IP prefix in the network.

The main advantage of BCP 84, compared with the BCP 38, is to avoid a long process of configuring access control lists for each border router, by implementing automatic configuration process using the settings from routing tables.

8.2 FCFS SAVI Solution

The objective of the FCFSSAVI solution is to verify that the source addresses of packets generated by hosts connected to the local link, have not been usurped. It preventsa hostto spoofthe source IP addressesofother hostsattached to thesamelink.Thissolutionisalsomodularandreproducible(based onthenetworkonly) [15].

The FCFSSAVI solution is designed to be used inexisting networks,which do not require changes.For this reason,FCFSSA VIdoes not require changes inhostsand verification of source addresses is based solelyon the use ofalreadyavailable protocols [14].In otherwords,FCFSSAVIsolutiondoes not definea new protocolanddoes not develop anynew message onexisting protocolsanddoes not requirethat a hostuses an existingprotocol messagein a different way. TheFCFSSAVIsolutionisbased on the analysisof the protocols usedin thenetworksand, therefore, ithas limits,since itinheritsthe disadvantagesrelated to them.It is also reported that there exist two types of denial of service(DoS)[24] that can be considered in a

FCFSSAVI environment[14]: Attacks against the device resources FCFSSAVI and attacks againsthosts connected to the network where FCFSSAVI is installed. Fortunately,effective solutions have been proposed to imit the effects of such attacks [14].

9. CONCLUSION

IP Spoofing attacks are a still a dangerous phenomenon for information systems. Actually all the solutions that are currently used are not very effective, becausethearchitecture of the Internetdoes not preventthis type of attack[2]. To fight against this kind of attack, we proposed in this paper, the Network Ingress Filtering techniques and the FCFS SAVI solution.

Ingress filtering approaches are essentially preventive. They are standardized by IETF and represent highly efficient solutions to prevent against the addresses spoofing by malicious people. The techniques usedby the approachesofingress filteringare different,but they havea common limitation: ingressfilteringdoes not guaranteetotal protectionof the entirenetwork.These techniquesprohibit address spoofing,onlyin a limitedpart of the network. In addition, Ingress Filtering techniques are generally ineffective against the encapsulated packets, attackers can generate attacks using legitimate addresses and legitimateflow. Network Ingress Filtering techniques are not entirely reliable. They can only be applied to transit traffic. All this does not encourage entities to implement this type of filtering [25].

The FCFSSAVI solution complementary to the Network Ingress Filtering technique, solves that one limitation of this technique: granularity [15].In addition, its applicability is limited to local traffic. The verification of the source addresses of the transit traffic is out of the scope of FCFS SAVI.

The FCFSSAVI solution is still being standardized, so it is necessaryto revise itto improveits performance.In this sense, it is useful to provide:

- The use of the protocol: Simple Management Protocol (SNMP), which helps in the management and deployment of SAVI solutions [23].
- The extension of the scope of SAVI protection, o it integrates FCFSSAVI solution and Ingress Filtering Techniques. The techniques of Network Ingress Filtering valid transit traffic and FCFSSAVI does the local transit. This allowsto form a largertrusted zone.

Currently, the techniques of"NetworkIngress Filtering" are most commonly used. Inour future work, we will implement theamendments we haveproposedin this paper, that the FCSFSAVIsolution isthe most widespread inthe fightagainstIP spoofingattacks.

ACKNOWLEDGMENT

This Project was funded by Deanship of Scientific Research at the University of Dammam under No. 2014076.

REFERENCES

[1] Kak, A." TCP/IP Vulnerabilities: IP Spoofing and Denial-of-Service Attacks ". AvinashKak, Purdue University, 2015.
[2] McPherson, D. ,Baker, F. and Halpern, J." Source Address Validation Improvement (SAVI) Threat Scope ". RFC 6959, Internet Engineering Task Force, ISSN: 2070-1721, 2013.

[3] John Scudder, J. " Router Scaling Trends ". Juniper Networks, Inc, 2007. [Online]. Available: http://meetings.ripe.net/ripe-54/presentations/Router_Scaling_Trends.pdf

[4] Baker, F., Savola, P. " Ingress Filtering for Multihomed Networks ". RFC 3704, Internet Engineering Task Force, 2004.

[5] Chopra, R. and Farooqui, R. A. " IP Spoofing Attacks ", 2012.[Online]. Available: http://www.slideshare.net/apijay/ip-spoofing-attacks

[6] Agence nationale de la sécurité des systèmes d'information ANSSI. " Bonnes pratiques de configuration de BGP ", 2013. [Online]. vailable: http://www.ssi.gouv.fr/uploads/IMG/pdf/guide_configuration_BGP.pdf

[7] Bellovin, S.M. " Security Problems in the TCP/IP Protocol Suite". AT&T Bell Laboratories Reprinted from Computer Communication Review, Vol. 19, No. 2, pp. 32-48, April 1989. Murray Hill, New Jersey 07974.

[8] Ballan, E. and SURANGKANJANAJAI,G. " Dénis de Service et usurpation d'identité ", 2002. [Online]. Available: http://www.master-informatique.net/~fnolot/Download/Cours/reseaux/m2pro/SESY0708/attaques_classiques.pdf

[9] Patrick Ducrot, P. " Sécurité Informatique ". ENSICAEN, 2015. [Online]. Available: http://patrick.ducrot.free.fr/securite.pdf

[10] Ferdous A. B. , Gunjan B. , Niteesh K. , Santosh B. and Sukumar N. " Detection of neighbor discovery protocol based attacks in IPv6 network ". Networking Science, 2: 91–113, 2013.

[11] Bhaiji, Y. " Router Security and Infrastructure Protection", Cisco Systems, 2007. [Online]. Available: http://www.sanog.org/resources/sanog17/sanog17-security-tutorial-bhaiji.pdf

[12] Ferguson, P. , - Senie, D. " Network Ingress Filtering:Defeating Denial of Service Attacks which employIP Source Address Spoofing". RFC 2827,Internet Engineering Task Force, 2000.

[13] Bagnulo, M. and García-Martínez, A. " SAVI: The IETF Standard in Address Validation " IEEE Communications Magazine, 54(4), 66-73, 2013.

[14] Nordmark, E. , Bagnulo, M. and Levy-Abegnoli, E. " FCFS-SAVI: First-Come First-Serve Source-Address Validation for LocallyAssigned Addresses ". RFC 6620, Standards Track.Internet Engineering Task Force, ISSN: 2070-1721, 2012.

[15] Wu, J. , Bi, J. , Bagnulo, M. , Baker, F. and Vogt, C. " Source Address Validation Improvement Framework ". RFC 7039, Internet Engineering Task Force, ISSN: 2070-1721, 2013.

[16] Thomson, S. , Narten, T. and Jinmei, T. " IPv6 Stateless Address Autoconfiguration". RFC 4862, Internet Engineering Task Force, September 2007.

[17] Narten, T. , Nordmark, E. , Simpson, W. and Soliman, H. " Neighbor Discovery for IP version 6 (IPv6) ". RFC 4861, Internet Engineering Task Force, September 2007.

[18] Conta, A. , Deering, S. and Gupta M. " Internet Control Message Protocol (ICMPv6)for the Internet Protocol Version 6 (IPv6) ". RFC 4443, Internet EngineeringTask Force, March 2006.

[19] Devin A. " Robust Security Network (RSN) – Fast BSS Transition (FT) ". CWNP Program,2008. [Online]. Available: https://www.cwnp.com/uploads/802-11_rsn_ft.pdf

[20] Deering, S. and Hinden, R. " Internet Protocol, Version 6 (IPv6) Specification ". RFC 2460, Internet Engineering Task Force, December 1998.

[21] Moore, N. "Optimistic Duplicate Address Detection (DAD) for IPv6". RFC4429, Internet Engineering Task Force, April 2006.

[22] Chown, T. " IPv6 Address Accountability Considerations ". Internet EngineeringTask Force, July 2011.[Online]. Available: http://tools.ietf.org/id/draft-chown-v6ops-address-accountability-01.html

[23] Harrington, D. , Presuhn, R. and Wijnen, B. " An Architecture for Describing Simple Network Management Protocol (SNMP) ". RFC 3411, Internet Engineering Task Force, December 2002.

[24] Handley, M., Rescorla, E. "Internet Denial-of-Service Considerations". RFC 4732, Internet Engineering Task Force, November 2006.

[25] COMBE, J. M. " Requirements on Security in 6QM Project" . Information Society Technologies – Version : 3.1 – Project number : IST-2001-37611 – 2003.

[26] Leborgne, F. " Traçage et Filtrage: Recherche, Etude et analyse des solutions de trace back et de filtrage dans le cadre des attaques par déni de service". Informatique Signaux et Systèmes de Sophia-Antipolis CNRS - Université de Nice - juillet 2005