

# IPv6 SECURITY

**May 2011**

© The Government of the Hong Kong Special Administrative Region

The contents of this document remain the property of, and may not be reproduced in whole or in part without the express permission of the Government of the HKSAR.

**Disclaimer:** Whilst the Government endeavours to ensure the accuracy of the information in this paper, no express or implied warranty is given by the Government as to the accuracy of the information. The Government of HKSAR accepts no liability for any error or omission arising from or related to the use of the information.

## TABLE OF CONTENTS

Summary .....	3
1 Introduction .....	4
2 Security Considerations .....	6
A. Security Improvements Over IPv4.....	6
B. Concerns, Potential Threats and Measures .....	8
C. Common Attacks In Both IPv4 and IPv6 .....	11
D. IPv6 Transition .....	12
3 Best Practices.....	14

## SUMMARY

The IPv6 protocol has solved some, but not all, of the security problems found in IPv4 networks. One example is the mandatory inclusion of IP Security (IPsec) in the IPv6 protocol, which makes it fundamentally more secure than the older IPv4 standard. However, given its flexibility, the IPv6 protocol introduces new problems. A mobile IP protocol is built into the IPv6 protocol, and security solutions for this protocol are still under development.

In addition, the dynamic configuration flexibility of IPv6 (such as stateless address auto-configuration) could also become a serious security problem, if not implemented correctly. The overall enhancements in IPv6 may provide better security in certain areas, but there are areas that attackers may be able to exploit. This article will focus on the security improvements over IPv4, possible threats, security considerations and some best practices on IPv6 deployment.

# 1 INTRODUCTION

The prevailing Internet Protocol standard is IPv4 (Internet Protocol version 4), which dates back to the 1970s. There are well-known limitations of IPv4, including the limited IP address space and lack of security. IPv4 specifies a 32-bit IP address field, and available address spaces are rapidly running out. The only security feature provided in IPv4 is a security option field that provides a way for hosts to send security and handling restrictions parameters<sup>1</sup>.

As a result, the Internet Engineering Task Force (IETF) has been working on the IPv6 (Internet Protocol version 6) specifications in order to address these limitations, along with a number of performance, ease-of-configuration, and network management issues. The core IPv6 specifications have been defined by various Request for Comments (RFCs) such as RFC 2460<sup>2</sup> (IPv6 Protocol), RFC 4861<sup>3</sup> (IPv6 Neighbour Discovery), RFC 4862<sup>4</sup> (IPv6 Stateless Address Auto-Configuration), RFC 4443<sup>5</sup> (Internet Control Message Protocol for IPv6 (ICMPv6)), RFC 4291<sup>6</sup> (IPv6 Addressing Architecture), and RFC 4301<sup>7</sup> (Security Architecture for IP or IPsec). IPv6 is also referred as the Next Generation

---

<sup>1</sup> <http://www.ietf.org/rfc/rfc0791.txt>

<sup>2</sup> <http://tools.ietf.org/html/rfc2460>

<sup>3</sup> <http://tools.ietf.org/html/rfc4861>

<sup>4</sup> <http://tools.ietf.org/html/rfc4862>

<sup>5</sup> <http://tools.ietf.org/html/rfc4443>

<sup>6</sup> <http://tools.ietf.org/html/rfc4291>

<sup>7</sup> <http://tools.ietf.org/html/rfc4301>

Internet Protocol (IPng). The differences between IPv6 and IPv4 headers are outlined in the tables below:

1. IPv6 header format

**IPv6 Header**

Version	Traffic Class	Flow Label	
Payload Length		Next Header	Hop Limit
Source Address			
Destination Address			

2. IPv4 header format

**IPv4 Header**

Version	IHL	Type of Service	Total Length	
Identification		Flags	Fragment Offset	
Time to Live	Protocol	Header Checksum		
Source Address				
Destination Address				
Options			Padding	

The new features introduced with the IPv6 protocol can be summarised as:

1. A new header format
2. A much larger address space (128-bit in IPv6, compared to the 32-bit address space in IPv4)
3. An efficient and hierarchical addressing and routing infrastructure
4. Both stateless and stateful address configuration

5. IP Security
6. Better Quality of Service (QoS) support
7. A new protocol for neighbouring node interaction
8. Extensibility

These enhancements in IPv6 provide better security in certain areas, but some of these areas are still open to exploitation by attackers.

## 2 SECURITY CONSIDERATIONS

### A. Security Improvements Over IPv4

#### 1. Massive Size of the IP Address Space

##### *Makes Port Scanning Harder*

When they start, attackers usually employ port scanning as a reconnaissance technique to gather as much information as possible about a victim's network. It is estimated that the entire IPv4 based Internet can be scanned in about 10 hours with enough bandwidth<sup>8</sup>, given that IPv4 addresses are only 32 bits wide. IPv6 dramatically increases this limit by expanding the number of bits in address fields to 128 bits. By itself, such a massive address space creates a significant barrier for attackers wanting to conduct comprehensive port scanning.

---

<sup>8</sup> <http://www.opte.org/history/>

However, it should be noted that the port scanning reconnaissance technique used in IPv6 is basically the same as in IPv4, apart from the larger IP address space. Therefore, current best practices used with IPv4, such as filtering internal-use IPv6 addresses in border routers, and filtering un-used services at the firewall, should be continued in IPv6 networks.

### *Cryptographically Generated Address (CGA)*

In IPv6, it is possible to bind a public signature key to an IPv6 address. The resulting IPv6 address is called a Cryptographically Generated Address (CGA)<sup>9</sup>. This provides additional security protection for the IPv6 neighbourhood router discovery mechanism, and allows the user to provide a "proof of ownership" for a particular IPv6 address. This is a key differentiator from IPv4, as it is impossible to retrofit this functionality to IPv4 with the current 32-bit address space constraint. CGA offers three main advantages:

1. It makes spoofing attacks against, and stealing of, IPv6 addresses much harder.
2. It allows for messages signed with the owner's private key.
3. It does not require any upgrade or modification to overall network infrastructure.

## 2. IP Security (IPsec)<sup>10</sup>

IP Security, or IPsec for short, provides interoperable, high quality and cryptographically based security services for traffic at the IP layer. It is optional in IPv4 but has been made mandatory in the IPv6 protocol. IPsec enhances the original IP protocol by providing authenticity, integrity, confidentiality and access control to each IP packet through the use of two protocols: AH (authentication header) and ESP (Encapsulating Security Payload).

---

<sup>9</sup> Cryptographically Generated Addresses (CGA) is specified in RFC 3972 (<http://www.ietf.org/rfc/rfc3972.txt>).

<sup>10</sup> RFC4301 (<http://tools.ietf.org/html/rfc4301>)

### 3. Replacing ARP by Neighbour Discovery (ND) Protocol

In the IPv4 protocol, a layer two (L2) address is not statically bound to a layer three (L3) IP address. Therefore, it can run on top of any L2 media without making significant change to the protocol. Connection between L2 and L3 addresses is established with a protocol named Address Resolution Protocol (ARP), which dynamically establishes mapping between L2 and L3 addresses on the local network segment. ARP has its own security vulnerabilities (such as ARP Spoofing). In the IPv6 protocol, there is no need for ARP because the interface identifier (ID) portion of an L3 IPv6 address is directly derived from a device-specific L2 address (MAC Address). The L3 IPv6 address, together with its locally derived interface ID portion, is then used at the global level across the whole IPv6 network. As a result, the security issues related to ARP no longer apply to IPv6. A new protocol called Neighbour Discovery (ND) Protocol for IPv6 is defined in RFC 4861<sup>11</sup> as a replacement to ARP.

## B. Concerns, Potential Threats and Measures

### 1. IP Addressing Structure

The IP addressing structure defines the architecture of a network. A well-planned addressing structure will reduce potential risks associated with new features provided by IPv6. The following areas should be considered when designing an IPv6 network.

#### Numbering plan and hierarchical addressing

The numbering plan describes how the organisation segregates its IPv6 allocation, for example, if an organisation is granted with a 16 subnet bits (/48) address block, this will

---

<sup>11</sup> <http://tools.ietf.org/html/rfc4861>

allow to support 65,000 subnets. A good numbering plan can simplify access control lists and firewall rules in security operations, and identify ownership of sites, links and interfaces easily. Organisations should carefully plan and create a site hierarchy by consider subnet methods as follows:

- Sequentially numbering subnets
- VLAN number
- IPv4 subnet number
- Physical location of network
- Functional unit of an organisation (Accounts, Operation, etc)

#### Problems with trackable EUI-64 addresses

The IEEE EUI-64 address<sup>12</sup> represents a new standard for network interface addressing in IPv6. Physical address of the network interface (MAC address) is an input to the algorithm that generates EUI-64 address for network interfaces. With the capability of auto-configuration, a global IPv6 address for the interface can be generated by combining the network identifier with the EUI-64 address. By using a EUI-64 address, an attacker could potentially reveal the make and model of a remote machine, and use the information to target attacks. To mitigate the risk, non-predictable addresses should be used by making use of cryptographic algorithm (e.g. Cryptographically Generated Address) or assigning addresses with DHCPv6.

## 2. Unauthorized IPv6 Clients

IPv6 support is available for most modern operating systems or equipment, it can be easy and sometime unnoticeable to user where the IPv6 protocol is enabled. Due to the

---

<sup>12</sup> EUI is an acronym for Extended Unique Identifier, e.g. "3BA7:94FF:FE07: CBD0" is an EUI-64 identifier in colon hexadecimal notation.

extended capabilities of IPv6, as well as the possibility of an IPv6 host having a number of global IPv6 addresses, it potentially provides an environment that make network level access easier for attacker if the access controls are not properly deployed.

To reduce the risk, the following measures could be considered:

- Locate and disable any IPv6 enabled equipment
- Detect and block IPv6 or IPv6 tunnel traffic at network perimeter
- Include IPv6 usage policies in the organization's security plan

### 3. Neighbour Discovery and Stateless Address Auto-configuration

Neighbour discovery (ND) is a replacement for ARP, and stateless address auto-configuration—which allows an IPv6 host to be configured automatically when connected to an IPv6 network—is a lightweight DHCP-like function provided in ICMPv6. They are both powerful and flexible options in the IPv6 protocol. However, ND may be still subject to attacks that could cause IP packets to flow to unexpected places. Denial of service may be one of the results. Also, such attacks could be used to allow nodes to intercept and optionally modify packets destined for other nodes. While this may be protected with an IPsec AH, RFC 3756<sup>13</sup> (IPv6 ND Trust Models and Threats) also defines the type of networks in which the secure IPv6 ND mechanisms are expected to work. The three different trust models can roughly corresponding to secured corporate intranets, public wireless access networks, and pure ad hoc networks. Moreover, the SEcure Neighbor Discovery (SEND) protocol is developed to provide an alternate mechanism for securing neighbor discovery with a cryptographic method.

Neighbour discovery, as well as router solicitation in the IP network (v4 or v6) uses ICMP. While ICMPv4 is a separate protocol on the outside of IPv4, ICMPv6 is an

---

<sup>13</sup> <http://tools.ietf.org/html/rfc3756>

integral protocol running directly on the top of the IPv6 protocol, which again could lead to security problems.

Exchanging ICMPv6 messages on the top of the IPv6 protocol for vital "network health" messages and environment solicitations are crucial for IPv6 communication. However, this could be abused by sending fake, carefully crafted response messages for denial of service, traffic re-routing or other malicious purposes. For security reasons, the IPv6 protocol recommends that all ICMP messages use an IPsec AH, which is able to offer integrity, authentication and anti-relay functions.

It may be better to specify critical systems as static neighbour entries to their default router, instead of using ND, this would avoid many typical neighbour-discovery attacks. However, certain administrative efforts would be required.

#### 4. Dual Operations

Organisations cannot change all their networks to IPv6 overnight, IPv6 will be gradually deployed while IPv4 will be supported for legacy clients and services. A dual protocol environment increases the complexity for operations and also security. Nevertheless, existing measures on IPv4 should be maintained while the same level of coverage should be applied to IPv6. Organisations need to implement a consistent security policy for both IPv4 and IPv6 (including firewalls and packet filters). During operations, administrators should be aware of relevant threats and vulnerabilities in both protocols and apply appropriate measures to mitigate the risks.

### **C. Common Attacks In Both IPv4 and IPv6**

IPv6 cannot solve all security problems. Basically it cannot prevent attacks on layers above the network layer in the network protocol stack. Possible attacks that IPv6 cannot address include:

1. Application layer attacks: Attacks performed at the application layer (OSI Layer 7) such as buffer overflow, viruses and malicious codes, web application attacks, and so on.
2. Brute-force attacks and password guessing attacks on authentication modules.
3. Rogue devices: Devices introduced into the network that are not authorised. A device may be a single PC, but it could be a switch, router, DNS server, DHCP server or even a wireless access point.
4. Denial of Service: The problem of denial of service attacks is still present with IPv6.
5. Attacks using social networking techniques such as email spamming, phishing, etc.

#### **D. IPv6 Transition**

Transitioning tools allow IPv4 applications to connect to IPv6 services, and IPv6 applications to connect to IPv4 services. However, attackers might exploit this if the security issues have not been fully addressed.

There are a variety of IPv6 transition technologies, such as 6to4 (defined in RFC 3056<sup>14</sup>), Simple Internet Transition<sup>15</sup> (SIT) tunnels, and IPv6 over UDP (such as Teredo<sup>16</sup>). IPv6

---

<sup>14</sup> <http://tools.ietf.org/html/rfc3056>

<sup>15</sup> <http://playground.sun.com/ipv6/ipng-transition.html>

traffic can enter networks via these methods while administrators are not aware that networks are vulnerable to IPv6 exploits. In addition, many firewalls permit UDP traffic, allowing IPv6 over UDP to get through firewalls without the knowledge of administrators. Attackers might also use 6to4 tunnels to evade intrusion detection or prevention systems. Some firewall products are only capable of filtering IPv4 traffic and not IPv6 traffic. Attackers can exploit this loophole and hence compromise the network by using IPv6 packets.

SIT tunnels and tunnelling routers make it possible to deploy islands of IPv6, within sea of IPv4 networks, without IPv6 routers being directly connected to each other. This arrangement allows intruders to subvert simple workstations and use them as routers to direct traffic across entire sub-networks without having to compromise infrastructure routers or firewalls. To inspect encapsulated traffic within tunnels, deploy security devices that can understand tunnelled traffic. Moreover, security policies should be enforced at both the inbound and outbound of the tunnel.

For host security on IPv4-IPv6 mixed networks, it should also be noted that applications are subject to attacks in both IPv6 and IPv4 networks. Therefore, if traffic blocking is required, it is necessary to block traffic for both IP versions on any host control systems (firewalls, VPN clients, intrusion detection or prevention systems, and so on). IPv6 network traffic should be monitored, router and neighbor solicitations should be audited to detect the insertion of any rogue router or unauthorised device to the network.

---

<sup>16</sup> <http://technet.microsoft.com/en-us/network/cc917486.aspx>

### 3 BEST PRACTICES

Below are some best practices for reference in building and maintaining secure IPv6 networks:

- Use standard, non-obvious static addresses for critical systems;
- Ensure adequate filtering capabilities for IPv6;
- Filter internal-use IPv6 addresses at border routers;
- Block all IPv6 traffic on IPv4-only networks;
- Filter unnecessary services at the firewall;
- Develop a granular ICMPv6 filtering policy and filter all unnecessary ICMP message types;
- Maintain host and application security with a consistent security policy for both IPv4 and IPv6;
- Use IPsec to authenticate and provide confidentiality to assets;
- Document the procedures for last-hop traceback; and
- Pay close attention to the security aspects of transition mechanisms.

Last Update/Review: May 2011