International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.08, March 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

IPv6 Security Features

Rajinder Singh

Department of Computer Science and Applications
Panjab University S.S.G. R.C. Hoshiarpur Punjab, India

ABSTRACT

Nowadays Internet Protocol (IP) is used successfully on the internet. It is a very important protocol. The main task of this protocol is to identify individual hosts on the network through logical addresses. There are two versions of internet protocol, IPv4 (Internet protocol version 4) and IPv6 (Internet protocol version 6). In this paper a c study of security features of IPv6 has been made.

Keywords: Internet Protocol; DOS, MITM, IPv4, IPv6, IPSec;

I. INTRODUCTION

In computer networks, Internet Protocol (IP) is the mail protocol used for exchanging communication messages between the nodes. Messages are exchanged with the help of datagrams. It is used to identify each host on the network. But in case of IPv4 very little attention was given to security of data of the users. This protocol does not support built in security protocols. Therefore, it does not guarantee the security of the data transferred between the various users. There are many advantages of IPv6 over IPv4[1] .

II. MAIN BENEFITS OF IPV6

a) Efficient Routing
In case of IPv6 size of routing tables is small and routing is more efficient and hierarchical.
b) Efficient Packet Processing
IPv6's packet header is very simple so it is processed more efficiently. There is no check sum so it is not processed at every intermediate nodes.
c) Simple Network Configuration
IPv6 supports auto configuration of address.
d) Support For New Services
Ipv6 also support new and valuable services.
e)Security

IPSec protocol is used for the security purposes [15].

III. MAIN SECURITY THREATS IN IPV4

According to [2] [3] main security threats that can be made in IPv4 are:

i) Denial of Service attack (DOS)

In denial-of-service attack is an attacker prevents legitimate users from accessing targeted computer systems or other type of resources. Here the main focus of the attacker is to deny network resources. Network resources are unavailable to its legitimate users. This is done by flooding the network with a lot of packets. For example Ping of Death and Teardrop Attacks. [4][16].

ii) Man In the Middle Attack (MITM)

AIn case of man-in-the-middle (MITM) attack communication between two users can be monitored and can be modified by an unauthorized user. In case of IPv4 there is no proper mechanism for authentication.. So attackers take this to lead MITM attack. In this type of attack an attacker can monitor and alter messages. In this, the two original nodes appear to communicate normally[5][16].

iii) Fragmentation Attack

Fragmentation attacks is a denial of service type attack, in which an attacker exploiting datagram fragmentation mechanisms. Fragmentationis a process of breaking down an IP datagram. Attackers have used a lot of fragmentation methods to cause a denial of service attack to network. Examples of fragmentation attack are i) The teardrop Attack ii) The Overlapping Fragment Attack [6].

To avoid this type of attack users can use various firewalls.

iv) ARP poisoning Attack

ARP Poisoning is a type of attack which is carried over a Local Area Network (LAN). In this attack, the attacker sends fake ARP messages to a network. This is done by changing the Media Access Control (MAC) address and then attacking the network with forged request and reply packets [7][16].

vii) Viruses/Worms

Mainly these are application layer threats. These consist of malicious code or these may consist of malicious programs. This threat can be avoided by using appropriate antivirus and timely updating them [2].

IV. MAIN SECURITY THREATS IN IPV6

Many IPv4 threats are common to IPv6. Main attacks which are common to both ipv6 and ipv4 are: Sniffing, Application Layer Attacks, Rogue Devices, Man-in-the-Middle Attacks (MITM), and Flooding attacks[8].

V. IPSEC PROTOCOL

Main purpose of IPSec protocol are a) data authentication b) integrity c) confidentiality. In IPSec protocol security is provided at the IP packet level [10].

IPv6 allows using of IPSec. IPSec protocol uses Authentication Headers (AH), Encapsulating Security Payloads (ESP) and Security Associations (SA) features to perform various security related activities. IPSec is used to provide data integrity, authentication and data confidentiality.

This protocol is optional in case of IPv4 but in case of IPv6 it is mandatory. Authentication Headers (AH) provide integrity and data authentication for all the IP Packets. ESP provides confidentiality by hiding the packet contents through various encryption schemes. The IPSec protocol uses the concept of a security association. Security Association means that the two devices will communicate securely [11][12][13][14].

VI. CONCLUSIONS

As compared to IPv4, IPv6 represents a big step relted to security. IPSec uses Authentication Headers (AH), Encapsulating Security Payloads (ESP) and Security Associations (SA) to perform security. It is used to provide data integrity, authentication and data confidentiality. It is optional in case of IPv4, but it is mandatory in IPv6.

REFERENCES

[1 https://www.techopedia.com/definition/5366/internet-protocol-ip

[2] http://www.ukessays.com/essays/computer-science/ipv4-internet-protocol-security-features-computer-science-essay.php

[3] Convery, Sean, and Darrin Miller. "IPv6 and IPv4 threat comparison and best-practice evaluation." (2004).

[4] http://en.wikipedia.org/wiki/Denial-of-service_attack

[5] http://en.wikipedia.org/wiki/Man-in-the-middle_attack

[6] https://www.incapsula.com/ddos/attack-glossary/ip-fragmentation-attack-teardrop.html

[7] http://www.techopedia.com/definition/27471/address-resolution-protocol-poisoning-arp- poisoning

[8] http://security.stackexchange.com/questions/377/what-are-the-security-risks-in-enabling-ipv6

[9] http://www.tcpipguide.com/free/t_IPSecurityIPSecProtocols.htm

[10] http://documentation.netgear.com/reference/enu/vpn/VPNBasics-3-02.html

[11] https://en.wikipedia.org/wiki/IPsec

[12] http://www.tcpipguide.com/free/t_IPSecAuthenticationHeaderAH.htm

[13] http://www.tcpipguide.com/free/t_IPSecEncapsulatingSecurityPayloadESP.htm

[14] http://www.ciscopress.com/articles/article.asp?p=24833&seqNum=7

[15] https://www.networkcomputing.com/networking/six-benefits-ipv6/1148014746

[16]http://resources.infosecinstitute.com/ipv6-security-overview-a-small-view-of-the-future/#gref