The Study on Security Vulnerabilities in IPv6 Autoconfiguration

Myung-Eun Kim*, Dong-il Seo**

* Department of Network Security, ETRI, Daejeon, Korea
(Tel : +82-42-860-5303; E-mail: mekim@etri.re.kr)

**Department of Network Security, ETRI, Daejeon, Korea
(Tel : +82-42-860-3814; E-mail: bluesea@etri.re.kr)

Abstract: According as computer is supplied in a lot of homes and offices and Internet use increases, various service based on the Internet. Including wireless PDA in the future, many devices such as Internet telephone, TV, refrigerator and oven will be connected on the Internet and Internet address exhaustion will be raised to serious problem gradually. Today, the IPv4 address exhaustion problem has been solved partially using NAT (Network Address Translation) however, the transition to next Generation Internet will be accelerated because of advantages such as mobility, security service, QoS, and abundant IP addresses. In IPv6, all hosts are designed to create and set their address automatically without manager’s intervention using Neighbor Discovery Protocol. But, when an IPv6 host sets its address automatically, there are serious security vulnerabilities. In this paper, we analyze security vulnerabilities in auto-configuration and provide security requirements for secure auto-configuration.

Keywords: IPv6, secure auto-configuration, security vulnerability, neighbor discovery protocol

1. INTRODUCTION

Recently, by entrance on the stage of digital home, interest about field of Internet information electronic is rising gradually regarding home networking. Including wireless PDA in the future, many devices such as Internet telephone, TV, refrigerator and oven will be connected on the Internet and problem called Internet address exhaustion will be raised to serious problem gradually. Number of available address that is calculated by experts is forecasted about 500 million however, More than 70% of 4300 million is already allocated November 2001 and the exhaustion of IPv4 address is expected all over the world around 2005. To solve these problems IETF (Internet Engineering Task Force) developed IPv6 standard (IP version 6, RFC2460). The IPv6 was standardized in 1996 as a Next Generation Internet address and it has 128 bit addresses length that can generate about \(3.4 \times 10^{38}\) addresses. Also the IPv6 offers new function such as new address that is extended from 32 bits to 128bits, the setting of life time, auto-configuration and anycast. In addition, the IPv6 offers more powerful security by providing extension header to support authentication, data integrity and data secret preservation.

Some advanced nations including The United States of America, Europe and Japan already knew IPv4’s limit and have prepared the conversion from IPv4 to IPv6. Recently they are spurring in technical development for IPv6’s introduction to preoccupy high position in Next generation network development. Now, the IPv6 has an important role as a next generation network infrastructure as well as a solution of IP address exhaustion. Hereafter, various electronic devices in home and office may create own IP address without manager’s intervention using IPv6 auto-configuration and connect on Internet by oneself, if IPv6 will be a next generation network infrastructure. However, many researchers have indicated some security problems of auto-configuration, which is the leakage of an IPv6 device’s important configuration information. So many researchers have studied about methods for secure address generation.

In this paper, we analyze security vulnerability of IPv6 auto-configuration and we wish to quote security technology development direction by examining about secure address generation technique that is studying present.

2. NEIGHBOR DISCOVERY PROTOCOL

2.1 Overview

The IPv6 Neighbor Discovery protocol corresponds to a combination of the IPv4 protocols ARP, ICMP Router Discovery, and ICMP Redirect. This protocol solves a set of problems related to the interaction between nodes attached to the same link. It defines mechanisms for solving each of the following problems:

- Router Discovery: How hosts locate routers that reside on an attached link
- Prefix Discovery: How hosts discover the set of address prefixes that define which destinations are on-link for an attached link
- Parameter Discovery: How a node learns such link parameters as the link MTU or on-link Internet parameters as the hop limit value to place in outgoing packets
- Address Autoconfiguration: How nodes automatically configure an address for an interface
- Address resolution: How nodes determine the link-layer address of an on-link destination given only the destination’s IP address
- Next-hop determination : The algorithm for mapping an IP destination address into the IP address of the neighbor to which traffic for the destination should be sent. The next-hop can be a router or the destination itself
- Neighbor Unreachability Detection: How nodes determine that a neighbor is no longer reachable. For neighbors used as routers, alternate default routers can be performed again.
- Duplicate Address Detection: How a node determines that an address it wishes to use is not already in use by another node
- Redirect: How a router informs a host of a better first-hop node to reach a particular destination.
2.2 Neighbor Discovery Message

Neighbor Discovery defines five different ICMP packet types such as a pair of Router Solicitation and Router Advertisement messages, a pair of Neighbor Solicitation and Neighbor Advertisements message, and a Redirect message.
- Router Solicitation: When an interface becomes enabled, hosts may send out Router Solicitations that request routers to generate Router Advertisements immediately rather than at their next scheduled time.
- Router Advertisement: Routers advertise their presence together with various link and Internet parameters either periodically, or in response to a Router Solicitation message. Router Advertisements contain prefixes that are used for on-link determination and/or address configuration, a suggested hop limit value etc.
- Neighbor Solicitation: Sent by a node to determine the link-layer address of a neighbor, or to verify that a neighbor is still reachable via a cached link-layer address. Neighbor Solicitations are also used for Duplicate Address Detection.
- Neighbor Advertisement: A response to a Neighbor Solicitation message. A node may also send unsolicited Neighbor Advertisements to announce a link-layer address change
- Redirect: Used by routers to inform hosts of a better first hop for a destination

2.3 Neighbor Discovery Process

2.3.1 Router and Prefix Discovery

Router Discovery is used to locate neighboring routers as well as learn prefixes and configuration parameters related to address autoconfiguration. Prefix Discovery is the process through which hosts learn the ranges of IP addresses that reside on-link and can be reached directly without going through a router. Routers send Router Advertisements that indicate whether the sender is willing to be a default router. Router Advertisements also contain Prefix Information options that list the set of prefixes that identify on-link IP addresses.

Stateless Address autoconfiguration must also obtain subnet prefixes as part of configuring addresses. Although the prefixes used for address autoconfiguration are logically distinct from those used for on-link determination, autoconfiguration information is piggybacked on Router Discovery messages to reduce network traffic.

2.3.2 Next Hop Determination

Next-hop determination for a given unicast destination operates as follows. The sender performs a longest prefix match against the Prefix List to determine whether the packet’s destination is on-link or off-link. If the destination is on-link, the next-hop address is the same as the packet’s destination address. Otherwise, the sender selects a router from the Default Router List. If the Default Router List is empty, the sender assumes that the destination is on-link.

For efficiency reasons, next-hop determination is not performed on every packet that is sent. Instead, the results of next-hop determination computations are saved in the Destination Cache. When the sending node has a packet to send, it first examines the Destination Cache. If no entry exists for the destination, next-hop determination is invoked to create a Destination Cache entry.

2.3.3 Address Resolution

Address resolution is the process through which a node determines the link-layer address of a neighbor given only its IP address. Address resolution is performed only on addresses that are determined to be on-link and for which the sender does not know the corresponding link-layer address. Address resolution is never performed on multicast addresses.

2.3.4 Neighbor Unreachability Detection

Neighbor Unreachability Detection is used for all paths between hosts and neighboring nodes, including host-to-host, host-to-router, and router-to-host communication. Neighbor Unreachability Detection may also be used between routers, but is not required if an equivalent mechanism is available, for example, as part of the routing protocols.

When a path to a neighbor appears to be failing, the specific recovery procedure depends on how the neighbor is being used. If the neighbor is the ultimate destination, for example, address resolution should be performed again. If the neighbor is a router, however, attempting to switch to another router would be appropriate. The specific recover that takes place is covered under next-hop determination. Neighbor Unreachability Detection is performed only for neighbors to which unicast packets are sent. It is not used when sending to multicast addresses.

2.3.5 Redirect

Redirect messages are sent by routers to redirect a host to a better first-hop router for a specific destination or to inform hosts that a destination is in fact a neighbor (i.e., on-link). The latter is accomplished by having the ICMP Target Address be equal to the ICMP Destination Address.

A router must be able to determine the link-local address for each of its neighboring outers in order to ensure that the target address in a Redirect message identifies the neighbor router by its link-local address. For static routing this requirement implies that the next-hop router’s address should be specified using the link-local address of the router. For dynamic routing this requirement implies that all IPv6 routing protocols must somehow exchange the link-local addresses of neighboring routers.

3. AUTO-CONFIGURATION IN IPv6

As preceding section refers, An IPv6 device can configure automatically and connect to network even if it does not use stateful configuration protocol such as DHCPv6. Basically, An IPv6 device can generate link-local address in each interface and resolve global site-local address using router address, other configuration parameter and on-link prefix. When An IPv6 device connects to network, it uses the one of two address setting methods for initialization. One is stateful auto-configuration that acquires address from DHCP server, the other is Stateless auto-configuration that an IPv6 device generates own address by oneself.

The stateful auto-configuration method is that a DHCP server allocates one of addresses that are managed in it, if an IPv6 device requests address to a DHCP server. In the stateful auto-configuration method, a DHCP server must equip a large scale database and manage addresses strictly. The stateless auto-configuration method is that an IPv6 device creates address using interface ID information, prefix information acquiring from Router or well-known prefix information. In the stateless auto-configuration method, an IPv6 device takes the responsibility for generation and allocation of own address.
The initialization process of an IPv6 device using address auto-configuration method is as following.

First, an IPv6 device creates temporary link-local address with link-local prefix FE80::/64 and 64 bits interface ID. For example, an IPv6 device which has Ethernet MAC address 00-AA-00-3F-2A-1C creates temporary link-local address as following. It inserts FF-FF between the third byte and the fourth byte. And then it complements U/L (Universal/Local) bit. Thus, the last result is 02-AA-00-FF-FF-2A-1C and it can be expressed 2A::FF:FF:2A1C by hexadecimal. Therefore, link-local address that corresponds to network adaptor that has MAC address 00-AA-00-2A-1C becomes FE80::2A:FF:2A1C.

Second, an IPv6 device performs Duplicate Address Detection (DAD) to check if other IPv6 devices use the same link-local address or not. An IPv6 device sends a NS (Neighbor solicitation) message including link-local address to all devices to perform Duplicate Address Detection. If any IPv6 device that uses identical link-local address sends a NA (Neighbor Advertisement) message and then auto-configuration is failed. After failure, an administrator set address manually.

Third, if an IPv6 device doesn’t receive a NA message in response to NS message, an IPv6 device sends a RS (Router Solicitation) message to acquire network prefix information for initialization of global site-local address. An IPv6 device uses stateful auto-configuration method if there is no response for a RS message.

Fourth, an IPv6 device accepts a RA (Router Advertisement) message from router and set own address. If there is no prefix information within RA message, an IPv6 device can set own address using stateful auto-configuration.

Next picture illustrates that exchanges message between IPv6 device and Router to set address automatically.

1. Host A creates temporary link-local address.
2. Host A sends NS message to all hosts for on link to perform Duplicate Address Detection.
3. If host A receives NA message in response to NS message, auto-configuration is failed and administrator set address manually.
4. Host A sends RS message to obtain network prefix information from router.
5. If host A doesn’t receive RA message from router, host A can set own address using stateful auto-configuration method.

### 4. THE SECURITY VULNERABILITIES OF AUTOCONFIGURATION

The Auto-configuration is one of IPv6’s advantages and offers user convenience. However, the important configuration information of an IPv6 device is revealed to attacker, if the message that is used in auto-configuration process isn’t...
The Next Table explains threats of IPv6 auto-configuration. Detailed content of threat is following.

<table>
<thead>
<tr>
<th>Threats</th>
<th>Redirect / DoS</th>
<th>Redirect / NA</th>
<th>Msg.</th>
</tr>
</thead>
<tbody>
<tr>
<td>DAD DoS</td>
<td>ND</td>
<td>DoS</td>
<td>NA</td>
</tr>
<tr>
<td>Bogus on-link prefix</td>
<td>RD</td>
<td>DoS</td>
<td>RA</td>
</tr>
<tr>
<td>Bogus address configuration</td>
<td>RD</td>
<td>DoS</td>
<td>RA</td>
</tr>
<tr>
<td>Parameter Spoofing</td>
<td>RD</td>
<td>DoS</td>
<td>RA</td>
</tr>
</tbody>
</table>

4.1 DAD DoS attack

In networks where the entering hosts obtain their addresses using stateless address autoconfiguration, an attacking node could launch a DoS attack by responding to every duplicate address detection attempt made by an entering host. If the attacker claims the address, then the host will never be able to obtain an address. The attacker can claim the address in two ways: it can either reply with an NS, simulating that it is performing DAD, too, or it can reply with an NA, simulating that it has already taken the address into use. The issue may also be present when other types of address configuration are used, whenever DAD is invoked prior to actually configuring the suggested address. This is a DoS attack.

4.2 Bogus on-link prefix attack

An attacking node can send a Router Advertisement message specifying an invalid subnet prefix to be used by a host for address autoconfiguration. A host executing the address autoconfiguration algorithm uses the advertised prefix to construct an address, even though that address is not valid for the subnet. As a result, return packets never reach the host because the host’s source address is invalid. This is a DoS attack.

The attacker can use an arbitrary lifetime on the bogus prefix advertisement. If the lifetime is infinity, the sending host will be denied service until it loses the state in its prefix list e.g., by rebooting, or after the same prefix is advertised with a zero lifetime. The attack could also be perpetrated selectively for packets destined to a particular prefix by using 128 bit prefixes.

Additionally, the attack may cause a denial-of-service by flooding the routing table of the node. The node would not be able to differentiate between legitimate on-link prefixed and bogus ones when making decisions as to which ones are kept and which are dropped. Inherently, any finite system must have some point at which new received prefixes must be dropped rather than accepted.

This attack can be extended into a redirect attack if the attacker replies to the Neighbor Solicitations with spoofed Neighbor Advertisements, thereby luring the nodes on the link to send the traffic to it or to some other node.

4.3 The Bogus Address Configuration Prefix

An attacking node can send a Router Advertisement message specifying an invalid subnet prefix to be used by a host for address autoconfiguration. A host executing the address autoconfiguration algorithm uses the advertised prefix to construct an address, even though that address is not valid for the subnet. As a result, return packets never reach the host because the host’s source address is invalid. This is a DoS attack.

This attack has the potential to propagate beyond the immediate attacked host if the attacked host performs a dynamic update to the DNS based on the bogus constructed address. DNS update causes the bogus address to be added to the host’s address record in the DNS.

4.4 The parameter spoofing Attack

IPv6 Router Advertisements contain a few parameters used by hosts when they send packets and to tell hosts whether or not they should perform stateful address configuration. An attacking node could send out a valid-appearing Router Advertisement that duplicates the Router Advertisement from the legitimate default router, except the included parameters are designed to disrupt legitimate traffic. This is a DoS attack.

5. CONCLUSION

This paper has describes neighbor discovery protocol and autoconfiguration in IPv6 and examines security vulnerability of autoconfiguration. Recently, the security vulnerability of IPv6 autoconfiguration has been indicated to serious problem. The most vulnerabilities of autoconfiguration occur from the vulnerabilities of neighbor discovery message such as Router Solicitation, Router Advertisement, Neighbor Solicitation, Neighbor Advertisement messages. Therefore, method that can protect neighbor discovery messages so that an attacker cannot forge neighbor discovery messages should be considered. Also mechanism that can communicate between IPv6 nodes so that an attacker cannot feign by a router or a host should be considered.
Today many countries have been preparing to construct IPv6 environment because of IP address exhaustion. However, we think the security problem of autoconfiguration should be solved for the first of all before IPv6 is introduced. The security vulnerability that refers in this paper will be foundation of the development of secure autoconfiguration method in the future.

REFERENCES