
Mohit Wadhwa
Student-CSE Department
Ambedkar Institute of Technology
New Delhi, India
mohitwadhwa86@gmail.com

Suresh Kumar
Assistant Professor-CSE Department
Ambedkar Institute of Technology
New Delhi, India
sureshpoonia@yahoo.com

Abstract - The current generation of the Internet is based on IPV4 protocol. IPV4 has been a great success on that time but due to less address space and lack of security it does not fulfill the requirement of the exponential growth of the internet. Because of limited address space and lack of security IPV4 is replaced by IPV6, proposed by the network working group of the Internet Engineering Task Force (IETF) which provides various improvements over IPV4 like simplicity, large address space, auto-configuration, simple routing header, flow label capabilities, security and so on. This Paper identifies flaws common in IPV4/IPV6 and security issues in IPV6.

Keywords – Ipv4, IPv6, IPsec, Threat, IP

I. INTRODUCTION

IPV4 is a key component of the current Internet infrastructure, which was developed, in the mid 1970’s. There are some problems with IPV4 like too few address, too large routing tables, lack of security (because IPV4 does not use IPsec by compulsion) and demand for a real time data transfer. To eliminate some of the mentioned imperfection, network working group of the internet engineering task force (IETF) proposed a new suite of protocols called the internet protocol version (IPV6) [1].

IPV4 specifies a 32 bit IP address fields, which cannot fulfill the requirement of the experimental growth of internet therefore internet protocol IPV6 was introduces with 128 bit IP address field which provides the large address space and improve security by using IP sec as a part of packet header.

IPV6 provides various improvements over IPV4 like simplicity, large address space, simpler auto-configuration, and simple routing header, flow laddling capability and enhanced security. Although the IPV6 protocol is still developing, it is fully functional and its implementation and usage in the real network is possible [2].

In section 2, we will discuss the comparison between IPV4 and IPV6, in section 3, threats common in IPV4 and IPV6 are discussed. Section 4 outlines security issues which are related with IPV6 alone. Finally the conclusion will be given.

II. COMPARISON BETWEEN IPV4 AND IPV6

Some of the key difference between ipv4 and ipv6[3][4] are outlined in the below table.

<table>
<thead>
<tr>
<th>Features</th>
<th>IPv4</th>
<th>IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>32 bit IP address</td>
<td>12 bit IP address</td>
</tr>
<tr>
<td>IPsec</td>
<td>Optional</td>
<td>IPsec support is required</td>
</tr>
<tr>
<td>Quality of service</td>
<td>Differentiated services</td>
<td>Use traffic classes and flow labels</td>
</tr>
<tr>
<td>Fragmentation</td>
<td>Done by routers and source node</td>
<td>Done by the source node only</td>
</tr>
<tr>
<td>Unicast, multicast and broadcast</td>
<td>Use all</td>
<td>Use unicast, multicast and anycast cannot used broadcast</td>
</tr>
<tr>
<td>IP configuration</td>
<td>Manually or DHCP</td>
<td>Auto configuration or DHCP</td>
</tr>
<tr>
<td>Checksum</td>
<td>Header include checksum</td>
<td>Header does not include checksum</td>
</tr>
<tr>
<td>Option field in header</td>
<td>Required</td>
<td>Moved to IPv6 extension header</td>
</tr>
<tr>
<td>ARP(address resolution protocol)</td>
<td>Use to resolve an ipv4 address</td>
<td>Replaced by ND(Neighbor Discovery)</td>
</tr>
<tr>
<td>Mobility</td>
<td>Uses mobile IPv4</td>
<td>MIPv6 with faster handover, routing and hierarchical mobility</td>
</tr>
<tr>
<td>Internet Group Management Protocol(IGMP)</td>
<td>Use to manage local subnet group</td>
<td>Replaced with Multicast Listener Discovery</td>
</tr>
<tr>
<td>Packet Size</td>
<td>Must support a 576 byte packet size(possibly fragmented)</td>
<td>Must support a 1280 byte packet size(without fragmentation)</td>
</tr>
</tbody>
</table>

A. Address space

IPV6 has 128 bit (16 byte) source and destination IP address as compared to 32 bit (46 byte) for IPV4. IPV6 thus
B. TCP/IP administration [5]

IPv6 provides the ability for stateful and safe-less auto configuration of IP addresses whereas IPv4 is limited to stateful protocol such as the dynamic host configuration protocol (DHCP) in which static tables are maintained to determine the IP address to be assigned to a newly connected node [6]. Neighbor discovery protocols allows on IPv6 to engage in stateless auto address configuration [7].

C. Better mobility support

When IPv4 was developed, there really was no concept of mobile IP devices. Main goal of the mobile IP protocol (MIP) is to maintain the IP address of the node while roaming through the different network segments [8]. So MIPv6 protocol was introduced in the IPv6 which allow the mobile nodes to maintain their connection with the existing node while changing their location and address.

D. Quality of services

The IPv6 packet header contains the flow label fields that facilitate the support for QoS for both differentiated and integrated services [9]. QoS can be achieved by assigning high priority to certain packets that need to reach at destination in timely manner.

E. IPsec

In IPv6, IPsec is a part of IPv6 header whereas in IPv4 it is not a part of header but can be adapted optionally. The objective of IPsec is to authenticate and/or encrypt all traffic at the IP level [10]. Therefore IPv6 provides end to end security i.e. data is secured from source to destination. In IPv4, IPsec typically provides security between border routers of separate network [7].

F. Option versus Extension header [11]

With IPv4, options were integrated into the basic IPv4 header whereas in IPv6 they are handled as extension header [11]. Extension header included into the IPv6 header whenever they are necessary. This way packet became flexible and transmitting of packet is much more efficient.

III. Threats common in both IPv4 and IPv6 [12][13]

A. Sniffing attack

Sniffing is a popular way to steal information from a network usually in the form of password, id or some important information that are useful for the attacker. Through sniffing attack the attacker steal password or id of the legitimate user and using this information later to log into the network and gather secret information of the network. Sniffing attack can be preventing through tight security, one way is to use one time password or ticketing authentication.

B. Application Layer Attack

Application layer attacks those are very famous in current internet protocol ipv4 are still existing in ipv6. Various application layer attack like buffer overflow, CGI attack, various type of malicious codes that attacks on the seventh layer i.e. application layer of the ISO/OSI model. Enhanced security in ipv6 still cannot provide any mechanism to prevent these attacks at application layer.

C. MITM (Man In The Middle Attack)

Like IPv4, IPv6 headers have no security mechanism each protocol relies on the IPsec protocol suit for security. In this type of attack, the attacker situates himself between the communications of two nodes or the communication between client and server.

D. Flooding Attack

Flooding attack is more frequent in IPv4 and this attack also exists in IPv6. Dos/DDos is a kind of flooding attack that objective is to consumes the bandwidth of the targeted system in such a way that the legitimate user unable to access their legitimate services. The various kind of flooding attacks are: smurf attack, UDP/TCP flooding attack, TCP syn attack etc. through which attacker consumes the bandwidth of target.
system make the target system unavailable and the legitimate user cannot access the services of that system. Dependence of multicast address in IPv6 provides a new ways of misuse and attacker performs flooding attack.

E. Rouge Devices

Rouge devices are that devices that are introduced in the network in an unauthorized way. Rouge devices like wireless access point, DNS server, router or switches. These attacks are common in IPv4 and are not substantially changed in IPv6. In IPv6, IPsec is a part of header which provides strong authentication mechanism, so authentication for devices could mitigate this attack somewhat in IPv6 as comparison to IPv4 but cannot stop this type of attack.

IV. SECURITY ISSUES IN IPV6

A. Type 0 routing header threats in IPv6

Routing header is a kind of extension header of IPv6 and it’s used by an IPv6 source list one or more intermediate nodes to be visited on the way to a packet destination [1]. An attacker can generate malicious packet with routing header that containing victim address and then sends a packet to publically accessible address further publically accessible address checks the routing header and forwards the packet to the destination address (victim address). Through this way malicious packet will reach at victim system without breaking the security rules. By using this vulnerability attacker can bypass the packet filtering mechanism and create the opportunity for denial of service attack.

B. Threat through ICMPv6 and multicast [3][5]

In IPv4 it was possible to block most of ICMP (Internet control message protocol) message for security purpose but in IPv6 some of network operations are depend on ICMPv6 message so it was difficult to block ICMPv6 messages. In IPv6 some of the ICMPv6 message must be allowed because of proper network operations like error message which includes destination unreachable, packet too big, time exceeded and parameter problem).ICMPv6 message also includes information message such as MLD (multicast listener discovery) and ND (Neighbor Discovery). MLD is a set of message exchange by routers and nodes, enabling routers to discover set of multicast address. Through this way attacker can gain access of the multicast address by sending a suitable packet to routers and in response to that router sends a list of victim addresses to attacker.

C. Threat through Neighbour discovery (ND) and Auto configuration

Like MLD message, ND message uses the ICMPv6 message structure. ND message provides additional information, typically indicating MAC address, on link network prefix, on link MTU information and consist of router solicitation, router advertisement, neighbor solicitation, neighbor advertisement and redirect. Router solicitation message was generated by IPv6 source node to gather information from IPv6 routers present on the link. An IPv6 node sends a multicast router solicitation to prompt routers to respond immediately rather than waiting for periodic router advertisement (RA) message [3]. In response to receive router solicitation message, IPv6 router sends the RA message back to the source node and also the information required by the source node like link prefix, the link MTU and whether or not to use the address auto configuration. Through this way attacker can misuse it and by using spoofed address attacker can gather all the important information and later by using it insert itself into the network through auto configuration mechanism provided by IPv6 protocol because auto configuration in IPv6 provides any rogue node to get an IPv6 address without authentication or administration configuration, thereby, providing IPv6 access to any system with physically network access [14].

D. Reconnaissance threat in IPV6 [15]

There are two methods (host probing and port scanning) through which attacker can achieve reconnaissance attack. In host probing, the attacker identifies the number of host connected on the network and after identifying number of host attacker uses port scanning to exploit the vulnerabilities. This way reconnaissance attack enables attacker to gather information about host and other network devices. The attacker uses ping probe to determine the IP address of the victim in IPv6. The Potentially huge size of IPv6 subnets makes reconnaissance attack more difficult, but there are other ways to identify target system [12]. IPv6 multicast address structure provides an advantage to attacker to identify various routers or DHCP server connected on the network and thereby providing an opportunity to attacker to scan these devices vulnerabilities. IPsec is mandatory in IPv6 which reduces port scanning but due to huge sizes of IPv6 subnets it is difficult to identify the host that are malicious inside the network and performing port scanning.

E. Fragmentation threat in IPV6

In IPv6 protocol packet fragmentation can only be done by source node it cannot be handled by the intermediate nodes unlike in IPv4 where packet fragmentation can also be achieved by intermediate nodes. RFC 2460 says “IPv6 minimum MTU is 1280 octets”. For this reason packets size less than 1280 octet is discarded by the security devices. It is responsibility of the source operating system to fragment the packet minimum of 1280 octet and this procedure is going on in continuation until last segment of the original packet is delivered. If source not cannot behave in this manner than the security devices receives the packet with size less that 1280 octet. Through this way by sending a large number of small fragmented packets attacker can achieve a denial of service attack. To avoid such a problem it is recommended security practice to limit the total number of fragments and their allowed arrival rate [5].

F. Theft of password threat in IPv6 [16]

Password attack still exists in IPv6. Access to computer and network resources depends on the username and password. Once attacker makes its existence into the network
than by using various attacking techniques attacker can acquire valid user name and password and after having password attacker can enter into the system and carry out malicious activity.

![System A](image1) ![System B](image2) ![Attacker](image3)

**Fig. 3 Attacker access system A**

V. CONCLUSION

IPV6 is the new version of the internet protocol will replace the IPV4 protocol. Due to prevailing security problems occur in IPV4 day by day the acceptance of the IPV6 on the internet is grown at the very fastest rate in the present scenario. The new version of the internet protocol provides numerous features over IPV4 which directly or indirectly improve security for devices that are connected to the internet. Beside these improvements some of the security issues are still exists and needs thorough attention. IPsec protocol in IPV6 is mandates which enhanced the security in IPV6 but cannot solve all the security problems exist in IPV6. Even though IPV6 is accepted protocol but if we provide some more ways and means to solve the existing issues in IPV6 than it can be widely accepted protocol on the internet.

REFERENCES

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