Semiconductor Optoelectronics
ISSN: 1001-5868

SECURITY ATTACKS IN IPV4 AND IPV6 AT THE NETWORK LAYER

S. Manimozhi
Assistant Professor, Department of Computer Science and Applications, Periyar Maniammai Institute of Science and Technology, Vallam, Thanjavur, Tamilnadu-613 403, India.
manimozhi.subramanian@gmail.com

S.Arumugam
Associate Professor, Department of Computer Science and Applications, Periyar Maniammai Institute of Science and Technology, Vallam, Thanjavur, Tamilnadu-613 403, India.
arumugamtnj@mail.com

P.Ranjani
Assistant Professor, Department of Computer Science and Applications, Periyar Maniammai Institute of Science and Technology, Vallam, Thanjavur, Tamilnadu-613 403, India.
ranjanirengan@gmail.com

Abstract— The current version of Internet Protocol (IPv4) is used for the hosts to be communicate in the network. The main lack of IPv4 is providing address space to the host when beyond the size of available address space. The next lack is to provide better security at the network routing rather than end-to-end security attacks. The first lack overcome by introduced new protocol called IPv6. The second lack is overcome using harder security concepts in network routing. The newly developed Internet Protocol 6 (IPv6) faces many security attacks in the network routing similar to IPv4. This paper reviews the IPv4 and IPv6 security attacks and possible solutions for these attacks in the network routing.

Keywords— IPv4 header,IPv6 header, IPv4 Security attacks, IPv6 security attacks, IPv6 headers

I. INTRODUCTION

The current version of Internet Protocol (IPv4) is used for the hosts to be communicating in the network. It provides better way to communicate hosts in the network. But, it faces two lacks in the network communication. The first lack is described as supports only 232 bit address space=4 billion in the network communication. And the second important lack is providing better security at the network routing rather than concentrating security in end-end security [1]. The first lack is overcome by introduced newly developed Internet protocol-6 (IPv6). It supports 2128 bit address space= trillion and trillion address spaces in the network. This address space provides a combination of 3.4X1038 addresses [2].

The second lack is providing better security to the network routing rather providing security at the end-end network communications. IPv6 structure also look similar and different security

attacks in the network routing which was been faced by IPv4. By providing better security architecture in the network, implies that the communications are in secured way. It ensures that the network is not flooded with attacks.

II. IPV4 AND IPV6 HEADER FORMAT

The IPv4 has 32 bit address space with 14 fields. The figure, Fig.1 shows the header format of IPv4. The IPv6 header itself is always exactly 32 bytes, and contains exactly 8 fields. Version field is common to both headers which indicate the version of the Header. Both headers have Source and destination address field with different size Flow label added as a new field in IPv6. Fragment Offset field, Header Checksum field, Option field and Padding field are dropped in IPv4. TTL filed replaced with Hop Limit field. Protocol field replaced with Next Header Type field. Extension header carries out the functionality of Protocol field, Option field, and Fragment field functionality. The figure, Fig.2, Shows the header format of IPv6.

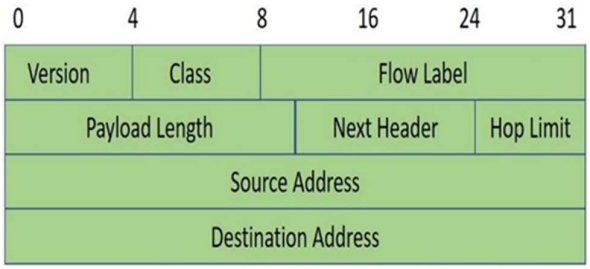

Fig.1 IPv4 header format

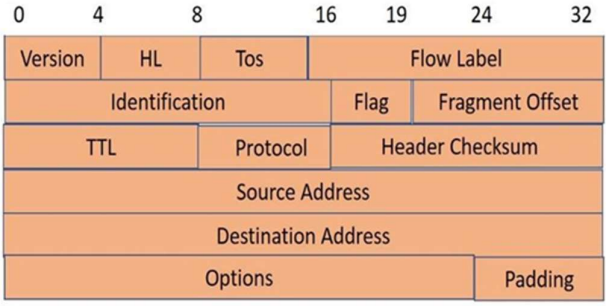

Fig.2 IPv6 header format

III. IPV4 SECURITY ATTACKS

At the initial development of IPv4, the end-to-end communications between networks were concentrated rather than concentrating network security. There are many security attacks were pioneer by the attacker at the network [4,5].

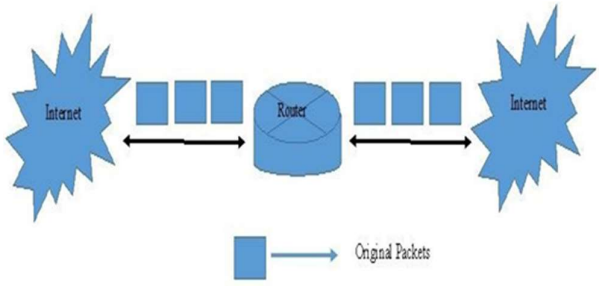

Fig 3. Sending Packets before hacking in network laye

Fig 3 shows the packet transformation without hacking which implies that the both the sender and receiver have a secured communication. But in Fig 3.2, the packets are attacked by the attacker and the receiver receives the attacked packet which implies that the communication is in unsecured way. For providing better security architecture, should understand the basic attacks in the network.

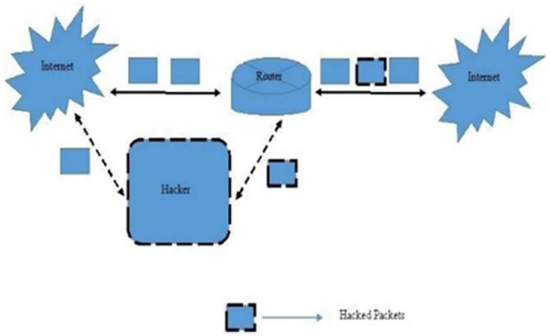

Fig.4 Sending Packets when hacking in network layer

The following sections summarize the various network security attacks under routing protocol.

A. Information gathering

Attackers are trying to know the individual host that are involved in the network. In this type of attacks, the attackers identify the machine's basic software and type of instructions running in the network. The attackers are hacked the Domain Names, Server Names, IP Addresses, Network Map, ISP / ASP information, System and Service Owners etc.

B. Denial of Service Attack

In DoS attack, the attackers deny the authorized users from accessing the servers. The attacker sending flooding of request to the router when is it in busy in routing process. The result is to be affecting the usage of the router and become the router should be identical.

C. Routing Table Poisoning

Routing table is an important table in the network which is help to move a packet between the routers based on the information in the routing table. The routing table information are modified or deleted by the attackers in the network. It creates the entire network to be damaged by create this type of attack.

D. Hit and run attacks/ Packet Mistreating Attacks

In this attack, the attacker sends malicious packets to the router. The router reads the malicious code and doing the activities which are defined in the malicious packet. The routers are suffered from malicious code of packets from the attacker. So, the malicious router couldn't deliver the pocket properly. Hence, it creates loops, denial-of-service, and congestion in the network. This type of attack is very difficult to find and debug.

E. Persistent attacks

The attacker doing continuous hit and run attacks to the router. The router doing the repeated task based on the continuous hits. The packets are modified continuously and identified easily with the help of routing table information.

F. Fragmentation attacks

The attackers exploiting the size of the packets. In this attack, the packet size will be changed beyond the size of the packet. So, it causes the packet may not be sent to the destination machine. It stops or suspends the router processing task.

H. Man in the Middle Attack

IPv4's authentication mechanism allows an attacker to read, insert and modify the messages between two hosts without their communication has been negotiated. ICM used to carry out this type of attacks.

IV. IPV6 SECURITY ATTACKS

In IPv6, the security protocols like, firewalls, network Intrusion Detection Systems have less support for IPv6 protocols rather than supporting in IPv4. IPv6 developed with the concentration of security concerns not only in the end-end hosts but also in intermediate hosts. Even though, it faces many security attacks in network communications.

A. Neighbor discovery attacks

The attacker finds the neighbor address with the help of the last hop and sends the attacked packets to the neighbor address which results the router to be flooded.

B. Router advertisement spoofing

In this type of attack, the attackers may flood huge number of RA at a time. Hence, the Microsoft Windows computers stops its execution overloaded with that numerous SLAAC processes. This bug is renowned for numerous years but still exploitable.

C. Block Hole Attack

The attacker creates a node as an optimum node between the source and destination address. It fakes the routing information into the router. The router information are faked in this attack.

D. Wormhole Attack

The attackers read the packet information from one location and manipulate the packet from another location and resend it. So, the router confused about the packet information.

E. Colluding Miss Relay Attack

The attackers are grouped together to modify the packets from different routing places and to modify / drop the routing packets to disrupt routing operations. In this type of attack, the router may confuse lot about a routed packet.

F. Link withholding Attack

The attacker introduces the malicious node in between the communication of required node

and the router. So, the communication between the host and router is disturbed through malicious node.

G. Reply Attack

The attackers get the information from the routing table and reply the old value. It causes the router read old value rather than read new value.

H. ICMPv6 and multicast attacks

The multicast group of systems sends the response when attacker sends the information. Then, the attacker uses the information for further attacks.

IV. COMMON ROUTING ATTACKS IN IPV4 AND IPV6

Some of the network attacks are common in IPv4 and IPv6. The routing differences are identified by the size of the packets and the structure of IPv6 header. But the common routing attacks are attacked by hackers both in IPv4 and IPv6 in network routing [6].

A. Network sniffing Attack

Attackers capturing data being transmitted in plain text in the network. In network sniffing the attacker sends the data to the router as act as from the original source. The information like password, user id and account information etc are hacked in this attack.

B. Network Spoofing Attack

It faking the address or identity of packets. The router accepts the data from the spoofed packet and sends it to the router. The router sends the data from the spoofed source address in to the destination address. The spoofed packets are identified and filtered by using ingress filtering and egress filtering. It exchanges the network resources to affect the network performance.

C. Session hijacking

The original source has been strongly authenticated after the connection take over by the intruder. The encryption facilities of the IPSec protocols protect a connection from an intruder that the intruder does not know the session keys mandatory to encrypt or decrypt the data stream.

V. POSSIBLE SOLUTIONS FOR NETWORK SECURITY

The network communications are protected from the attacks only by providing better architecture in the routing network. There is a strong routing protocols are developed. The main possible solutions for security attacks are,

1. The network administrator should know the architecture of router and firewall.
2. Increase the reliability, performance and security of the network.
3. Routing vulnerabilities are monitored at each communication.
4. Update the network in the way of providing password and firewall activation etc.
5. Protect the network from worms, attackers and virus, etc. 6.Should maintain a separate entry for machines or hosts is to be participated.
7. Encrypt whole network.

8. Provide different access permission to each level in the network.

VII. CONCLUSION

Both IPv4 and IPv6 meet many security attacks in network level communication. The main disadvantage of the security at the Internet Layer is that IP Packets are either changed or modified. All security attacks create an authorized service in the network. For better services in the network, the routing attacks are protected from unauthorized users. All the security issues are solved with the better secured firewall and router architecture in the network.

REFERENCES

[1] ISIUSC, "DARPA Internet Program Protocol specification", Information Sciences Institute University of Southern California,1981.

[2] M. Cooper and D. C. Yen. "IPv6: business applications and implementation concerns", Computer Standards and Interfaces, vol. 28, no. 1, pp. 27–41. July 2005.

[3] Redhwan M. A. Saad, Sureswaran Ramadass and Selvakumar Manickam, "A Study on Detecting ICMPv6 Flooding Attack based on IDS", Australian Journal of Basic and Applied Sciences, 7(2): 175-181, 2013,ISSN 1991-8178

[4] Varsha Alangar ,Anusha Swaminathan, "Ipv6 Security: Issue Of Anonymity", International Journal Of Engineering And Computer Science ISSN:2319-7242,Volume 2 Issue 8 August, 2013 Page No. 2486-2493.

[5] Rolf Oppliger, "Security at the Internet Layer",1998,IEEE.

[6] Emre Durda, Ali Buldu,"IPV4/IPV6 security and threat comparisons", Procedia Social and Behavioral Sciences 2 2010,Page No. 5285–5291