Network and Complex Systems
ISSN 2224-610X (Paper) ISSN 2225-0603 (Online)
Vol 2, No.4, 2012

Look at IPV6 Security advantages over IPV4

Mansour A. Abu Sameeha*
Princess Rahmah College, Balqa Applied University, Jordan -Salt, PO box 19117, Jordan
* E-mail of the corresponding author: Mansour_153@yahoo.com

Abstract

Due to the increase of internet usage especially in homes, offices and there will be many devices that will use the new 3G/4G technologies ,so Internet address exhaustion will be raised to serious problem gradually. Now days, the IPv4 address shortage problem has been solved incompletely using NAT (Network Address Translation) anyway, the changeover to IPV6 address will be accelerated because of advantages such as mobility, QoS etc.., .we here show some of the improvements associated with the Internet Protocol version 6, with an emphasis on its security-related functionality

.

Keywords: IPV6 security, security, addressing, IP threats; IP attacks.

1. Introduction

Ipv6 (Internet Protocol version 6) is a network layer that is utilized by packet-switched internet worked applications. The protocol is the successor to IPv4 and is used for Internet based general applications. And it was made-up due to the need of large address space, hence IPv4 uses a 32-bit address space, in which can accommodate about 4 billion unique addresses. But, the practical number of usable addresses is actually much lower. The current Internet has grown much bigger than was anticipated. There are several problems such as impending exhaustion of the IPv4 address space, configuration and complexities and poor security at the IP level. Today, however, that amount is insufficient, even more if we consider emerging new technologies such as 3G/4G wireless devices and other wireless appliances [1].

To overcome these concerns, in the early 90's, IETF (Internet Engineering Task Force (IETF), began developing a new IP protocol namely IPv6 (other name, Next Generation IP, IPng), with this new addressing scheme.

1.1 IPV6 HEADER

The IPv6 header itself is always exactly 40 bytes, and contains exactly 8 fields. Unlike the IPv4 header, the IPv6 header cannot vary in size. The figure1 below shows the header in IPV4 and IPV6 [2]. The checksum field was simply dropped; all checksum computations in IPv6 must carry out by upper-layer protocols like TCP and UDP. The fragment fields, which appear in the IPv4 header, were dropped from the main IPv6 header. Fragment information was relegated to an extension header. In addition, IPv6 routers are not allowed to fragment packets they forward; only the original sender of an IPv6 packet is permitted to break the packet into fragments. This has significant implications for network security because ICMP control packets that support path maximum transmission unit (MTU) discovery must be permitted through all IPv6 networks [3].

The functionality provided by the "Time to Live" field has been replaced with the "Hop Limit" field. The "Protocol" field has been replaced with the "Next Header Type" field. The "Options" field is no longer part of the header as it was in IPv4. Options are specified in the optional IPv6 Extension Headers. The removal of the options field from the header provides for more efficient routing; only the information that is needed by a router needs to be processed [4]

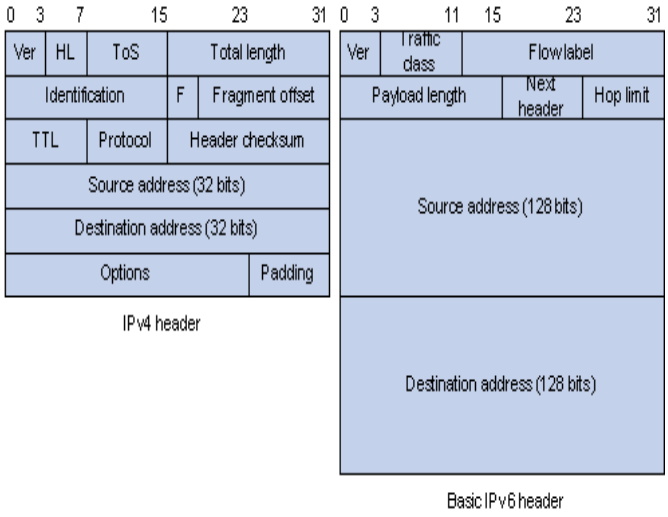

Figure1: IPV4 and IPV6 header

2. Type of attacks that was in IPV4

2.1 Overview

The following attacks have substantial differences when moved to an IPv6 world. In some cases the attacks are easier, in some cases more difficult, and in others only the method changes:

Reconnaissance: In this attack the adversary attempts to learn as much as possible about the victim network, this includes both active network methods such as scanning as well as more passive data mining such as through search engines or public documents.[5]

Header manipulation and fragmentation: This of attack has been primarily used for one of two purposes. The first purpose is to use fragmentation as a means to evade network security devices, such as NIDS or stateful firewalls. The second purpose of the attack is to use fragmentation or other header manipulation to attack the networking infrastructure directly.

Layer 3 and Layer 4 spoofing: A key element enabling numerous different types of IP attacks is the ability for an adversary to modify their source IP address and the ports they are communicating on to appear as though traffic initiated from another location or another application. This so-called “spoofing” attack is prevalent despite the presence of best practices to mitigate the usefulness of the attack. .

Address Resolution Protocol (ARP) and Dynamic Host Configuration Protocol (DHCP) attacks: In ARP Poisoning, forged ARP request and reply packets are used to update the target computer's ARP cache. The target computer is being fooled into believing that the attacker computer (which has a totally different MAC and IP address) as the computer that has the desired IP address with a specific MAC address. Thus, the attacker can monitor the packet sent by the target computer to the original destination since it is sent to the attacker's computer request before they are sent to the original destination [6].

Broadcast amplification attacks (smurf): In which attack certain services are flooded with a large amount of illegitimate requests that render the targeted system unreachable by legitimate users, which causes a DoS attack. [7]

3. IPV6 security issues

3.1 Address Space:

The most obvious distinguishing feature of IPv6 is its use of much larger adresses. The size of an address in IPv6 is 128 bits, a bit-string that is four times longer than the 32-bit IPv4 address. A 32-bit address space allows for 232, or 4,294,967,296, possible addresses. A 128-bit address space allows for 2128, or 340,282,366,920,938,463,463,374,607,431,768,211,456 possible addresses.[8]

The new features introduced with the IPv6 protocol can be summarized as:

1. A new header format.

2. A much larger address space (128-bit in IPv6, compared to the 32-bit address space in IPv4)

3. An efficient and hierarchical addressing and routing infrastructure.

4. Both stateless and stateful address configuration.

5. IP Security.

6. Better Quality of Service (QoS) support .

7. A new protocol for neighboring node interaction.

8. Extensibility. [9]
These enhancements in IPv6 provide better security in certain areas, but some of these areas are still open to exploitation by attackers.

3.2 Security analysis at IPV6.

IPv6 was designed to protect data. Unreasonably, its deployment may sometimes lead to decreasing security level, especially in the transformation period. The operating system vendors long ago started to support IPv6 in their products. Nevertheless interoperability and compatibility tests [10] of IPv6 implementations show some implementation problems

3.3 Dealing with threats:

IPv6 security is in many ways the same as IPv4[11] security. The basic mechanisms for transporting packets across the network stay mostly unchanged, and the upper-layer protocols that transport the actual application data are mostly unaffected. Mandates the inclusion of IP Security (IPSec) [12], it has often been stated that IPv6 is more secure than IPv4.

3.3.1 Reconnaissance, In IPv4 the adversary has several well-established methods of collecting this information:
Ping sweeps—By determining the IPv4 addresses in use at an organization (through active probes)

Port scans - after identifying reachable systems, the adversary can systematically probe these systems on any number of Layer 4 ports to find services both active and reachable. By discovering hosts with active services, the adversary can then move to the next phase

Application and vulnerability scans - The adversary can then probe these active ports by various means to determine the operating system and the version numbers of applications running on the hosts, and even test for the presence of certain well-known vulnerabilities.

IPV6 reconnaissance is different from IPv4 reconnaissance in two major ways:
The first is that the ping sweep or port scan, when used to enumerate the hosts on a subnet, are much more difficult to complete in an IPv6 network according to the huge number of probable address range that it will scan.
The second is that new multicast addresses in IPv6 enable an adversary to find a certain set of key systems (routers, Network Time Protocol [NTP] servers, and so on) more easily. Beyond these two differences, reconnaissance techniques in IPv6 are the same as in IPv4. Additionally, IPv6 networks are even more dependent on ICMPv6 to function properly. Aggressive filtering of ICMPv6 can have negative effects on network functions.

3.3.2 Header manipulation and fragmentation:

In IPv4 fragmentation is a technique used to fit the IPv4 datagram into the smallest MTU on the path between end hosts. IPv4 fragmentation has been used as a technique to bypass access controls on devices such as routers and firewalls. Fragmentation also has been used to obfuscate attacks in order to bypass network security monitoring products such as NIDS. [13].

IPv6 fragmentation by intermediary devices is prohibited per RFC 2460. One of the most common fragmentation attacks uses overlapping fragments to obfuscate attacks from IPv4 security devices.

In IPv6, overlapping fragments is not a proper way of handling fragmentation based on the rules outlined in RFC 2460; these fragments can possibly be viewed as an attack and dropped. Additionally, if the overlapping packets are allowed to bypass the security device, several end-host operating systems drop overlapping fragments in their IPv6 stack software. [14]

3.3.3 Layer 3 and Layer 4 spoofing, IPv4, spoofing attacks (principally Layer 3-based) occur daily. They can make DoS, spam, and worm or virus attacks more difficult to track down. Layer 3 spoofing attacks are not generally used in interactive attacks as return traffic routes to the spoofed location, requiring the adversary to "guess" what the return traffic contains (not an easy proposition for TCP-based attacks because TCP has 32-bit sequence numbers). Layer 4 spoofing can be used in interactive attacks in order to make traffic appear to come from a location it did not (such as injecting false Simple Network Management Protocol (SNMP) messages or syslog entries). [15] Specifies methods to implement ingress filtering to prevent spoofed Layer 3 traffic at its origin. Unfortunately such filtering is not broadly implemented, and because it requires widespread usage to have a significant benefit, spoofed traffic is still very common. It is important to note that ensures that only the network portion of an address is not spoofed, not the host portion. So in the 24-bit subnet 192.0.2.0/24, RFC 2827 filtering ensures that traffic originating from 192.0.3.0 is dropped but does not stop an adversary from spoofing all the hosts within the 192.0.2.0/24 subnet assigned to a broadcast domain.

In IPV6 One of the most promising benefits of IPv6 from a Layer 3 spoofing perspective is the globally aggregated nature of IPv6 addresses. Unlike IPv4, the IPv6 allocations are set up in such a way as to easily be summarized at different points in the network. This allows filtering to be put in place by Internet service providers (ISPs) to ensure that at least their own customers are not spoofing outside their own ranges. Layer 4 spoofing attacks are not changed in any way, because Layer 4 protocols do not change in IPv6 with regard to spoofing. [16]

3.3.4 Address Resolution Protocol (ARP) and Dynamic Host Configuration Protocol (DHCP) attacks. Address Resolution Protocol (ARP) [17] is used to map the IP addresses onto the data link layer MAC address. In ipv6 Replacing ARP by Neighbor Discovery (ND) Protocol in the IPv4 protocol, a layer two (L2) address is not statically bound to a layer three (L3) IP address. Therefore, it can run on top of any L2 media without making significant change to the protocol. Connection between L2 and L3 addresses is established with a protocol named Address Resolution Protocol (ARP), which dynamically establishes mapping between L2 and L3 addresses on the local network segment. ARP has its own security vulnerabilities (such as ARP Spoofing). In the IPv6 protocol, there is no need for ARP because the interface identifier (ID) portion of an L3 IPv6 address is directly derived from a device-specific L2 address (MAC Address). The L3 IPv6 address, together with its locally derived interface ID portion, is then used at the global level across the whole IPv6 network. As a result, the security issues related to ARP no longer apply to IPv6. A new protocol called Neighbor Discovery (ND) Protocol for IPv6 as a replacement to ARP.[18]

4. IPSEC

4.1 Introduction.

it is important to note that IPv6 is not necessarily more secure than IPv4. In fact, IPv6 approach to security is only marginally better than IPv4 but not radically new [19]. IPv4 also offers IPSec support. However, IPv4's support for IPSec is optional. By contrast, it is mandatory for IPv6 to use IPSec in all nodes [20] [21].

4.2 Header manipulation and fragmentation

The AH [22] provides connectionless integrity and data origin authentication for IP data grams, and provides protection against replay attacks. AH provides authentication for as much of the IP header as possible, as well as for upper level protocol data. However, some IP header fields may change en route and so the value of these fields upon receipt may not be predictable by the sender. Consequently, such fields are not afforded AH protection. AH may be applied alone, in combination with ESP, or in a nested fashion using tunnel mode. AH and ESP [23] headers are being modified along the following guidelines:

The AH format is substantially changing to accommodate new and stronger authentication algorithms (HMAC) [24] that support prevention of packet replay and cancellation.

The ESP specification is only marginally changing to achieve a better orthogonally with algorithms, to simplify application of different encryption algorithms. The net benefit of these changes will be that more security will be available at the network level; hence, applications will be able to concentrate on different security aspects, such as authorizations and no repudiation. The authentication header prevents IP packets from being tampered or altered. In a typical IPv4 packet, the AH is part of the payload. [25].

4.3 Encrypted Security Payload (ESP)

The Encrypted Security Payload, which is one of the general extension headers defined in IPv6, The ESP header provides a variety of security services for IP. ESP may be applied alone or in a combination with AH. Alternatively, with tunnel mode, ESP can provide confidentiality, non-repudiation, connectionless integrity, replay protection and traffic- flow confidentiality .it consists of an integer number of 32-bit blocks, with the first one containing the SPI to select the SA to be used in decrypting all other blocks in the packet. The exact format of the encrypted part depends on the encryption algorithm used. The default encryption technique in IPv6 is DES-CBC[26], which is the DES algorithm applied in Cipher Block Chaining (CBC) mode. DES is a private key encryption algorithm that is normally applied to 64-bit data blocks with a 56-bit key (extended to 64 bits by adding one parity bit for each 7 bits of the key). Various techniques have been proposed to apply the DES transformation to blocks bigger than 64 bits. The CBC mode divides the data stream into a sequence of 64-bit blocks.

4.4 IKE protocol

The IKE protocol [27] is a sophisticated key exchange and management system, which is included in the IPSec protocol suite to provide secure key distribution services between parties wishing to communicate over an un trusted network. IKE is a hybrid protocol composed of features from the Internet Security Association and Key Management Protocol (ISAKMP) [28], Oakley [29] and the Secure Key Exchange Mechanism (SKEME) [30]. IKE uses parts of Oakley and SKEME in conjunction with ISAKMP to obtain authenticated keying material for security associations such as AH and ESP for IPSec.

4.5 IPSec Security Associations (SAs)

An SA is an agreement between two parties on the methods they will employ to support secure communication. This agreement is reached upon the completion of a negotiation phase that discerns the common features supported by the potentially different implementations at each end. Security services are afforded to an IPSec SA using AH or ESP, but not both. Therefore, if both AH and ESP protection is to be applied to a traffic stream, then two or more SAs must be created in order to afford the desired protection. To secure typical, bi-directional communication between two hosts or security gateways, two SAs are required; one in each direction, as SAs are uni-directional, there are two types of security associations defined for IPSec:

Transport mode. A transport mode SA is an agreement between two hosts. In the case of ESP, a transport mode SA provides security services only for higher layer protocols, not for the IP header or any extension headers preceding the ESP header. In the case of AH, the protection is also extended to specific portions of the IP header and any extension headers Tunnel mode. A tunnel mode security association is essentially a transport mode SA that is applied

to an IP tunnel. This mode is required whenever a security association ends at a security gateway3, in order to avoid IPSec packet fragmentation and reassembly, and in situations where multiple paths to the same destination behind the security gateways exist. Two hosts may optionally establish a tunnel mode SA if increased security is required.

If AH is employed in tunnel mode, portions of the outer IP header are afforded protection, as well as all of the encapsulated IP packet. If ESP is employed, protection is afforded only to the tunneled packet, not to the outer header.

Conclusion

This paper discussed the brief introduction of IPv6-to-IPv4 and their comparison. Ipv6 provides a sizeable address space in addition to the use of encrypted communication, this does not mean that ipv6 solves all the old security issues related to ipv4, but the improvement is noticeable, some of the old threats related to ipv4 should be taken in consideration when using the ipv6.

REFERENCES

[1] Davies, J., Understanding IPv6, Microsoft Press,Redmond, WA, 2003.

[2] S Deering, R Hinden, "Internet Protocol, Version 6 (IPv6) Specification" (December 1998), RFC 2460 at http://www.ietf.org/rfc/rfc2460.txt

[3] Ziring N. (May 2006). Router Security Configuration Guide Supplement - Security for IPv6 Routers. [Online]. Available: www.nsa.gov/ia/_files/routers/I33-002R-06.pdf

[4] Hermann,P.-Seton (2002).Security Features in IPv6. [Online]. Available:www.sans.org/reading_room/whitepapers/.../security_features_in_ipv6_380

[5]Sean Convery& Darrin Miller IPv6 and IPv4 Threat Comparison and Best-Practice Evaluation (v1.0), Cisco Press, , 2004.

[6] C. Nachreiner, Anatomy of an ARP Poisoning At-tack, Washington, USA,2003.(http://www.watch-uard.com/infocenter/editorial/135324.asp)

[7] Campbell, P.; Calvert, B.; Boswell, S., Security+Guide to Network Security Fundamental, Thomson,Canada, 2003.

[8] Popoviciu C.; Levy-Avegnoli, E.; Grossetete, P.,Deploying IPv6 Networks, Cisco Press, Indianapolis, IN,2006

[9] http://tools.ietf.org/html/rfc2460 3 http://tools.ietf.org/html/rfc48614 http://tools.ietf.org/html/rfc4862

[10] TAHI Project. Test and Verification for IPv6, http://www.tahi.org, (last access 7.03.2011).

[11] J Postel, "Internet Protocol, DARPA Internet Program Protocol Specification" (September 1981), RFC 0791 at http://www.ietf.org/rfc/rfc0791.txt

[12] S Kent, R Atkinson, "Security Architecture for the Internet Protocol" (November 1998), RFC 2401 at http://www.ietf.org/rfc/rfc2401.txt