Router Advertisement based privacy extension in IPv6 autoconfiguration

<draft-rafiee-6man-ra-privacy-01.txt>

Abstract

Privacy is an important issue for many governments [eurolaw] and users where its importance becomes more evident every day. Nodes might change their IP addresses frequently in order to avoid being tracked by attackers and which also results in the prevention of information being leaked from their nodes. In IPv6 networks there is currently one solution for maintaining privacy for nodes when IPv6 StateLess Address AutoConfiguration (SLAAC) (RFC 4662) is used. Unfortunately this solution, i.e., Privacy Extension (RFC 4941), has some problems, such as not generating a new Interface ID (IID) after changing the router prefix. The RFC also gives no explanation as to how to use CGA in its randomizing solution. The purpose of this document is to address these issues and to update the current RFC.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on Expires: November 2, 2013.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the
document authors. All rights reserved. This document is subject to
BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF
Documents (http://trustee.ietf.org/license-info) in effect on the
date of publication of this document. Please review these documents
carefully, as they describe your rights and restrictions with respect
to this document. Code Components extracted from this document must
include Simplified BSD License text as described in Section 4.e of
the Trust Legal Provisions and are provided without warranty as
described in the Simplified BSD License.

Table of Contents

1. Introduction .................................................. 3
2. Conventions used in this document .............................. 3
3. Algorithms Overview ............................................... 3
   3.1. DAD Process ................................................. 4
4. Lifetime of Interface ID (IID) ................................. 4
   4.1. Automate the process for setting the lifetime ........... 5
5. Security Considerations ........................................... 5
6. IANA Considerations ............................................... 5
7. Conclusions ....................................................... 5
8. References ......................................................... 6
   8.1. Normative .................................................... 6
   8.2. Informational ................................................ 6
Authors’ Addresses .................................................. 7
1. Introduction

This document defines the meaning of privacy as it relates to methods for maintaining our confidential data so that it does not become available to or is exposed to unscrupulous people who would use it to harm us or use it for their ill gains. There is currently only one solution available in IPv6 autoconfiguration (RFC-4662), i.e., Privacy Extension [RFC4941]. In the Privacy Extension document, two different approaches are used for IID generation. In the first approach, the use of stable storage enables it to find which IIDs are used and which are reserved. In the second approach, where stable storage is not available, it offers the use of either Cryptographically Generated Addresses (CGA) [RFC3972] or Dynamic Host Configuration Protocol (DHCPv6). The Privacy Extension document also referred to the use of named approaches as a mechanism for greater randomization. Here we offer an update to section 3.2.2 of RFC 4941 in order to explain how to use CGA when security is not the issue. Another update to this RFC will be how to maintain the lifetime of the IP address when the router prefix changes. This is because, in this RFC, the key role is the lifetime of the IID, and it might not expire when the router prefix is changed. This means that the node might not change its IID when it moves to another network unless it is rebooted. This might give an attacker the ability to track this node, and obtain enough confidential information about this node, to allow for further attacks.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [RFC2119].

In this document, these words will appear with that interpretation only when in ALL CAPS. Lower case uses of these words are not to be interpreted as carrying RFC 2119 significance.

In this document the use of || indicates the concatenation of the values on either side of the sign.

3. Algorithms Overview

This section explains how to use the modified version of the CGA algorithm for the randomization of the IID. This approach is RECOMMENDED and preferable than the first approach where need stable storage.

1. Generate a 16 byte random number called modifier. To generate this
modifier implementations SHOULD use a random seed to aid in the randomization of this number.

2. Obtain Router prefix from the router advertisement

3. Obtain the nodes' current time and convert it to timestamp. The timestamp is a 64-bit unsigned integer field containing a timestamp. The value indicates the number of seconds since January 1, 1970, 00:00 UTC, by using a fixed point format.

4. Concatenate the modifier to the timestamp and router prefix.

\[ R1 = (\text{modifier(16 bytes)} || \text{timestamp(8 bytes)} || \text{router prefix}) \]

5. Execute SHA2 (256) on the result from step 4.

\[ \text{digest}=\text{SHA256}(R1) \]

The use of SHA2 (256) is RECOMMENDED because the chances of finding a collision are less than when using SHA1 and the generation time is acceptable (in microseconds using a standard CPU). If, in the future, a faster and collision free algorithm becomes available, then it SHOULD be used. It is RECOMMENDED that the implementation be able to support any new algorithms.

6. Take the 64 leftmost bits from the resulting output from step 5 (SHA2 digest) and set bits u and g (bits 7 and 8) to zero and call this the IID.

7. Concatenate the IID to the local subnet prefix in order to set the local IP address. If the lifetime of the old local address has not expired, then the node MIGHT skip this step. Otherwise it will receive a new router prefix.

8. Concatenate the IID to the router subnet prefix (Global subnet prefix), obtained from the RA message, and set it as a tentative global IP address. This IP address will become permanent after Duplicate Address Detection (DAD) processing. This is another update to RFC 4941. The status of IP addresses in RFC 4941 are temporary while it SHOULD be permanent with a life time explained in section 4.

3.1. DAD Process

After the DAD process, if the node finds collisions in the network then the modifier will be incremented and the DAD process will be repeated. If after 3 times, it receives the same result, it will consider this an attack and will start using that IP address.

4. Lifetime of Interface ID (IID)
One of the problems with the Privacy Extension document as explained earlier is that the IID might not change when the node joins new network or receives a new router prefix. Here we update this document. The router prefix has a higher priority than the IID’s current lifetime. This means that if the node receives new router prefix while its current IID is still valid, it MUST generate new randomized IID and start using it. It should not start any new sessions with the old IID, but it MIGHT keep the current sessions as what is explained in the Privacy Extension document. The IIDs MUST only be valid for a short period of time which will depend on the network policy in vogue. Any implementations SHOULD provide a means of allowing for users to change the lifetime default value.

4.1. Automate the process for setting the lifetime

The implementations MIGHT consider an option where the RA messages update the lifetime of all addresses generated when using this approach when processing RA messages. This will eliminate the need for the manual step during installation which sets the default value of lifetime for any future IIDs generated using this approach based on network policy. The format for this lifetime value will be the same as that explained in section 5.3.1 RFC 3971. In this lifetime option the type for SHOULD be set to next sequential number available in the SeND options, i.e., 15. This field SHOULD be added to the ICMPv6 option of RA messages.

5. Security Considerations

As is explained in the Privacy Extension document. the same approaches are used to maintain security, such as using Secure Neighbor Discovery (SeND) (RFC-3971) or using a monitoring system which would inform the administrator of the status of the network and of any suspended activities in the network.

6. IANA Considerations

-

7. Conclusions

Privacy has become a very important issue in recent years. There is one solution to the privacy issues, but the current solution has some deficiencies. The purpose of the current document is to address and solve the problem which exists with the Privacy Extension document [RFC4941].
8. References

8.1. Normative References


8.2. Informational References

Authors’ Addresses

Hosnieh Rafiee
Hasso-Plattner-Institute
Prof.-Dr.-Helmert-Str. 2-3
Potsdam, Germany
Phone: +49 (0)331-5509-546
Email: ietf@rozanak.com

Dr. Christoph Meinel
(Professor)
Hasso-Plattner-Institute
Prof.-Dr.-Helmert-Str. 2-3
Potsdam, Germany
Email: meinel@hpi.uni-potsdam.de