International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 11
July 2016

IPV6 Vulnerabilities to Web Server Integration in Network Environment

AMADI E.C., MBAGWU C. P., MBAMARA H., ASORONYE C. P.

Department Of Information Management Technology Federal University Of Technology Owerri

emmanuel.amadi@gmail.com

ABSTRACT

One of the main purposes of Internet Protocol version 6 (IPv6) developments was to solve the IP address depletion concern due to the burgeoning growth of the Internet users. The new Internet protocol provides end-to-end communication, enhanced security and extensibility apart from the other features such as address auto-configuration or plug-and-play and faster packet processing in the routers. However, as a new technology, it is also reported that the protocol introduces some security. This paper reviews IPv6 security vulnerabilities that have large potential exploitation. The IPv6 security vulnerabilities are classified under three categories that include the IPv6 main header field, IPv6 extension header and Neighbor Discovery Protocol (NDP). This paper also summarizes the current mitigation methods proposed by researchers and practitioners to secure from these IPv6 security vulnerabilities in network environment.

KEYWORDS

Protocol, IP, IPv6, IPv6 Security Vulnerabilities

INTRODUCTION

IPv6 stands for Internet Protocol version 6 also known as Ipng (IP next generation) is the second version of the Internet Protocol to be used generally across the virtual world. The first version was IPv4. IPng was designed to take an evolutionary step from IPv4. It was not a design goal to take a radical step away from IPv4. Functions which work in IPv4 were kept in IPng, functions which didn't work were removed.

The Internet operates by transferring data between hosts in packets that are routed across networks as specified by routing protocols. These packets require an addressing scheme, such as IPv4 or IPv6, to specify their source and destination addresses. Each host, computer or other device on the Internet requires an IP address in order to communicate. The growth of the Internet has created a need for more addresses than are possible with IPv4.

Like IPv4, IPv6 is an internet-layer protocol for packet switched internetworking and provides end-to-end datagram transmission across multiple IP networks. While IPv4 allows 32 bits for an IP address, and therefore has 2^{32} (4 294 967 296)

possible addresses, IPv6 uses 128-bit addresses, for an address space of 2^{128} (approximately 3.4×10^{38}) addresses. This expansion allows for many more devices and users on the internet as well as extra flexibility in allocating addresses and efficiency for routing traffic. It also eliminates the primary need for network address translation (NAT), which gained widespread deployment as an effort to alleviate IPv4 address exhaustion. Amer Nizar Abu Ali, (2012).

1 OVERVIEW OF IPv6 PROTOCOL

The internet, in very broad terms, is a connected network of networks which comprises billions of devices, including personal computers, mobile phones, switches, routers and many other end user or intermediary nodes. The growing number of internet-enabled appliances has reached a scale at which the current network infrastructure and its underlying protocols, such as IPv4, were never expected to work when they were designed. Today even some household devices are able to connect to the internet and have something in common with all other high-tech devices such as PCs and smart phones; they require an Internet Protocol (IP) address to operate and get connected to the internet.

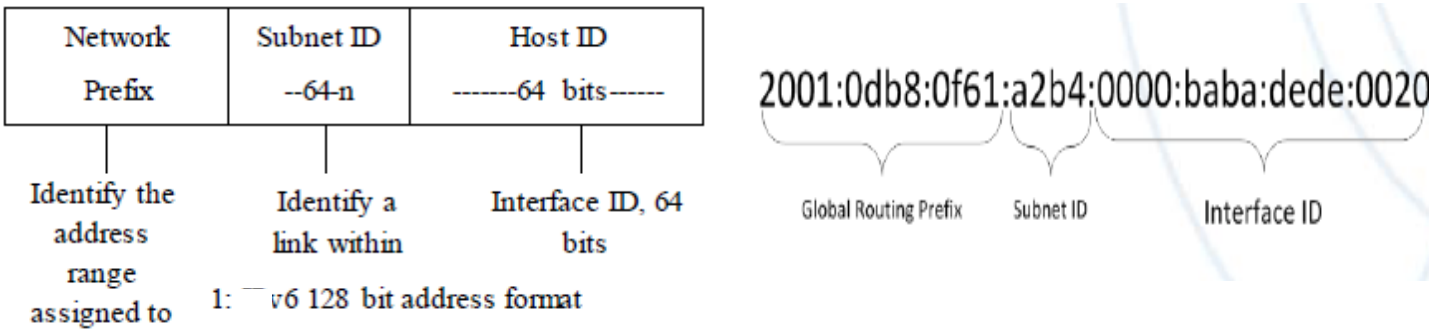
One of the main reasons behind creation of IPv6 is related to IPv4's scarce IP space. IPv4 uses a 32-bit address space which can be used to assign 4,294,967,296 unique addresses. Today, 2.7 billion people are connected to the internet and there are more than 10 billion internet-enabled devices in the world. This clearly shows why IPv4 addresses have run out. There are technical solutions such as Dynamic Host Configuration Protocol (DHCP) and Network Address Translation (NAT) which enable users to share public IP addresses in order to connect to the internet from an inner domain and thus circumvent the problem. Nevertheless, IPv4 routing is getting more complex every day. IPv6 uses a 128-bit address space which can accommodate up to $34x10^{37}$ IP addresses. Thus, it is reasonable to say that the IPv6 address space is more than enough for now and for the foreseeable future. This is one of main drivers behind the IPv6 shift and it can be summarized as 'scalability related improvements'. Emin Çalışkan, (2014).

3 .IPv6 PROTOCOL ARCHITECTURE

3.1 IPv6 ADDRESS FORMAT

IPv6 not only brings vast number of IP addresses which would enable numerous devices to have their own unique identifiers, it also has different peculiarities in terms of packet layout and underlying transmission techniques. IPv6 addresses are written in hexadecimal digits and divided into eight pairs of two byte blocks. The global routing prefix is a value which is assigned to a site and can be a cluster of subnets or links; the subnet ID is an identifier of a link within the site; and the Interface ID is being used to identify interfaces on a link.

FIG 1 : IPv6 Address Example (Emin Çalışkan, 2014)



3.2 IPv6 PACKET FORMAT

The format of IPv6 packet was standardized in RFC 2460 is depicted in Figure 2below. It consists of:

a. Fixed Main Header
b. Optional Extension Header and
c. Data from upper layer.

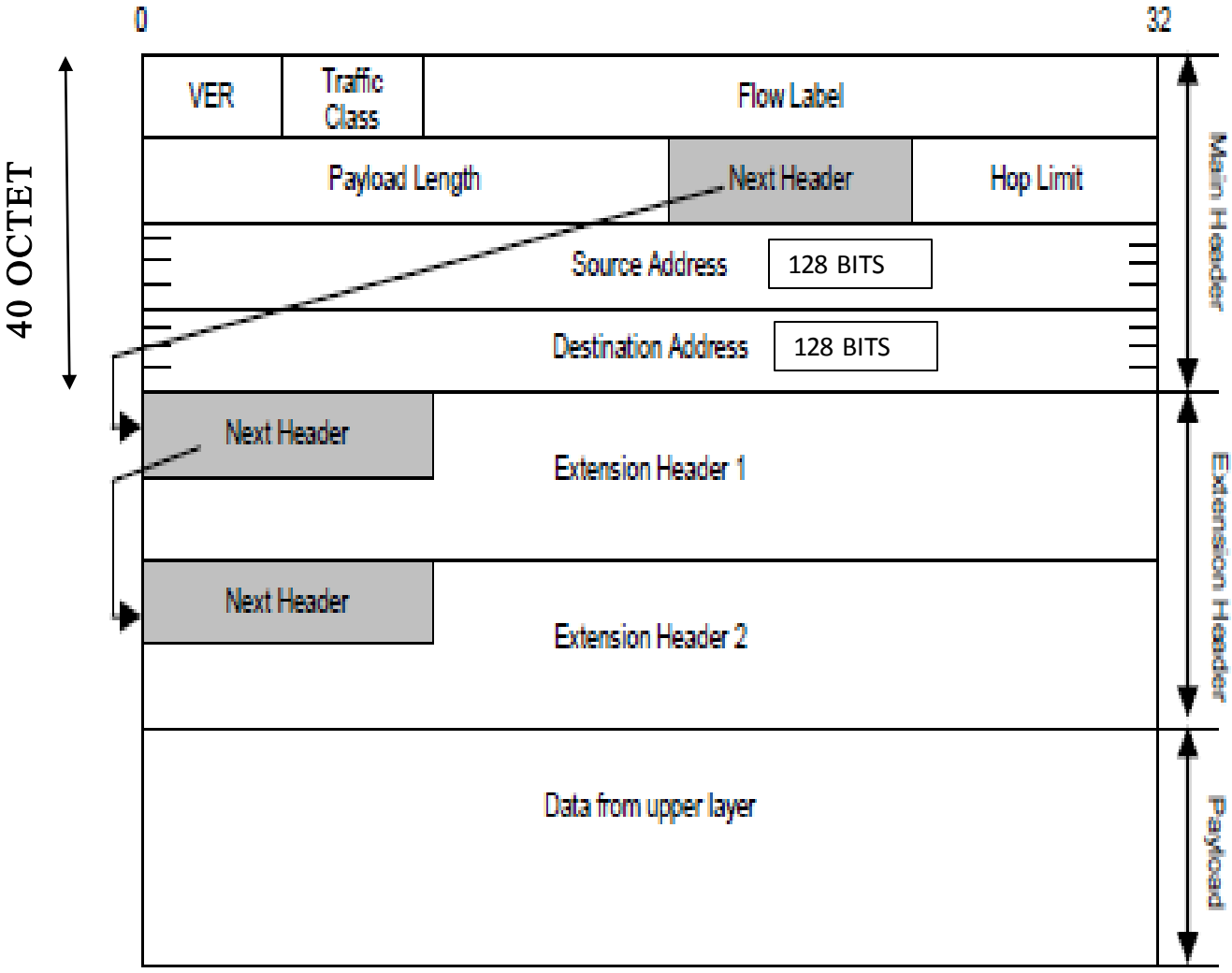


Fig 2: IPv6 Packet Format

SOURCE: International Journal of Network Security & Its Applications (IJNSA),Vol.4, No.6, November 2012.P(175).

3.21 MAIN HEADER

IPv6 main header is fixed 40 bytes that consists of 8 fields:

1. VER

Is Version field that indicates the protocol version. The field is 4 bits that has a value of 06.

2. Traffic Class

Is an 8 bits field that describes packet priority or its enlistment into a certain traffic class.

3. Flow label

Is a 20 bits field that contains information that helps a router to determine the handling of each packet in the flow quickly. This flow label is the only new field introduced in the IPv6 header.

4. Payload Length

Is a 16 bits field that carries the information on packet size including extension header. With 16 bits, it can identify the maximum length of a packet, 2^{16} or 65,535 bytes.

5. Next Header

Is an 8 bits field that defines either header or data type that follows the IPv6 main header.

The value of this field decreases by one each time a router forwards the packet.

6. Hop Limit

Is an 8 bits field defined in units of seconds, which defines the time limit within which the packet would be discarded.

7. Source Address

Is a 128 bits field that identifies the address of the source of the IPv6 packet.

8. Destination Address.

Is a 128 bit field that bears the address of the recipient of the IPv6 packet.

3.22 EXTENTION HEADER

IPv6 extension header is placed after destination address field before upper layer data and they are counted as part of IPv6 payload. In general, most extension headers are not required of processing in routers but each intermediate router must check for their existence and process them when present. They are:

1. Hop-by-Hop Options Header: used to specify delivery parameters at each hop on the path to the destination. It is identified by the value of 0 in the IPv6 Header's Next Header field.
2. Destination Option Header: used to specify packet delivery parameters for either intermediate or the final destination. It is identified by the value of 60 in the previous header's Next Header field
3. Routing Header: used by IPv6 source nodes to specify loos source route, a list of intermediate destination for packet to travel to on its path to the final destination. It is identified by the value of 43 in the previous header's Next Header field.
4. Fragment Header used for fragmentation and reassembly service. It is identified by the value of 44 in the previous header's Next Header field.
5. Authentication Header provides data authentication (verification of the node that sent the packet), data integrity (verification that the data was not modified in transit), and anti-replay protection (assurance that captured packets cannot be retransmitted and accepted as valid data) for IPv6 packet. This header is part of the security architecture for the IPv6.
6. Encapsulation Security Payload Header and Trailer provides data confidentiality, data authentication, and data integrity services to the encapsulated payload and entire IPv6 packet. ESP header and trailer is identified by the value of 50 in the previous header's Next header field.(http://www.microsoft.com/windows2000/docs/ipv6.doc

3.23 UPPER LAYER PROTOCOL DATA UNIT (PAYLOAD)

Is the combination of the IPv6 extension headers and the upper layer PDU. Normally it can be up to 65,535 bytes long. For example an ICMPv6 message, a UDP message or a TCP segment.

3.3 FEATURES OF IPv6

- **Expanded Addressing Capabilities.** IPv6 increases the IP address size from 32 bits to 128 bits and written as eight 16-bits fields in colon delimited hexadecimal notation. (e.g. fe80:43e3:9095:02e5:0216:cbff:feb2:7474). This new 128-bit address space provides a significant number of unique addresses, 2128 (or$3.4x10^{38}$) addresses, compared with IPv4's 232 (or $4.3x10^{9}$) addresses.
- **Auto Configuration**IPv6 enables plug-and-play networking, or **auto configuration**, which allows devices to configure themselves independently using a stateless protocol and to configure their IP addresses and other parameters without the need for a server. IPv6 host can get an IPv6 address automatically using two types of auto configuration mechanism, stateful address auto-configuration that uses Dynamic Host Configuration Protocol version 6 (DHCPv6) to generate IPv6 address for host and stateless address auto-configuration that includes generating a link local address and generating global addresses.

- **Simpler Header Structure**

  In comparison with IPv4, the IPv6 header is much simpler and has a fixed length of 40 bytes (as defined in RFC 2460). An IPv6

datagram has a structure that always includes a 40-byte base header and, optionally, one or more extension headers. This base header is similar to the header of an IPv4 datagram, though having a different format. Five IPv4 header fields have been removed: IP header length, identification, flags, fragment offset and header checksum. The IPv6header fields are as follows: Version (IP version 6); Traffic Class (replacing IPv4's type of service field); Flow Label (a new field for Quality of Service (QoS) management); Payload length (length of data following the fixed part of the IPv6 header), which can be up to 64KB in size in standard mode, or larger with a jumbo payload option; Next Header (replacing IPv4's protocol field); Hop Limit (number of hops); and Source and Destination addresses.

- **Extension Headers**
  Extension headers are defined in RFC 2460 to indicate the transport layer information of the packet (TCP or UDP) or extend the functionality of the protocol. Extension headers are identified with the Next Header field within the IPv6 header, which identifies the header following the IPv6header. These optional headers indicate what type of information follows the IPv6 header in the formation of the packet. Extension headers are a sequential list of optional headers, which can be combined. Several appear in a single packet, but only a few are used in combination.

- **Protocol Security (IPsec).** IP Security, or IPsec for short, provides interoperable, high quality and cryptographically based security services for traffic at the IP layer. IPsec is a framework for securing Internet Protocol (IP) communications by authenticating the sender and thus provides integrity protection plus optionally confidentiality for transmitted data. IPsec is a mandatory part of an IPv6 implementation; however, its use is not required. IPsec is also specified for securing particular IPv6 protocols, such as Mobile IPv6 and Open Shortest Path First version 3 (OSPFv3).

  It basically uses the cryptographic security services for protection or authentication and encrypts each IP packet of a communication session. These can be either between a pair of nodes, or between a pair of security gateways or between a security gateway and a node.

4. IPv6 VUNERABILITIES

Although IPv6 both simplifies and improves IPv4, it poses several significant security challenges and also some of these features of IPv6 pose as vulnerabilities to security of web servers in network environment. These vulnerabilities will be treated below under sub heads below.

4.1 LARGE ADDRESS SPACE

Port scanning is one of the most common techniques in use today. Port scanning allows "black-hats" to listen to specific services (ports) that could be associated to well-known vulnerabilities. In IPv6 networks, IPv6 subnets use 64 bits for allocating host addresses. Scanning such a large address space (264) is not absolutely impossible. The hacker community has started exploring IPv6, and they are constructing tools that leverage weaknesses, back doors and bypass firewalls in the protocol. In fact, IPv6 capabilities have started to be added to several popular hacker tools. Many of these IPv6 attack tools are already available and relatively easy to install and operate. Tools such as Scapy6 and the Hacker's Choice IPv6 Toolkit come to mind.

4.2 MULTICAST SECURITY VULNERABILITY

IPv6 has no broadcast method of packet forwarding and instead uses multicast for all one-to-many communications. If an attacker could send traffic to these multicast groups and all the systems that are part of these groups respond, that would give the attacker information that could 4be used for further attacks. The attacker would have information about all the routers within the IPv6 network and all the DHCPv6 hosts. These are critically important nodes for aiding an attacker in determining what other computers are contained within the network, either through neighbor caches, binding updates, or DHCPv6 logs. To launch a blind attack (no return traffic) against all DHCPv6 servers, the attacker has only to send his packet to FF05::1:3.[5].

Multicast could not only be used for reconnaissance but also as a way to amplify traffic volumes for DoS attacks. A spoofed source address in a packet destined to a multicast address could result in amplification of the return traffic toward the target spoofed source address. Securing multicast has historically been a challenge. The nature of multicast is that there is a single source sending to many receivers. Harith A. Dawood,(2013.)

4.3 STATELESS ADDRESS AUTO CONFIGURATION ISSUES:

IPv6 enables plug-and-play networking, or **auto configuration**, which allows devices to configure themselves independently using a stateless protocol and to configure their IP addresses and other parameters without the need for a server. Also, the time and effort required to renumber a network by replacing an old prefix with a new prefix are reduced. An IPv6 host can get an IPv6 address automatically using two types of auto configuration mechanism, stateful address auto-configuration that uses Dynamic Host Configuration Protocol version 6 (DHCPv6) to generate IPv6 address for host and stateless address auto-configuration that includes generating a link local address and generating global addresses. Whereas IPv4, hosts were originally configured manually or with host configuration protocols like DHCP, IPv6 auto configuration goes a step further by defining a method for devices to configure their IP address and other parameters automatically without the need of a server. IPv6 defines both Stateful and Stateless address auto configuration. SLAAC requires no manual configuration of hosts, minimal (if any) configuration of routers and no additional servers.

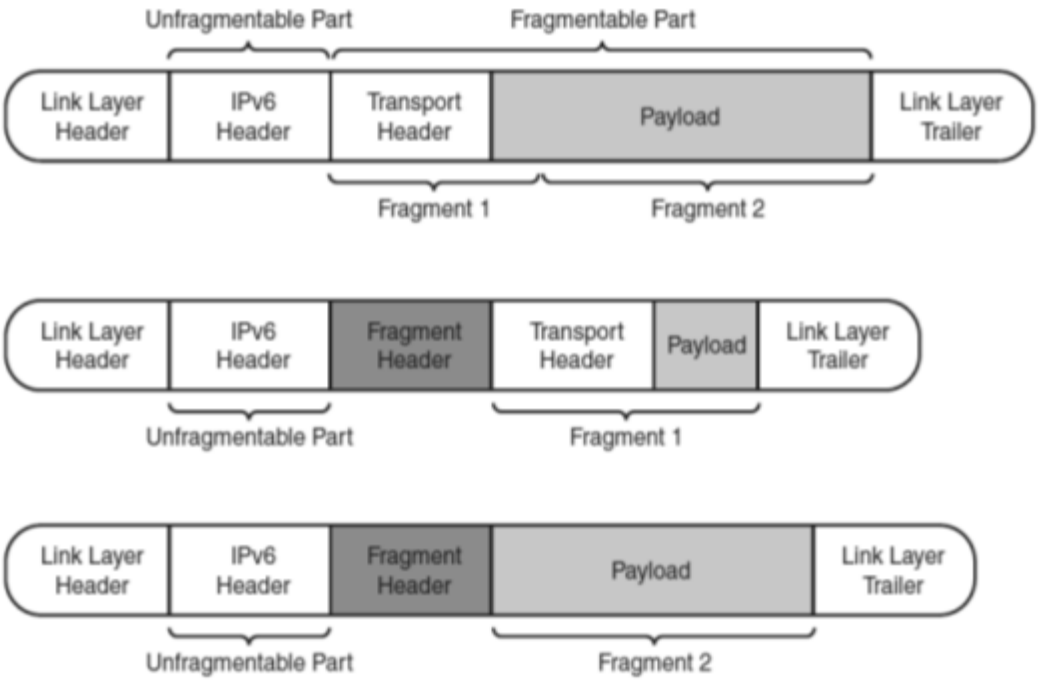
This allows a host to generate its own addresses using a combination of locally available information and information advertised by the routers.. SLAAC does not provide any authentication mechanism so a malicious user can send rogue RA messages and pretend to be the default router. This can be accomplished by an attacker which injects false information into the routing table of all other hosts. As a result all nodes send their packets leaving the subnet to the malicious host. Besides capturing the traffic, adversary can cause a Denial of Service by drop all packets sent by adjacent nodes to a new default route advertised in the RA message, which could or not exist.

4.3 NEIGHBOR DISCOVERY AND SOLICITATION SECURITY CONSIDERATION

In IPv4, subnets are generally small, made just large enough to cover the actual number of machines on the subnet. In contrast, the default IPv6 subnet size is a /64, a number so large it covers trillions of addresses, the overwhelming number of which will be unassigned. Consequently, simplistic implementations of Neighbor Discovery can be vulnerable to denial of service attacks whereby they attempt to perform address resolution for large numbers of unassigned addresses (Gelogo, Y. E. Caytiles, R. D. Park, B. (2011). Such denial of service attacks can be launched intentionally (by an attacker), or result from legaloperational tools that scan networks for inventory and other purposes

4.4 FRAGMENTATION SECURITY VULNERABILITY

Fragmentation is the process of dissecting an IP packet into smaller packets to be easily carried across a data network that cannot transmit large packets, as shown in Figure below:



SOURCE: Harith Dawood " IPv6 Security Vulnerabilities" INTERNATIONAL JOURNAL OF INFORMATION SECURITY SCIENCE, *Vol. 1, No. 4 pp*-100

In IPv6, fragmentation is never performed by the intermediary routers but by the end nodes themselves. So, only the end hosts are allowed to create and reassemble fragments. This process can be used by attackers to either hide their attacks or to attack a node. By putting the attack into many small fragments, the attacker can try to bypass filtering or detection. Attackers can also create fragments in such a way as to exploit weaknesses in the method an end host uses to reassemble the fragments. Examples of this would be overlapping fragments, where there is an overlap in the offset and out-of-order fragments where the fragments' IDs do not match correctly with the data. Another type of fragment attack involves an attacker sending an incomplete set of fragments to force the receiving node to wait for the final fragment in the set. Fragmentation attacks can also involve nested fragments or fragments within fragments, where the IPv6 packet has multiple fragmentation headers. Fragmentation attacks are typically used by hackers with tools such as Whisker, Fragrouter, Teardrop, and Bonk.

4.5 IPV6 ADDRESS SPOOFING (MAC ADDRESS SPOOFING) VULNERABILITY

Because of IPv6 address depends on MAC address which in a sense the MAC address is a computer's true name on a LAN. A person might want to change the MAC address of a NIC for many reasons:

1. To get past MAC address filtering on a router.

2. Sniffing other connections on the network.

3. To keep their burned in MAC address out of IDS and security logs.

4. To pull off a denial of service attack.

Therefore, many people changing their MAC address in different operating systems (WindowXP/Vista, Linux and Mac OS X) either manually or by software. Unfortunately, this is privacy risk, because anyone who has your MAC address also has your IP address! and tracking the identity of the user is possible.(Harith Dawood, 2013).

5. SOME IPv6 COMMON ATTACKS

- Sniffing, header manipulation, session
- Hijacking, man-in-the middle.
- Buffer overflows, SQL injection, cross-sites cripting.
- Email (attachments, phishing, hoaxes)
- Worms, viruses, distributed denial of service (DDoS)
- Malicious insider, physical security, rogue devices, dumpster diving.

6. SECURITY FOR IPv6

- Protection host from scanning and attacking
- Protection of IPv6 packets
- Protecting & Controlling of what traffic is exchanged with the Internet.
- Authorization for automatically assigned addresses and configurations
- Prevention systems (Firewalls and intrusion detection)
- End-to-end data protection.
- Multicast routing protocol security (Multicast distribution tree protection).
- Membership access control at the subnet level.

7. CONCLUSION

IPv6 security is a major challenge nowadays as the migration to IPv6 is a short-term reality. Protection is required by every device that is participating in networked communication. So, IPSec should be considered more seriously to provide the necessary authentication, integrity and confidentiality services during web server integration in a network environment.

REFERENCES

Amer Nizar Abu Ali,(2012). "*Comparison study between IPV4 & IPV6*". IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 3, No 1, May 2012 ISSN (Online): 1694-0814 www.IJCSI.org.

Emin Çalışkan, (2014). "*IPv6 Transition and Security Threat Report*". NATO Cooperative Cyber Defence Centre of Excellence (the Centre), Tallinn 2014.

Harith A. Dawood,(2013). "*IPv6 Security Vulnerabilities*". International Journal Of Information Security Science *Vol. 1, No. 4.*

M. Buvaneswari and Dr. N. Rajendran (2015). *"A Comprehensive Study on Next Generation Internet Protocol (Ipv6) and Security Vulnerabilities".* International Journal of Computer Science Trends and Technology (IJCST) – Volume 3 Issue 5, Sep-Oct 2015.

Supriyanto, Raja Kumar Murugesan and Sureswaran Ramadass(2012). "*Review On Ipv6 Security Vulnerability Issues And Mitigation Methods".* International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.6, November 2012.