Security Holes in Contrast to the New Features Emerging in the Next Generation Protocol

Mohit Wadhwa
Student CSE Department
Ambedkar Institute of Technology
Indraprastha University
New Delhi, India

Manju Khari
Assistant Professor
Ambedkar Institute of Technology
New Delhi, India

ABSTRACT
The next generation protocol (Ipv6) also called Iping, which should replace the current generation of Internet protocol (Ipv4), brings many enhancements over Ipv4. Ipv4 has been a great success for more than 20 years, since its interception in 1980 but due to limited address space, complex configuration and very important lack of security it does not fulfil the requirement of the exponentially growing internet. Because of inadequate address and for other issues, Ipv6 was proposed by the network working group of the internet engineering taskforce (IETF) which provides many new features like quality of services, auto-address configuration, end to end connectivity, security, simple routing header and so on. This paper identifies security holes to the new features introduced in Ipv6 and security holes that are not altered by new futures of Ipv6.

Keywords:
Ipv4, Ipv6, Ipsec, NAT, TCP/IP, security holes, IP

1. INTRODUCTION

The current generation of Internet protocol (IPv4) has been in use for more than 20 years and has not significantly changed since it was introduced in 1981. IPV4 has proven to be robust, interoperable and easily implemented.

The IPV4 specifies a 32 bit IP address field is a key component of the internet infrastructure and have many issues like complex configuration, limited address space, large routing tables, demand for real time data transfer and lack of security which does not fulfil the requirement of the exponential growth of the internet. 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].

Industry stakeholder and Internet experts generally agree that IPv6-based network would be technically superior to the commonly installed base of IPv4-based networks [2]. The IPv6 with 128 bit address space provides large IP addresses and also with classless and auto address configuration features, IPv6 provides a new innovative communication services among the nodes and improved security by using IPsec as a part of packet header.

IPv6 provides various improvements over IPv4 like simplicity, large address space, simple routing header format, extension for authentication and privacy, flow labelling capabilities, quality of services (Qos) and very important security at IP level. In addition, through auto configuration and mobility feature of IPv6 nodes on the Internet can communicate in simpler way. However, IPv6 with new features will likely generate newer protocol attacks and IPv4 related attack would morph into new form. Although the IPv6 protocol is still developing, it is fully functional and its implementation and usage in the real network is possible [3].

In section 2, we will discuss the new features introduced in IPv6. In section 3, these features are discussed along with security holes. Section 4 outlines security threats that are common to IPv4. Finally the conclusion will be given.

2. IMPORTANT IPV6 FEATURES

The problem of lack of address space and lack of security was the main motivation for creating new features in Ipv6.Some of the important Ipv6 features are outlined below [4][5]

2.1 Option versus extension header

With Ipv4, options were integrated into the basic Ipv4 header whereas in Ipv6 they are handled as extension header [6]. Extension header included into the Ipv6 header whenever they are necessary. This way packet become flexible and transmitting of packet is much more efficient.

2.2 Large address space

Ipv4 provides a 32 bit IP address field, which cannot fulfill the requirement of the exponential growth of the internet therefore internet protocol version 6 (Ipv6) was introduced with 128 bit IP address field which provides large address space. This larger address size allows for the generation of $3.4 * 10^{38}$ address values, which should be more than enough for current and future applications, and eliminates the need for address conservation practices such as NAT that Ipv4 requires [7].

2.3 Option versus extension header

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.

2.4 TCP/IP Administrator

Ipv6 provides the ability for stateful and stateless 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 [5]. With stateless address configuration, hosts on a link automatically configure themselves with IPv6 addresses for the link (called link-local addresses) and even in the absence of a router, hosts on the same link can automatically configure themselves with link-local addresses and communicate without manual configuration. Neighbor discovery protocol allows an Ipv6 node to engage in stateless auto-configuration [8].

2.5 Better support for Mobility

When IPV4 was developed, there was no concept of mobile IP devices. The main problem arises when mobile node move from its home network to some other network than there is a need of mobile IP. Main goal of the mobile IP protocol (MIP) is to maintain the IP address of the node while roaming through the different network segments [9]. 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.

2.6 Better support for Mobility

Ipv4 was designed at a time when security wasn't much of an issue. But today, security is a big issue therefore Ipv6 was developed with inbuilt security feature. In Ipv6, IPsec is a part of IPv6 header where as 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]. 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 [11].

3. SECURITY HOLES RELATING TO THE NEW FEATURES OF IPV6.

3.1 Option versus extension header [4]

In Ipv4, options were integrated into the basic Ipv4 header whereas in Ipv6 they are handled as extension header [6]. Hop-by-Hop Options header, Destination Options header, Routing header, Fragment header, Authentication header, Encapsulating Security Payload header are the extension header of varying length. A Next Header field in the IPv6 header indicates the next extension header. Within each extension header is a Next Header field that indicates the next extension header. The last extension header indicates the upper layer protocol.

There a various security attack relating to extension header, here we considered routing header. Routing header is a kind of extension header of Ipv6 and is used by an IPv6 source list one or more intermediate nodes to be visited on the way to a packet destination [1].when routing header is used, destination address in Ipv6 header is not the final node but just the next node [12].See figure 1 there are two packets, packet 1 and packet 2. Packet filtering access list is applied at router and firewall before internal network to block the malicious packets. Packet 2 can easily blocked at firewall because access to the internal network is blocked in the access list therefore an attacker can generate a malicious packet, packet 1 with routing header that containing victim address and then sends a packet to publicly address HOST B shown in figure 1 further HOST B check the routing header and find that the packet 1 is not for HOST B and then HOST B forwards the packet 1 to HOST C i.e. internal network. Through this way malicious packet will reach at the internal network 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 [11].

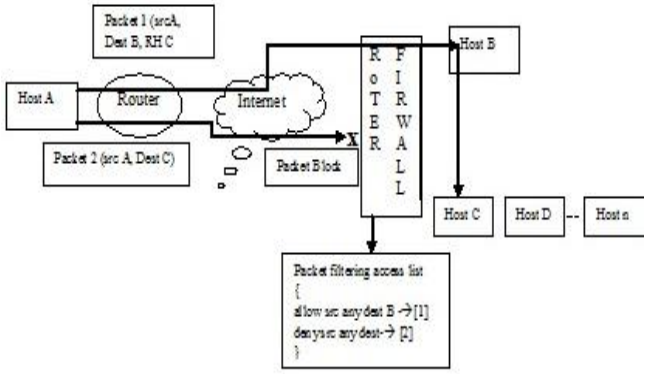

Fig. 1 Packet filtering access list

3.2 Large address space

At the time when the Ipv4 address space was designed, it was unimaginable that the address space could be exhausted but in the current generation number of user on the Internet growing at the exponential rate. Therefore it was clear by 1991 that the replacement of Ipv4 is necessary. So Ipv6 with 128-bit IP address field was developed by network-working group of the Internet engineering task force (IETF). The 128-bit address will solve address space problem at least for the next 50 years.
The attack relating to this feature was **reconnaissance attack [13][14],** by which an attacker can gather secret information about host and network devices. 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.

In IPv4 networks, port scanning is a relatively simple task. Most IPv4 segments are Class C, with 8 bits allocated for host addressing. Scanning a typical IPv4 subnet, at a rate of one host per second, translates into:

$$2^8 \text{ Host} \times \frac{1 \text{ second}}{1 \text{ Host}} \times \frac{1 \text{ minute}}{60 \text{ seconds}} = 4.267 \text{ minutes}$$

In IPv6 networks, the landscape is radically different. IPv6 subnets use 64 bits for allocating host addresses. Consequently, a typical IPv6 subnet requires:

$$2^{64} \text{Host} \times \frac{1 \text{ second}}{1 \text{ Host}} \times \frac{1 \text{ year}}{31{,}536{,}000 \text{ sec}} = 584{,}942{,}417{,}355 \text{years}$$

Scanning such a large address space is almost an impossible task [15]. The Potentially huge size of IPV6 subnets makes reconnaissance attack more difficult, but there are other ways to identify target system [14]. 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 [11].

3.3 Elimination of Network Address Translation (NAT)

NAT itself has some advantage and disadvantage from security point of view. NAT breaks end-to-end connectivity. As shown in figure 1[8], VOIP application between two private addresses cannot take place [16] because any outside address cannot communicate to private network directly, that's why they are blocked at firewall. The present internet makes use of NAT which provides a single point entry into networks and security mechanisms such as Firewalls can be set up at entry, as shown in figure 1 [8] but the next generation protocol does not support NAT because of large 128 bit address space which can assign to every single node in the world.

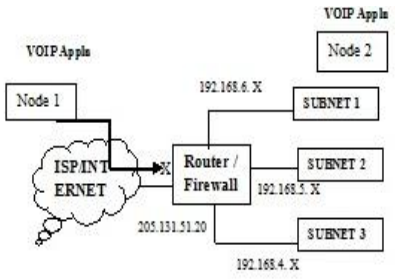

Fig 2 NAT

Through this way Ipv6 provides end-to-end connectivity to all host but with end-to-end connectivity there will be no single entry point, which provide security from outside addresses and the security will lie with the host. This way elimination of NAT gives some security issues.

3.4 Tcp/IP Administrator

In Ipv4 ARP protocol was used but in Ipv6 ARP is gone. Ipv6 provides the ability for stateful and stateless 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 [5]. Ipv6 also uses Neighbor discovery (ND) protocol that was built into Icmpv6 and 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. The purpose of ND is to determine the relationships between neibhboring nodes.

ND message start with Neighbor solicitation (NS) multicast query which was generated by IPV6 source node to gather information from neighbouring nodes present on the link. In response to receive NS message, IPV6 nodes sends the Neighbor advertisement (NA) 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 secret information and later by using it insert itself into the network through auto configuration mechanism provided by IPV6 protocol. 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 [17]

3.5 Better support for mobility

When IPV4 was developed, there really was no concept of mobile IP devices. MIpv6 protocol introduced in the Ipv6 which allow a mobile node to keep the same IP address visibility even when it moves from home network to foreign network. In this way when an MN (mobile node) moves from home link to a foreign link, it acquires an IP address from the FA called care of address (COA) and also keeps its own Home IP address. MN tells its new IP address (CAO) to HA for maintaining the relation with the home network because the entire packet will forward to MN through home network with tunneling. There are the several security questions arises for authentication and authorization of the mobile host in a foreign network.

Think for a moment When an attacker send fake registration request to HA, using its own address as CoA and then attacker will receive all the packets belongs to MN through this way attacker perform Denial of service attack.

3.6 Better support for security [18]

In Ipv6, IPsec is a part of Ipv6 header. The main objective of Ipsec is to provide IP level authentication and encryption of all the traffic. Therefore Ipsec provides end-to-end security i.e from source to destination. But it has the security issue because establishment of the initial SA (security association) is based on key management under other protocols. In Ipsec based host

all the secret parameters are in SAD (security association database), Once security association database is uncovered, black hats gain access to this database than they can very easily obtained the secret key and other important information regarding all the connections.

In Ipsec sniffing of encryption data was possible. Therefore "black hat" first sniff the encrypted data pattern and then by using secret key from SAD they can break the encrypted data very easily. Through this way attacker can avoid Ipsec but attacker has to scan huge size of Ipv6 address space. In Ipsec based hosts, all the secret parameters are in SAD, that is to say, read SAD, and have all the secrets [1].

4. SECURITY HOLES COMMON TO IPV4 AND IPV6

This section outlines attacks that are common to both Ipv4 and Ipv6 which are not altered by new features of Ipv6 [11][14].

4.1 Sniffing attack [19]

The 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.

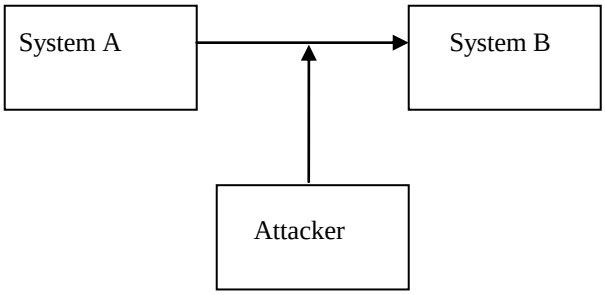

Fig. 3 Sniffing Attack

Sniffing attack can be preventing through tight security, one way is to use one time password or ticketing authentication.

4.2 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.

4.3 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.

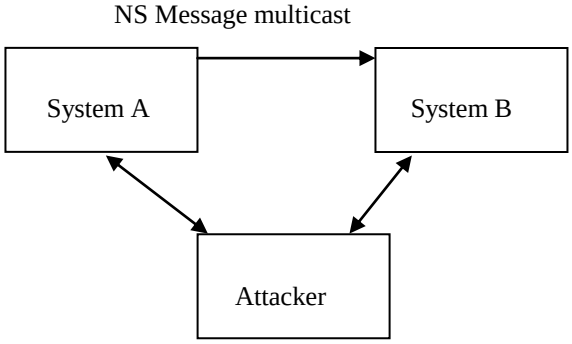

Fig 4 MITM

4.4 Flooding Attack

In this scenario, node A wants a MAC address of another node B for establishing a communication between Node A and Node B therefore Node A sends the NS (Neighbor solicitation) message to all nodes multicast address therefore an attacker on the same link can use the NS message and reply to node A with the corresponding NA (Neighbor Advertisement) message, thereby tacking over the communication held between Node A and Node B.

4.5 Flooding Attack

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.

5. CONCLUSION

IPV6 is the next generation of the Internet protocol will replace the present IPV4 protocol. Ipv6 provides numerous security features over Ipv4 that improves the overall functionality and provides improve security for the devices that are connected to the Internet. Beside these numerous improvements some of the potential security issues still exist and needs through attention. IPsec protocol in IPV6 is mandates that enhanced the security in IPV6 but cannot solve all the security problems exist in IPV6. Even though, IETF is still working on Ipv6 security for Ipv6 firewall, mobility, ICMPv6 and transition. Hence, 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.

6. ACKNOWLEDGMENTS

I, Mohit Wadhwa, author of this paper would like to thank my college , Ambedkar institute of Technology, New Delhi for providing me adequate recourses to make this paper. I would also like to thank my guide Mrs. Manju Khari for giving me valuable suggestions.

7. REFERNCES

[1] S.deering and R.hinden, Internet protocol version 6 (Ipv6) specification, RFC 2460, December 1998

[2] L. ladid, 3G Mobile Communication Technologies, Second International Conference on (Conf. Publ. No. 477),IEEE2001

[3] Cooper M, Yen DC. IPv6: business applications and implementation concerns. Computer Standards and Interfaces, vol. 28. Elsevier Science; 2005, 27–41

[4] Microsoft Corporation, Introduction to IP version 6, January2008

[5] Penny Hermann-Seton, Security features in IPv6 [Availableonline], http://www.sans.org/reading_room/whitepaper/protocols/security_features_ipv6_380, Last Visit-December 4, 2010

[6] O' Rielly, IPv6 Essentials, [Available online] Last visit-12Feb.2011

[7] G. Van de Velde et al., Local Network Protection for IPv6, IETF RFC 4684; www.rfc-archive.org/getrfc.php?rfc=4864&tag=Local-Network-Protection-for-IPv6, May2007

[8] R. Radhakrishnan, Majid Millia, Shabana Mehfuz and Moinuddin, Security issues in IPv6, IEEE 2007

[9] Davies. J, Understanding IPv6, Microsoft Corporation, 2003

[10] Radwan, A.M, IPsec: a basis for IPv6 security [available online]http://www.IPv6style.jp/en/tech/20040707/index.html 2005Lastvisit-December2010

[11] Mohit wadhwa, Suresh kumar: Security Flaws Common in IPV4/IPV6 & Security Issues in IPV6: A Study, ICSE 2011

[12] Jeodeok lim, youngki kim, protection algorith against security holes of ipv6 routing header, ICACT2006

[13] Carlos E. Caicedo and James B.D. Joshi : IPv6 Security Challenges,IEEE,2009

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

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

[16] IPv6 Security from point of view firewalls, Janos Mohácsi 09/June/2004, Information societ technologies, 6net

[17] Steffeno M. Faccin and Franck Lee, A secure and efficient solution to the IPv6 address ownership problem IEEE,2000.

[18] Dequan Yang, Xu Song and Qiao Guo, Security in IPv6 IEEE,2010.

[19] Basic-Sniffer-Attacks , http://www.scribd.com/doc/6394/Basic-Sniffer-Attacks Last visit - December 2010