Information Technology Seminar 2008
Kolej Yayasan Melaka, 16 October 2008

IPv6 and IPv4 Security Issues

Mohd Zaki Mas'ud, Erman Hamid, Nazrulazhar Bahaman, Abdul Samad Shibghatullah
Fakulti Teknologi Maklumat dan Komunikasi
Universiti Teknikal Malaysia Melaka
Zaki.masud@utem.edu.my

Abstract

In the near future IPv6 is said to become the new version of internet protocol replacing IPv4 protocol. Other than providing huge populated address, IPv6 also provides simplicity in configuration, routing speed, quality of services and more importantly improve the security mechanism. The deployment of IPv6 will not occur over night but it may take several years. Several methods have been found to be applied in the transition of IPv6 to IPv4 protocol. As IPv6 is not yet in full throttle there are possibilities of intrusion and computer threat especially during the transition period. This paper reviews the security threats of an IPv4 and how it's going to effect the implementation of IPv6.

Keywords: *IPv6; Network security; IPSec; Network threat;*

1. Introduction

Internet today has growth to million networks and one of the direct results is the exhaustion of IP address. It is predict that by 2011 the IP address for IPv4 will be depleted [1]. With the growth of wireless technology nowadays, IPv4 have to be replaced with a new protocol to support the huge request for IP address. The next generation protocol or IPv6 is the only options we have right now. The enormous size of IPv6 address can map for every observable star in the known universe with 2^{52} addresses, this comparison is just to show how IPv6 provides unlimited IP address. Each IPv6 addresses is represented with 128 bit compare to 32 bit for IPv4. The huge number of IPv6 addresses itself contribute a significance improvement for IPv6 security.

Another improvement in IPv6 protocol is the mandate requirement for Internet Security Protocol (IPsec) it its implementation [2]. Even though IPsec can be implemented in IPv4 but it just an optional option. IPsec is a suite of protocols for securing each packet in the data stream by providing authentication or encryption services in Internet Protocol (IP) communications. IPsec is implemented in layer 3 of the OSI model, thus providing the security services for the entire upper layer in the OSI model. By providing security in the lower level, an application does not need to incorporate IPsec in its design. IPsec incorporated two other protocols namely Authentication Header (AH) and Encapsulating Security payload (ESP) in which it help to authenticate IP source and encrypting the payload in packet.

Almost twenty years, IPv4 is already synonym with Internet Protocol, with a large infrastructure supporting IPv4; it will take several years to replace it with Ipv6. The most crucial point in implementing IPv6 is during the transition period of IPv4 to IPv6 in which will show whether the threat in IPv4 is still affecting this next generation IP or not or maybe it just going to generate a new challenge in protecting the network. This paper discuses the current computer threat in IPv4 and how IPv6 features handle the threats. Second section of this paper discusses the threat found in IPv4. In Section 3 discuss how the features in IPv6 can overcome the threat and section 4 discusses the security issues of IPv6 transition. Finally section 5 conclude and discuss the next direction of this research.

2. IPv4 Security threat

During the development of IPv4, Information Technology security is not one of the focus points [3]. This had caused a lot of loop hole that can be exploited in the IPv4 implementation. Even though there is a lot of methods (SSL, SSH and etc) introduce to overcome this weaknesses, still it is not enough. In a network attack, five phases are involves in exploiting IPv4 environment [4], which are Reconnaissance, Scanning, Gaining access, Maintaining access, and Clearing track. The first two phases involve a process of scanning for vulnerabilities in the host networks. Once vulnerabilities are exposed the process of gaining access is executed.

Freely available on the Internet, port scanning tools like Nmap [5] and Wireshark [6] can be used to execute the reconnaissance and scanning phase. As the number of IPv4's addresses is small, scanning a class C network take only a few minute. This show how vulnerable is IPv4 network, with a few minute all open access can be expose.

Address Resolution Protocol (ARP) and Internet Control Message Protocol (ICMP) are two protocols in layer 4 used for finding a host's hardware address and protocol for responding of error in datagram respectively. In an attack these two can be exploited by associating the packet with a fake address resulting in other packet to be mistakenly sent to a rogue address.

IP fragmentation referred to IP datagram that is broken up to smaller size. This is to make the IP datagram to pass through the data link medium which has a limit on the size of transmitting frame called Maximum Transmission unit (MTU). An attacker use this features to evade from being detected by firewall and Network Intrusion Detection System (NIDS)

Broadcast features in IPv4 can also be exploited. Huge number of frame is broadcast through a network can flood the network system. This large number of look alike legitimate packet will cause the hosts from receiving any valid packet.

Packet in IPv4 can be intercepted during it transmission by eavesdropping on the network. This attack is called man in the middle attack and its occurs as a result of lack of authentication mechanism provided in IPv4 protocol. This can be done by applying ARP attack as stated above.

In order to prevent all this threat extra tools is used to harden the network security in IPv4 environment. Application like Network Address Translation (NAT) is used to overcome the scanning of private network and also to overcome the shortage of IPv4's addresses. Firewall and IDS is deploy to protect and detect any anomalies in the network. Access Control List (ACL) can be applied in network to drop any packets that can cause security problem in the networks.

3. Security Features in IPv6

The fact that IPv6 is design with security is taken in its development not necessarily conclude that it is better than IPv4. There is a lot of unknown security threat that is not yet covered in IPv6 as it is not 100% deployed. This section review the security features that is offered in its protocol and how it can improved the network security in preventing the threat in the previous section.

First, the large address number of IP address provided in IPv6 can prevent the spoofing attack in the early phase of an attack. The fact that it uses 128 bit for it address will result in a larger number of host address to be scan. Samuel [7] shows that it only takes 4 minutes to scan all available hosts in a class C subnet that allocate 8 bits for host addressing. Whereas in IPv6, it takes billion of years to scan a subnets, this is due to the usage of 64 bits for allocating host address in its subnet. Although IPv6 have a large number of addresses but it is still possible to scan an IPv6 networks.

The major improvement in IPv6 is the mandate usage of IPsec. Even though it can also be implemented in IPv4, it stills an optional option and only applied in the host level. IPsec uses AH and ESP protocol which provide data authentication, data integrity and data confidentiality between two hosts.

AH provides data origin authentication and data integrity. Thus preventing host from IP spoofing and also prevent replay old datagram. AH applied digest algorithm like keyed MD5 or keyed-SHA, in order to provide a mechanism to proof the sender identity [8]. In the other hand ESP, provides encryption of data in ensuring only the sender and the receiver can read the data. Both AH and ESP can prevent from any man in the middle attack.

In order to standardize the algorithm and the key encryption used in AH and ESP, IPsec also introduce a key management system called Internet Key Exchange (IKE).IKE responsible to establish and negotiating a standard security parameter between two hosts. This implementation is similar to Public Key Infrastructure (PKI) which is part of the digital signature infrastructure where both of the sender and receiver must have the public and private key in order to proof the origin of the data.

IPv6 protocol has removed the concept of broadcast, thus eliminating Denial of service attack that based on the broadcast concept. The same goes for fragmentation attack, IPv6 do not allowed datagram fragmentation by intermediary devices as it going to be done at the source node.

ARP attack will become more difficult as the ARP itself is replaced with an element of ICMPv6 that is Neighbour Discovery (ND). However, [9] stated that there are still some issues to be resolved before ARP attack is permanently avoided as the current method is still inheriting ARP in IPv4.

4. IPv4 to IPv6 Transition Issues

The transition from IPv4 protocol to IPv6 protocol will take several years to happen. During this transition period a thorough study must be given on the security aspect of the network. It is an accepted fact that before IPv6 can be fully implemented it need to be coexist with it predecessor IPv4. This indeed will expose the host with the vulnerabilities found in IPv4 and also unknown vulnerabilities of IPv6 if it is not configured correctly. Two techniques are currently applied in the transition process which is the dual stack mechanism and the tunneling mechanism [10].

In Dual stack infrastructure both IPv4 and IPv6 are applied in the same level as depicted in figure 1. Implementing both of the protocol together will fabricate a new scenario in security management especially if the setting is wrongly configured. This will expose the host to two kinds of security problems.

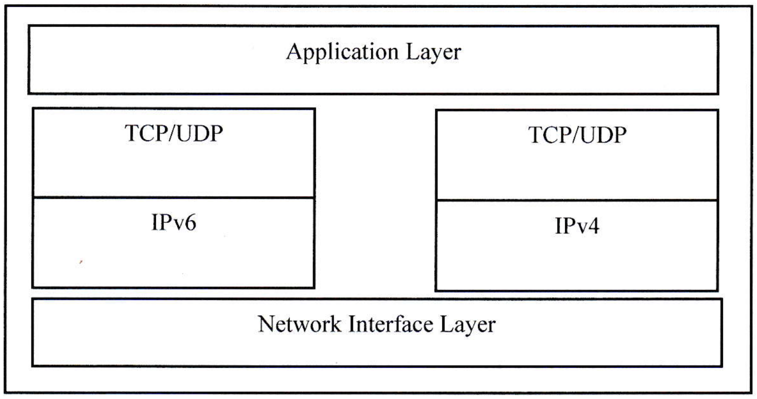

Figure 1: Dual Stack Architecture

Whereas, Tunneling techniques known as 6to4 encapsulate the packet of IPv6 with an IPv4 header in order to transmit IPv6 through IPv4 infrastructure, as depicted in figure 2. A malicious packet can masquerade as an external packet originated from the inside network, if the security policy is not carefully define it will become a route for an attack.

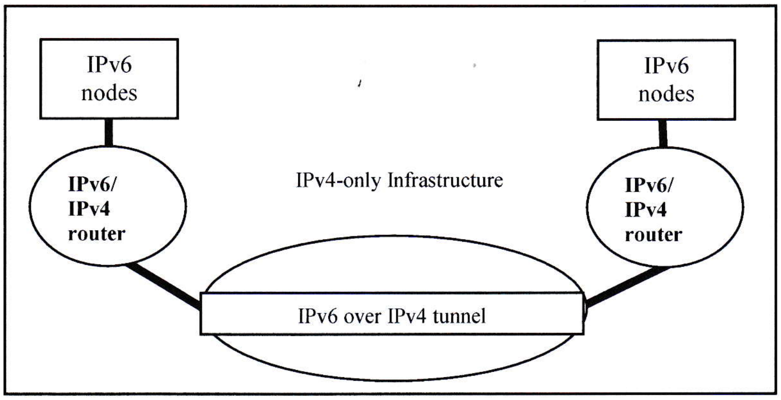

Figure 2: Tunnelling

Convey and Miller [9] Suggested three recommendations in implementing the right techniques in transition of IPv4 to IPv6. In dual stack technique they suggest administrator to use either native IPv6 or IPv4 services because it policy is better understood compared to translation. In tunneling techniques they recommend using static tunneling rather than dynamic tunneling as static tunneling give better trusting relationship between two points and finally implementing filtering of packets that goes outside the network for allowing only authorized tunneling endpoints.

5. Conclusion

There is no doubt after certain period IPv6 will be replacing IPv4. Although there are a lot of security improvements in IPv6 such as huge number of IP addresses, easier configuration and mandatory usage of IPsec, still the result of it effectiveness can only be tested when it is fully deploy meanwhile the unknown effect is still waiting during the transition period. Configuration must carefully done so that any threat in IPv4 will not be occurring in the IPv6 environment. Packet filtering and intrusion detection must be deployed during this transition period in order to achieve the highest possibility security level.

This paper is part of the preliminary studies on finding the security issues pertaining to the transition of IPv6 to IPv4. In the near future a few experiments will be done to see whether the security treats mention in this paper really can be prevented when we moved to the IPv6 environment.

Reference

[1] http://www.potaroo.net/tools/ipv4/index.html

[2] http://tools.ietf.org/html/rfc2411

[3] Szaboles Svigeti, Peter Risztics Will IPv6 Bring Better Security?, Proceedings of the 30th EUROMICRO Conference,2004

[4] certified ethical hacking course

[5] http://nmap.org/

[6] http://www.wireshark.org/

[7] Samuel Sotilo, IPv6 Security Issues, 2006

[8] www.cu.ipv6tf.org/literatura/chap8.pdf

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

[10] IPv6 Transition Technologies, Microsoft Corporation, 2008