Volume 5, Issue 7, July 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Comparison of Security Features of IPv4 and IPv6

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

Abstract—Internet Protocol (IP) is widely used on the internet. It is one of the important protocols in TCP/IP protocol suite. It is used to identify each host on the network through logical addresses. Nowadays there are two versions of internet protocol, IPv4 (Internet protocol version 4) and IPv6 (Internet protocol version 6). IPv6 is the latest (sixth) revision to the Internet Protocol and it is the successor to IPv4. In this paper a comparative study of security features of both IPv4 and IPv6 has been made.

Keywords: Internet Protocol; IPv4; IPv6; IPSec;

I. INTRODUCTION

In computer networks Internet Protocol (IP) is widely used on the internet. It is one of the major protocols in TCP/IP protocol suite which is widely used to identify each host on the network through logical addresses. Internet protocol is used for transferring packets across the network. Initially IPv4 was created for delivering data across the network and very little attention was given to security of data across the network. IPv4 is the widely used to connect various internet devices to the Internet. Internet Protocol IPv4 does not have a built in security protocol. Since it has not built in security features so many security threats can be made in IPv4. IPv6 (Internet Protocol Version 6) is successor to IPv4. Main reason for development of IPv6 was to deal with the problem of IPv4 address exhaustion.
Main Advantages of IPv6 over Ipv4 are:
i) Larger Address Space ii) No Network Address Translation iii) Auto-configuration iv) Better multicast routing v) Simple header format vi) Simple and more efficient routing vii) True quality of service (QoS) viii) Built-in authentication and privacy support [1].

II. MAIN SECURITY THREATS IN IPV4

IPv4 has no or very little security features and in IPv4 security is dependent within the applications.
According to [2] [3] main security threats that can be made in IPv4 are:

i) Denial of Service attack (DOS)
Here main focus of the attacker is to deny either computer resources present on the network or deny network resources. With this threat network resources are made unavailable to its legitimate users by flooding the network with useless packets. Some examples of DOS attacks are Ping of Death and Teardrop Attacks. In case of ping of death attack an attacker deliberately sends an IP packet larger than the 65,536 bytes allowed by the IP protocol. Some of the resources which are affected by DOS attacks are CPU and network's bandwidth [4].

ii) Man In the Middle Attack (MITM)
There is no proper mechanism for authentication in IPv4. So this can lead MITM attack. In this type of attack an attacker can monitor, alter or inject messages into a communication channel. Attacker can intercept, send and receive data which is meant for someone else [5].

iii) Fragmentation Attack
Fragmentation means process of breaking down an IP datagram into smaller packets, sending them over different types of networks and then reassembling them at the other end. Attackers have used fragmentation in many ways to cause a denial of service attack to network. Some common examples of fragmentation attack are i) The teardrop Attack ii) The Overlapping Fragment Attack [6].
To avoid this threat user can use various firewalls and IDS in IPv4 for reassembly of the fragments.

iv) ARP poisoning Attack
In Address Resolution Protocol poisoning attack attacker sends fake or spoofed ARP messages to a network. An attacker changes the Media Access Control (MAC) address and attacks the network with forged ARP request and reply packets. Because of forged ARP replies the victim computer unintentionally sends the frames to the hacker's computer. As a result user's data as well as privacy are compromised [7].

© 2015, IJARCSSE All Rights Reserved

vii) Viruses/Worms

These are application layer threats. These consist of malicious code/programs and they can propagate themselves across the network from one infected or compromised computer to another. Main reason is the small address space of IPv4. This threat can be avoided by using host antivirus and timely updating host operating system [2].

viii) Port scanning

With this threat attacker scan for multiple listening ports on a victim computer. After identifying Open ports on the victim computer they can be used to exploit the specific hosts further. Because of the small address space in IPv4, port scanning is easy in IPv4 architecture [2].

ix) Routing Attacks

Routing attacks is used to disturbing the traffic flow in the network or redirecting traffic flow in a network. In IPv4, routing protocols use cryptographic algorithms to secure the routing announcements between peers.

III. MAIN SECURITY THREATS IN IPV6

Many security threats which are common to IPv4 are also common to IPv6. Main attacks which are common to both ipv6 and ipv4 are:

Sniffing: Without IPSec , sniffing attack can easily made on IPv6 similar like IPv4.

Application Layer Attacks: This type of attack is also possible in IPv6 even with the presence of IPsec protocol.

Rogue Devices: Rogue devices insertion is also very easy in IPv6 as in IPv4.

Man-in-the-Middle Attacks (MITM): Without IPSec protocol Man in the Middle Attack is as easier as in IPv4 to implement. Many other attacks utilizing MITM in IPv4 are also possible in IPv6 without using IPSec.

Flooding: Flooding attacks are very much similar in IPv4 and IPv6 [8].

IV. IPSEC PROTOCOL

One major disadvantage of the IPV4 is that it lacks any mechanism for ensuring authenticity and privacy of the data which is passed across the network. Since IP packets are routed between two host over unknown networks so they can be intercepted and modified also. So security enhancements were needed for IP packets over the network. That was the main reason that IPSec was developed [9].

So main purpose of IPSec protocol is that it provides data authentication, integrity, and confidentiality when the data packets are transferred across IP networks. IPSec protocol provides data security at the IP packet level [10]. IPSec can be used to provide data security between two hosts, between a pair of gateways, or between a security gateway and a host [11].

Main features of IPSec:

Security architecture

The IPSec suite consists of following protocols.

a) Authentication Headers (AH)
b) Encapsulating Security Payloads (ESP)
c) Security Associations (SA)

a) Authentication Headers (AH)

Authentication Headers (AH) provide integrity and data authentication for IP Packets passed across the network.

Authentication Headers (AH) can also protect against replay attacks by using the sliding window technique [11].

Authentication is achieved by using a special hashing algorithm and a specific key only known to source and the destination. If any part of the packet is changed during transmission across the network it can be detected by the receiver because key is known to only sender and receiver [12].

b) Encapsulating Security Payloads (ESP)

The Authentication Header (AH) protocol provides only authentication, but this protocol cannot protect reading the contents of packets, and this is done through Encapsulating Security Payloads. ESP provides confidentiality by hiding the packet contents through various encryption schemes. It provides security to data by encryption. An encryption algorithm encrypts the data in the datagram with a key, and then transmits this encrypted data to the destination which then decrypts it [13].

c) Security Associations (SA)

The IPSec protocol uses the concept of a security association. Security Association means how the two devices will communicate securely using security services.

IPSec protocol has many options for performing network encryption and authentication. Main algorithms used by IPSec are DES, 3DES for encryption purpose and MD5 or SHA for integrity purpose [14].

V. CONCLUSIONS

IPSec protocol is used to secure the communication between the nodes on network. IPSec uses Authentication Headers (AH), Encapsulating Security Payloads (ESP) and Security Associations (SA) to perform various

© 2015, IJARCSSE All Rights Reserved

security related functions. This suite of protocols in IPSec is used to provide data integrity, authentication and data confidentiality. This protocol is optional in case of IPv4. But this protocol is mandatory in IPv6.

REFERENCES

[1] http://www.webopedia.com/DidYouKnow/Internet/ipv6_ipv4_difference.html
[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] http://www.ouah.org/fragma.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

© 2015, IJARCSSE All Rights Reserved