IPv6 Security Vulnerabilities

Harith A. Dawood

I.T. Department, British Royal University for Science and Technology, Erbil, IRAQ.

Harith.dawood@hotmail.com

Abstract- Internet Protocol version 6 (IPv6) is the newest version of the protocol that is used for communications on the Internet. This version has been in existence for many years. But, currently many organizations have slowed their migration to IPv6 because they realize that the security considerations and products for IPv6 might be insufficient, despite the fact that the network infrastructure is ready to support IPv6 transport. They realize that they cannot deploy IPv6 without considering the security of this protocol at first. IPv6 security vulnerabilities currently exist, and as the popularity of the IPv6 increases, so do the number of threats. This paper covers and reviews some of the fundamental vulnerabilities topics of IPv6 security, considerations, issues and threats. At the end, it summarizes some of the most common security concerns the new suite of protocols creates.

Keywords - IPv6; IPsec; Network Security; Security Vulnerabilities

1. Introduction

IPv6 defined in the mid-1990s in Request for Comments (**RFC**) 2460 "Internet Protocol, Version 6 (**IPv6**) Specification" and a host of other more recent RFCs, is an "improved, streamlined, successor version" of IP version 4 (**IPv4**).

IPv6 offers the potential of achieving increased scalability, reach ability, end-to-end interworking, Quality of Service (QoS), and commercial-grade robustness for data communication, mobile connectivity, and for Voice over IP (VoIP). The current version of the Internet Protocol, IPv4, has been in use successfully for almost 30 years and exhibits some challenges in supporting emerging demands for address space cardinality, high-density mobility, multimedia, and strong security.

IPv6 is an improved version of IP that is designed to coexist with IPv4 while providing better internetworking capabilities than IPv4, and resolving unanticipated IPv4 design issues and takes the Internet into the 21st Century [2],[3].

IPv6 was initially developed because of the anticipated need for more end system addresses based on anticipated Internet growth, encompassing mobile phone deployment, smart home appliances, and billions of new users in developing countries.

IPv6 features include the following [4], [11], [14], [17]:

1. Expanded Addressing Capabilities. IPv6 increases the IP address size from 32 bits to 128 bits.
2. Header Format Simplification.
3. Authentication and Privacy Capabilities. In IPv6, security is built in as part of the protocol suite: extensions to support authentication, data integrity (encryption), and (optional) data confidentiality are specified for Internet Protocol Security (IPsec). IPsec is a set of protocols and was originally developed as part of the IPv6 specification. IPsec is mandated as required in IPv6 while it is optional in IPv4, which means, "IPv6 is more secure."
4. Flow Labeling Capability.
5. Improved Support for Extensions and Options (with greater flexibility for introducing new options in the future).

Additionally, there are many others IPv6 features [12], [13], [15]:

- Stateless auto-configuration: The ability for nodes to determine their own address.
- Multicast: Increased use of efficient one-to-many communications.
- Jumbo grams: The ability to have very large packet payloads for greater efficiency.
- Mobility: Simpler handling of mobile or roaming nodes.

IPv6 is a technology now being deployed in various parts of the world that will allow truly explicit end-to-end device addressability. IPv6 becomes an institutional imperative in the final analysis. But the security considerations continue to be critically important.

2. IPv6 Security Vulnerabilities

The security features of IPv6 are described in the Security Architecture for the Internet Protocol (RFC 2401, RFC 2402, and RFC 2406), but we will describe the real IPv6 security issues:

2.1. Tracking The Identity Of The User

Traditional interface identifiers for network adapters use a 48-bit address called an IEEE 802 address. It consists of a 24-bit company ID (also called the manufacturer ID), and a 24-bit extension ID (also called the board ID). The combination of the company ID, which is uniquely assigned to each manufacturer of network adapters, and the board ID, which is uniquely assigned to each network adapter at the time of assembly, produces a globally unique 48-bit address. This 48-bit address is also called the Media Access Control (MAC) address.

In today's IPv4-based Internet, a typical Internet user connects to an Internet Service Provider (ISP) and obtains an IPv4 address using the Point-to-Point Protocol (PPP) and the Internet Protocol Control Protocol (IPCP). Each time the user connects, a different IPv4 address might be obtained. Because of this, the identity of users on the Internet is often unknown. So, it is difficult to track a dial-up user's traffic on the Internet on the basis of IP address [6]. And this has created an environment where attackers can easily operate, without their targets knowing much about the source of the messages.

Also, the use of Network Address Translation (NAT) is often misunderstood as a security protection measure because it hides the internal addresses and thus secures the internal network topology. NAT breaks the use of the full end-to-end communication model that IP Security (IPsec) needs to be fully effective.

For IPv6-based dial-up connections, the user is assigned a 64-bit prefix after the connection is made through router discovery and stateless address auto-configuration. If the interface identifier is always based on the EUI-64 address (as derived from the static IEEE 802 address) as shown in figure 1, it is possible to identify the traffic of a specific node regardless of the prefix, making it easy to track a specific user and their use of the Internet.

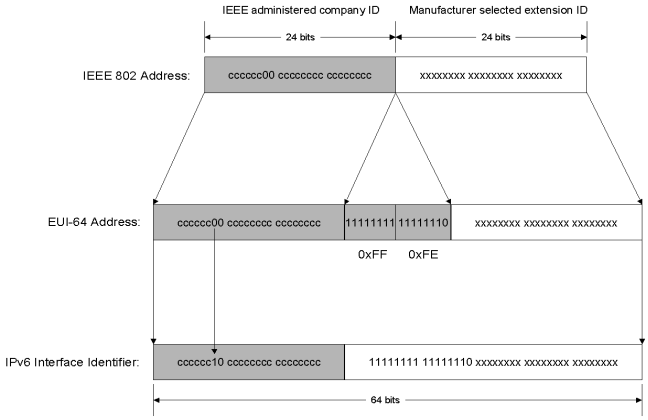


Fig. 1. The conversion of a universally administered, unicast IEEE 802 address to an IPv6 interface identifier.

2.2. 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 (Window XP/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!

2.3. 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 [8].

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.

2.4. Multiple Addresses Vulnerability

IPv6 assigns multiple addresses to an interface which challenges the filtering rules in the firewalls and access control lists [10]. In such cases, a firewall will need to learn all the addresses dynamically and the filtering rules will need to be automatically generate-able using sophisticated policy rule sets. And such capabilities are not available [19]

2.5. Multicast Security Vulnerability

We identify multicast security as one of the important problems to solve for the successful deployment of group communication applications. IPv6 has no broadcast method of packet forwarding and instead uses multicast for all one-to-many communications. IPv6 uses multicast for neighbor discovery, Dynamic Host Configuration Protocol (**DHCP**), and traditional multimedia applications.

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 be used for further attacks [23]. 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. We can even argue that the reconnaissance phase is no longer required with IPv6. 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.

2.6 Extension Header Vulnerability

Because the protocol specifications have not constrained the usage of extension headers as shown in figure 2, they could potentially cause problems if used maliciously [5].

Figure 2 shows the structure of an extension header and describes how they form a linked list of headers before the packet payload. There are many more types of extension headers available for use in IPv6 packets, but this figure shows how they are arranged in the packet.

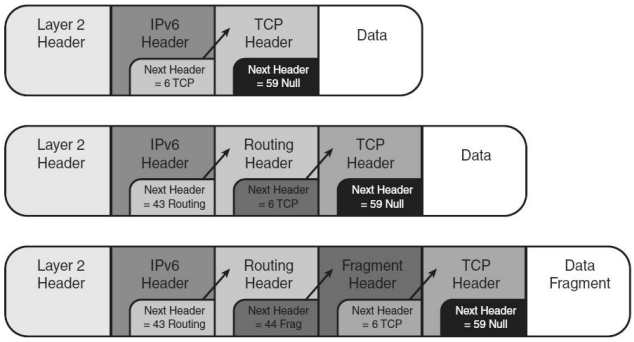


Fig. 2. Example of the Extension Headers.

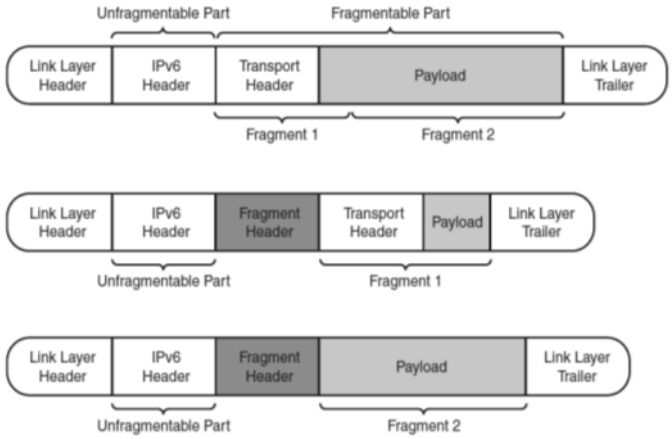
An attacker could perform header manipulation on the extension headers to create attacks. Someone could create an IPv6 packet that meets the protocol specification and has an unlimited number of extension headers linked together in a big list. A packet like this might cause a DoS of intermediary systems along the transmission path or the destination systems. The crafted packet might also pass through the network without causing any problems. Chaining lots of extension headers together is a way for attackers to avoid firewalls and Intrusion Prevention Systems (**IPS**).

Packets that have a large chain of extension headers could be dangerous. Numerous extension headers in a single packet could spread the payload into a second fragmented packet that would not be checked by a firewall that is only looking at the initial fragment.

2.7. 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 3 below:

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 [20],[21]. 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

Fig. 3. Packet Fragmentation.

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 [5].

2.8. 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 [26].

Such denial of service attacks can be launched intentionally (by an attacker), or result from legal

operational tools that scan networks for inventory and other purposes [27].

3. **IPSec and IPv6 Vulnerability**

IP security (IPsec) is available with IPv6. IPv6 headers have no security mechanisms themselves, just as in IPv4. Administrators rely on the IPsec protocol suite for security. The same security risks for man-in-the-middle attacks in Internet Key Exchange (IKE) in IPv4 are present in IPv6.

Most people recommend using IKE main mode negotiations when the use of pre-shared keys is required. On the other hand, IKE Version 2 (IKEv2) is expected to address this issue in the future [22].

The IPv6 IPsec packet format is basically the same as in IPv4. Figure 4 illustrates an IPv6 packet where Authentication Header (AH) and Encapsulation Security Payload (ESP) protocols are used. IPv6 AH and ESP extension headers are used to provide authentication and confidentiality to IPv6 packets.

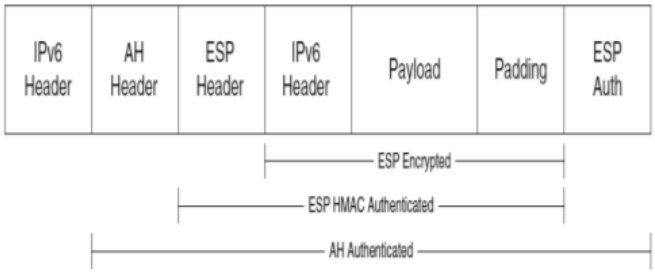


Fig. 4. IPv6 IPsec Packet.

It should be noted, however, that IP-Sec does not automatically secure everything; it's as secure as the computer, operating system or application it is working on. IP-Sec does attempt to standardize security mechanisms in the Internet [25].

4. **Some Common Attacks**

When you consider the ways that an IPv4 or IPv6 network can be compromised, there are many similarities. Attacks against networks typically fall within one of the following common attack vectors [5], [7], [9], [16], [18], [24]:

- Internet (DMZ, web pages, pop-ups).
- Sniffing, header manipulation, session hijacking, man-in-the middle.

- Buffer overflows, SQL injection, cross-site scripting.
- Email (attachments, phishing, hoaxes)
- Worms, viruses, distributed denial of service (**DDoS**)
- Macros, Trojan horses, spyware, malware, key loggers
    - VPN, business-to-business (**B2B**)
    - Chat, peer-to-peer (**P2P**)

- Malicious insider, physical security, rogue devices, dumpster diving.

As noticed above, it is important for considering that IPv6 is not necessarily more secure than IPv4 [1][19]. In fact, IPv6 approach to security is only slightly better than IPv4 but not fundamentally new.

Finally, many groups are performing extensive testing of IPv6, so they hopefully can find many of the issues before it is time to deploy IPv6. However, all the major vendors of IT equipment and software have published vulnerabilities in their IPv6 implementations, (such as: Microsoft, Linux, Sun, and Cisco) all have published vulnerabilities in their software. As IPv6 has been adopted, it is evident that these major vendors have drawn the attention of the hackers.

5. **Conclusion**

Defiantly, before deploying IPv6 you should be aware of the following aspects of security for IPv6 traffic:

- 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)

Besides, as mentioned in the previous Section 2.5, there are three components required to achieve IP multicast security:

1) End-to-end data protection.
2) Multicast routing protocol security (Multicast distribution tree protection).
3) Membership access control at the subnet level.

However, because IPv6 and IPv4 are both network layer protocols, many of the network layer vulnerabilities are therefore similar. 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.

Therefore, you must connect to IPv6 natively. By itself IPv6 is not a panacea for IP-layer/network-layer security concerns.

ACKNOWLEDGEMENTS

At first I must thank my lovely wife and my sweet family for their support.

I would also like to thank Mr. Alaa Al-Din Al-Radhi for providing me such good guidance.

6. References

[1] Al-Radhi, A, A. 2011. *IPv6 Promised Role in Mitigating Cyber Attacks: Really it's Time!.* Swiss Cyber Storm-International IT Security Conference, Switzerland.

[2] Khaldoun, B. Khaled, B. Amer, A. 2011. *THE NEED FOR IPv6*. International Journal of Academic Research, Vol. 3. No. 3. II Part. PP.431-448, Azerbaijan. http://www.ijar.lit.az

[3] Minoli, D. Kouns, J. 2009. *Security in an IPv6 Environment.* CRC Press, USA.

[4] Davies, J. 2008. *Understanding IPv6*. 2nd edition. Microsoft Press, USA.

[5] Hogg, S. Vyncke, E. 2009. *IPv6 Security*, Cisco Press, USA.

[6] White Paper, (Published: September 2003 & Updated: January 2008). *Microsoft Windows Server 2008, Introduction to IP Version 6*, Microsoft Corporation, USA.

[7] White paper 2004. *IPv6 and IPv4 Threat Comparison and Best Practice Evaluation(v1.0)* , Cisco Press, USA.

[8] Szigeti, S.; Risztics, P. 2004. *Will IPv6 bring better security?. Proceedings 30th Euromicro Conference*, vol., 532- 537, 31 Aug.-3 Sept.

[9] Sotillo, S. 2006. *IPv6 Security Issues*. East Carolina University, USA.

[10] Choudhary, A. R. Sekelsky, A. 2010. *Securing IPv6 Network Infrastructure: a New Security Model*. *IEEE Conference,* USA.

[11] Blanchet, M. 2006. Migrating to IPv6. *John Wiley & Sons Ltd, England.*

[12] Hagen, S. 2006. *IPv6 Essentials*, 2nd edition. O'Reilly Media.

[13] Popoviciu, C. Abegnoli, E. L. Grossetete, P. 2006. *Deploying IPv6 Networks*. Cisco Press, USA.

[14] Karlsson, B. 2003. *Cisco Self-Study: Implementing IPv6 Networks (IPV6).* Cisco Press, USA.

[15] Li, Q. Jinmei, T. Shima, K. 2009. *Mobile IPv6: Protocols and Implementation,* Elsevier Inc. USA.

[16] Hauser, V. 2008. *Attacking the IPv6 Protocol Suite*, The Hacker's Choice, http://www.thc.org/thc-ipv6.

[17] Cisco IOS Learning Services. 2002. *The ABCs of IP Version* 6, Cisco Press, http://www.cisco.com/go/abc.

[18] White Paper, October 2011, *IPv6 Security Brief*, Cisco Press.

[19] Yoo, H. S. Cagalaban, G. A. Kim, S. H. 2009, *A Study on the Connectivity of IPv6 to IPv4 Domains and Its Security Issues*, International Journal of Advanced Science and Technology, Vol. 10, Korea.

[20] Merike, K. Green D. Bound, J. and Pouffary, Y. July 2006. *IPv6 Security Technology Paper.* North American IPv6 Task Force (NAv6TF) Technology Report, http://www.nav6tf.org/documents/nav6tf.security_report.pdf

[21] Warfield, M. H. 2003. *Security Implications of IPv6 Whitepaper*. Internet Security Systems, http://documents.iss.net/whitepapers/IPv6.pdf.

[22] Santos, O. 2008. *End-To-End Network Security: Defense-In-Depth.* Cisco Press, USA.

[23] Hardjono, T. and Dondeti, L. R. 2003. *Multicast and Group Security.* Artech House computer security series. USA.

[24] White Paper. May, 2011. *IPv6 Security v1.1.* The Government of the Hong Kong Special Administrative Region.

[25] Ferguson, N. and Schneier, B. 2002. *A Cryptographic Evaluation of IPsec*, Counterpane Labs, http://www.counterpane.com/ipsec.html

[26] Gelogo, Y. E. Caytiles, R. D. Park, B. December, 2011. *Threats and Security Analysis for Enhanced Secure Neighbor Discovery Protocol (SEND) of IPv6 NDP Security*, International Journal of Control and Automation Vol. 4, No. 4. PP:179-184.

[27] Narten, T. Nordmark, E. Simpson, W. Soliman, H. September 2007. *Neighbor Discovery for IP version 6 (IPv6)*, Internet Engineering Task Force: RFC 4861, http://www.ietf.org/rfc/rfc4861.txt