Privacy Extensions for Stateless Address Autoconfiguration in IPv6 "Requirements for unobservability"

Alberto Escudero Pascual <aep@kth.se>
Royal Institute of Technology (KTH)
Kista. Sweden

26th March 2002

Abstract

Stateless address autoconfiguration defines the mechanism for a IPv6 node to generate an address without the need of an external DHCP server based on the interface identifier. In the case of Ethernet the Interface Identifier is based on the EUI-64 identifier derived from the interface's built-in 48-bit IEEE 802 address (MAC address). The IPv6 address generated via Stateless Autoconfiguration contains the same interface identifier regardless of the location the mobile node is attached to the Internet. RFC3041 presents a privacy extension to Stateless Autoconfiguration based on the idea of generating random interface identifiers periodically.

The paper introduces the concept of "unobservability" of the privacy extension and studies in which scenarios a third party will be able to determine with high probability if a node is running RFC3041 or not. The paper shows the privacy implications of the universal/local bit of the current IPv6 addressing architecture and presents a set of suggested changes to enhance privacy.

1 Background

This paper is divided as follows: Section 1 contains a very brief overview of the Internet Protocol Version 6, Section 2 describes the different mechanisms to generate a global scope address including the privacy extension for stateless address configuration RFC3041 [6]. Section 3 defines unobservability of the privacy extension. Section 4 introduces the level of privacy extension observability for different scenarios and finally in Section 5 we present a set of suggested changes to the current IP Version 6 Addressing Architecture", RFC 2373 [3] to enhance privacy.

1.1 The Internet Protocol version 6

The Internet Protocol Version 6 (IP*v*6), also called "IPng" (IP Next Generation), is the latest version of the Internet Protocol (IP). Formally, IPv6 is a set of specifications from the Internet Engineering Task Force (IETF). IPv6 was designed as an evolutionary set of improvements to the current IP Version 4. The most obvious improvement in IPv6 over the IPv4 are that IP addresses are lengthened from 32 bits to 128 bits which anticipates the future growth of the Internet and provides relief for what was perceived as an impending shortage of network addresses. Besides, IPv6 offers technical advantages over IPv4, including self-configuration mechanisms, enhanced security, quality of service features and native mobility support [1].

IPv6 includes a security protocol in the network layer that provides cryptographic security services that supports combinations of authentication, integrity, access control, and confidentiality. The IP

Encapsulating Security Payload (ESP) and the IP Authentication Header (AH) are part of the IP Security architecture (IPSEC) described in RFC 2401 [2].

Both ESP and AH are mandatory parts of IPv6 and make sure that a third party eavesdropping on the channel can not read and/or modify the IP datagram. The IP Authentication Header seeks to provide security by adding authentication information to each IP datagram whilst confidentiality requires the use of ESP. Neither AH nor ESP hide the source and destination IP addresses of the communicating parties and hence their network location.

The protocol operation defined for mobility in IPv6 is known as MobileIPv6 and allows a mobile node to move from one link to another without changing the mobile node's IP address. A mobile node is always addressable by its "home address", an IP address assigned to the mobile node within its home subnet, i.e., with the prefix of its home link. Packets may be routed to the mobile node using this address regardless of the mobile node's current point of attachment to the Internet, and the mobile node may continue to communicate with other nodes while using this address, even after moving to a new link. With specific support for mobility in IPv6, packets destined to a mobile node would be able to reach it even while the mobile node is away from its home network.

In summary, IPv6 provides new security opportunities which include message integrity, authentication, and confidentiality (IPSEC) and the possibility for a mobile node to be always addressable by its "home address" (MobileIP). All these functionalities rely on treating the fixed IP address of the node as an indentifier. In the case of IPSEC end-to-end security uses the fixed IP address as part of the security association and mobility requires to the mobile node to send the fixed home address included in a destination option.

In the next section, as part of the description of the different mechanisms to obtain a global address, we present the possible threats for privacy when an IP identifier can be linked with personal identifiable information as a "personal device" and how the existing privacy extension has not taken into consideration that the user might be also interested in hiding the fact that is using the privacy extension itself.

2 Mechanisms to obtain a global address

We have clasiffied the mechanisms to obtain a global address as follows: stateless and stateful address configuration, manual, cryptographic generated and random addresses which include the privacy extension and IPv6 over PPP with no global identifier available.

2.1 Stateless Address Autoconfiguration in IPv6

Stateless address autoconfiguration defines the mechanism for a IP_{v6} node to generate an address without the need for an external DHCP server based on the interface identifier [8,4]. The stateless approach is used when a site is not particularly concerned with the exact addresses hosts use.

To insure that all configured addresses are likely to be unique on given link, nodes do "duplicate address detection" on addresses before assigning them to an interface. The Duplicate Address Detection (DAD) algorithm is used to check all addresses, *independent* of whether they are obtained via stateless or stateful autoconfiguration.

2.1.1 Interface Identifier

In the case of stateless address autoconfiguration for Ethernet the Interface Identifier is based on the EUI-64 identifier derived from the interface's built- in 48-bit IEEE 802 address (MAC address).

The EUI-64 is formed as follows:

1. The first three octets that corresponds to the Organizationally Unique Identifier (OUI) of the Ethernet address become the *company_ id* of the EUI-64. The OUI blocks are assigned by IEEE.

2. The fourth and fifth octets of the EUI-64 are set to the fixed value FFFE hexadecimal (encapsulation of IEEE 802 address in EUI-64).

3. The last three octets of the Ethernet address (extension identifier values) become the last three octets of the EUI-64.

The Interface Identifier is then formed from the EUI-64 by complementing the "Universal/Local" (U/L) bit, which is the next-to-lowest order bit of the first octet of the EUI-64. Complementing this bit will generally change a 0 value to a 1, since an interface's built-in address is expected to be from a universally administered address space and hence have a **globally unique value**.

A universally administered IEEE 802 address or an EUI-64 is signified by a 0 in the U/L bit position, while a globally unique IPv6 Interface Identifier is signified by a 1 in the corresponding position. In brief, a globally unique IPv6 interface based on a hardware token that is unique will carry one bit indicating its uniqueness.

[3] states that motivation for inverting the "u" bit when forming the interface identifier is to make it easy for system administrators to hand configure local scope identifiers when hardware tokens are not available and to allow development of future technology that can take advantage of interface identifiers with global scope.

2.1.2 Link, site and global-scope addresses

The link-local address of an IP_{v6} node is the result of combining the global unique interface identifier with the reserved link-local prefix FE80. The site-local and global-scope addresses are created by combining prefixes advertised in Router Advertisements and Neighbor Discovery.

The IP_{v6} address generated via Stateless Autoconfiguration contains the same interface identifier *regardless* of the location the mobile node is attached to the Internet.

Even when higher communication layers encrypt their payloads (for example with ESP), there is not an easy mechanism to hide the addresses in packet headers as they appear in clear, this fact makes it very easy for an eavesdropper to track mobile nodes by analyzing the prefixes related to a certain interface identifier.

For example, let's consider a device with built-in 48 bit EUI-48 address 00:01:02:65:71:37 that moves from a network A with prefix 3ffe:200:15:1 to a network B with prefix 3ffe:200:17:2.

1. A unique EUI-64 value is generated by concatenating the company_id, an $FFFE_{16}$ valued label, and the extension identifier values, obtaining 00:01:02:ff:fe:65:71:37.

2. The global unique interface identifier is then formed by complementing the "Universal/Local" bit, resulting 02:01:02:ff:fe:65:71:37.

3. The link local address is fe80::201:2ff:fe65:7137 in both networks

4. When moving from network A to B the mobile device will change from 3ffe:200:15:1:201:2ff:fe65:7137 global IP_{v6} address to 3ffe:200:17:2:201:2ff:fe65:7137.

2.2 Privacy Extension for Stateless Address Configuration

Narten and Draves [6] developed a privacy extension for Stateless Address Configuration based on the idea of generating random interface identifiers periodically. They describe two approaches for the maintenance of the randomized interface identifier depending upon weather stable storage is present (history scheme) or not. The use of the history scheme tries to avoid the scenario where two nodes generates the same randomized interface identifier, both detect it via DAD, but then proceed to generate identical randomized interface identifier via the same flawed random number generation algorithm.

The first big difference between the EUI-64 based interface identifiers and RFC3041 is that the latest can not claim to be globaly unique and hence the universal bit must be set to zero.

2.3 Stateful address configuration

The dynamic host configuration protocol (DHCP) is the stateful counterpart to stateless autoconfiguration in which hosts obtain interface addresses and/or configuration information and parameters from a server. Servers maintain a database that keeps track of which addresses have been assigned to which hosts. Stateless and stateful autoconfiguration complement each other. For example, a host can use stateless autoconfiguration to configure its own addresses, but use stateful autoconfiguration to obtain other information.

2.4 Manual configuration

If an IEEE global identifier is not available a different source of uniqueness should be used. Suggested sources of uniqueness include link-layer addresses, machine serial numbers, etc. In this case the "u" bit of the interface identifier must be set to zero.

If a good source of uniqueness cannot be found, it is recommended that a random number be generated. In this case the "u" bit of the interface identifier must also be set to zero.

2.5 Cryptographically Generated Addresses

The Cryptographically Generated Address where introduced to solve the problem of address ownership [14] in mobileip. In all the different proposals the CGA addresses have a strong cryptographic binding with a public key. CGA are obtained by means of a one-way hash functions.

For example in the case of SUCV IDs [7] the CGA addresses are created as follows:

$$CGA = 64bit - prefix + CGIID$$
$$CGIID = f(PublicKey, j)$$

where $f()$ is the least significant 64 bits of SHA-1 hash of Public Key concatenated with 16 bit counter j. The universal bit u is set to zero.

2.6 Classification of Interface Identifiers

The IPv6 interface identifiers can be clasified as follows:

1. Half of this space, with the universal bit set to 1, is given to IEEE EUI-64 identifiers.
2. The other half, with the universal bit set 0 is used for Interface Identifiers that are not globally unique including:

- manually assigned.
- local unique assigned by DHCPv6.
- random interface identifiers used in RFC 3041 [6] and RFC 2472 [5] section 4.1.
- cryptographically generated addresses.

3 Unobservability of the privacy extension

In [15] unobservability is defined as the property that ensures that a user may use a resource or service without others, especially third parties, being able to observe that the resource or service is being used.

Unobservability requires that a third party cannot determine whether an operation is being performed based on certain knowledge of the subject(s) of observation.

In our analysis we define as the item of interest for the attacker to be able to determine if the victim is using RFC3041. In order to try to describe different scenarios it is important to identify possible sources of knowledge for the attacker to make a decision. The basic source of information is the link local or global scope address of the victim but other sources could be available as:

- The victim's mac address.
- The presence of a DHCPv6 serving the prefix of the victim's network.
- If the victim has mobility support and if its address is a CGA.
- The victim's hardware type and/or operative system.

4 Scenarios

According to the amount of knowledge available to the attacker we can divide all scenarios in two.

4.1 Attacker is not present in the link

In this scenario the attacker is not present in the link and is in the path between the victim and a correspondent node. In our model we assume that the attacker knows about which OUIs has been assigned by IEEE but not the distribution of the "extension identifier values" for certain OUI.

In first place the attacker determines if the interface identifier is based on a EUI-64 identifier by checking the universal/local bit. If the universal/local bit is set to one, the attacker checks if the OUI has been assigned by IEEE. If the OUI has not been assigned by IEEE the attacker can presume that the victim has either modified its MAC address, configured manualy the interface identifier or generated a random interface identifier without setting the u-bit to zero.

If the universal/bit is set to zero, the attacker can choose among different possibilities : the interface has been configured by stateful address configuration, manualy or is random interface identifier (CGA, RFC3041, RFC2472).

The attacker can gather extra knowledge as follows:

- By observing the nature of the traffic between the victim and a correspondent node. Cryptographically Generated Addresses are included in authentified binding updates and are part of destination/routing header options.

- By discovering the presence of a DHCP server via the (FF05::1:3) site-scoped multicast address.

4.2 Attacker is present in the link

In the second main scenario the attacker is present in the link, most of the information required to observe if the victim is using the privacy extension can be gathered by victim's traffic analysis. The attacker will be able to observe not only the presence of a DHCP server but also the traffic exchange between the DHCP server and the victim. If the victim has a CGA, the attacker will be also able to observe the flow of authentified mobility bindings.

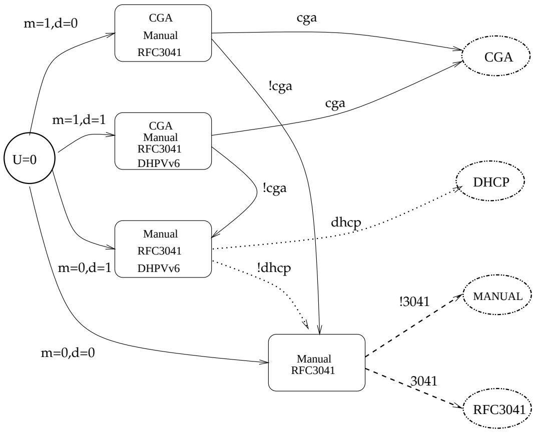

Figure 1: Possible scenarios

In the case that the victim is not using stateful address configuration or is a mobile node with a CGA, the attacker has to decide between two possible options [Fig. 1]: the victim is running RFC3041 privacy extension or has configured manualy its address. The attacker then, can try to match during a certain period of time the hardware addresses with the link or global scope addresses. Nodes running RFC3041 will change their addresses periodicaly while keeping the same hardware address.

4.3 Conclusions

[Fig. 1] shows all possible scenarios considering the amount of knowledge available to the attacker. In all the cases the attacker starts checking if the universal/local bit of the interface identifier is set to zero. If the node is not running MobileIP with CGA and there is not a DHCP server available in the victim's subnet, the attacker assumes that the victim is running RFC3041 or has configured the address manualy. Finally, the attacker can observe the addresses associated with a certain hardware address and determine if the victim is running RFC3041.

5 Recommendations

A better privacy protection can be achieved if the random interface identifier can not be distinguished from a *common* one. i.e. an eavesdropper can not determine if certain node is using or not the stateless address configuration privacy extension.

Unobservability can be garanteed as follows:

- All the hosts generate their interface identifier randomly by default. (suggested change in RFC2373).

- The universal/local bit is not reserved and hosts always rely in duplicate address detection (DaD).

- Alternatively, the host generates an interface identifier based on the addresses present in the link. The main idea is that the mobile node should keep statistical records of the presence of the different OUIs in the media and generate a random identifier based on that information. The host learns about the nodes in the media by sending a neigbor discovery message to the all hosts multicast address.

References

[1] **C. Huitema,** *IPv6, the new Internet Protocol.* 2nd Edition. Prentice Hall. 1997

[2] **S. Kent and R. Atkinson**, *"Security Architecture for the Internet Protocol"*. RFC 2041.

[3] **R. Hinden and S. Deering**, *"IPv6 Addressing Architecture"*, RFC 2373, July 1998.

[4] **R. Hinden, M. O'Dell, S. Deering**, *"An IPv6 Aggregatable Global Unicast Address Format"*, RFC 2374, July 1998.

[5] **D. Haskin and H. Allen** *"IP Version 6 over PPP",* RFC 2472, December 1998

[6] **T. Narten and R. Draves**, *"Privacy Extensions for Stateless Address Autoconfiguration in IPv6"*. RFC3041, January 2001.

[7] **G. Montenegro and C. Castelluccia,** *"SUCV Identifiers and Addresses".* draft-montenegro-sucv-01.txt. July 2001.

[8] **S. Thomson and T. Narten,** *"IPv6 Address Autoconfiguration"*, RFC 2462, December 1998.

[9] **A. Escudero.** *"Location privacy in IP_{v6} internetworking - Pseudorandom interface identifiers".* IDMS2001. Lancaster. UK. August 2001.

[10] **D. Johnson and C. Perkins,** *"Mobility Support in IPv6"*, draft-ietf-mobileip-ipv6 v14, July 2000.

[11] **H. Soliman, C. Castelluccia, K. El-Malki and L. Bellier,** *"Hierarchical MIPv6 mobility management"*, draft-ietf-mobileip-hmipv6 v3. February 2001.

[12] **C. Perkins,** *"IP Mobility Support"*, RFC 2002, October 1996.

[13] **A. Escudero**, *"Anonymous and Untraceable Communications: Location Privacy in Mobile Internetworking".* Licentiate Thesis. July 2001.

[14] **Pekka Nikander**, *"An Address Ownership Problem in IPv6"*, draft-nikander-ipng-address-ownership-00.txt, February 2001.

[15] **ISO99** IS 15408, 1999, `http://www.csrc.nist.gov/cc`