Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: January 2, 2016

C. Huitema
Microsoft

July 1, 2015

Implications of Randomized Link Layers Addresses for IPv6 Address Assignment
draft-huitema-6man-random-addresses-00.txt

Abstract

Hosts may assign random link-layer addresses to network interfaces in an attempt to increase privacy and reduce trackability. Careless assignment of IPv6 addresses may negate the privacy advantages of random link-layer addresses. We propose simple solutions to ensure that IPv6 addresses do change whenever the link layer addresses change.

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 January 2, 2016.

Table of Contents

1. Introduction 2
1.1. Requirements 3
2. Randomized link-layer addresses 3
2.1. Randomized link-layer address format 3
2.2. Link-layer address life time 4
3. Considerations on IPv6 address assignment 4
3.1. IEEE-identifier-based IIDs 4
3.2. Static, manually configured IIDs 5
3.3. Constant, semantically opaque IIDs 5
3.4. Stable, semantically opaque IIDs 5
3.5. Temporary IIDs 6
3.6. DHCPv6 generation of IIDs 6
3.7. Transition/co-existence technologies 7
4. Security Considerations 7
5. IANA Considerations 7
6. Acknowledgments 7
7. References 7
7.1. Normative References 7
7.2. Informative References 8
Author's Address 8

1. Introduction

Reports surfaced recently of systems that would monitor the wireless connections of passengers at Canadian airports [CNBC]. We can assume that these are either fragments or trial runs of a wider system that would attempt to monitor Internet users as they roam through wireless access points and other temporary network attachments. We can also assume that privacy conscious users will attempt to evade this monitoring, for example by ensuring that low level identifiers like link-layer addresses are "randomized," so that the devices do not broadcast a unique identifier in every location that they visit.

Of course, link layer "MAC" addresses are not the only way to identify a device. After connecting to a link, the host will try to obtain IPv6 addresses for that link. There are multiple ways to assign these addresses. The privacy implications of various assignment methods are studied in [I-D.ietf-6man-ipv6-address-generation-privacy], but this study does not fully take into account the effect of link-layer address randomization.

The purpose of this document is to provide guidance to implementers, so they chose address assignment methods that are compatible with link layer address randomization. This document is complementary to [I-D.ietf-dhc-anonymity-profile], which specifies how to use DHCPv6 in conjunction with randomized link-layer addresses.

1.1. Requirements

The keywords MUST, MUST NOT, REQUIRED, SHALL, SHALL NOT, SHOULD, SHOULD NOT, RECOMMENDED, MAY, and OPTIONAL, when they appear in this document, are to be interpreted as described in [RFC2119].

2. Randomized link-layer addresses

Mobile nodes can be tracked using multiple identifiers, the most prominent being the MAC addresses. For example, when devices use Wi-Fi connectivity, they place the MAC address in the header of all the packets that they transmit. Standard implementation of Wi-Fi use unique 48 bit MAC addresses, assigned to the devices according to procedures defined by IEEE 802. Even when the Wi-Fi packets are encrypted, the portion of the header containing the addresses will be sent in clear text. Tracking devices can "listen to the airwaves" to find out what devices are transmitting near them.

The obvious solution is to "randomize" the MAC address. Before connecting to a particular network, the device replaces the MAC address with a randomly drawn 48 bit value. MAC address randomization was successfully tried at the IETF in Honolulu in November 2014 [IETFMACRandom]. However, we have to consider the linkage between MAC addresses and IPv6 addresses.

From a privacy point of view, it is clear that MAC Addresses and IPv6 addresses and DHCP identifiers shall evolve in synchrony. For example, if the MAC address changes and the IID portion of the IPv6 address stays constant, then it is really easy to correlate old and new MAC address. Conversely, if the IID changes but the MAC address remains constant, the old and new identifiers and addresses can be correlated by listening to the link's traffic.

2.1. Randomized link-layer address format

At the time of this writing, there is no standard way to construct randomized link layer addresses, but many implementations use the following algorithm for IEEE 802 48 bit MACs:

Set the the "u" (universal/local) bit to 1 (local).

Set the the "g" (individual/group) bit to 0 (individual).

Pick random values for all the other bits.

2.2. Link-layer address life time

This document makes the hypothesis that randomized link layer addresses are chosen just prior to the connection to a link. Hosts are expected to maintain the same link-layer address for the duration of the connection.

There are circumstances where a host may decide to reset its link layer address while maintaining an attachment to a link. For example, a host Ethernet interface may remain "plugged in" while the interface driver is reset to use a new MAC address. These conditions will be considered equivalent to disconnecting and then reconnecting with a new link layer address. The previously used IPv6 addresses will be discarded, and a new set of addreses will be assigned.

There are circonstances where a host may decide to reconnect to a particular link using the same link-layer address as for a previous attachment. In this case, the assignment algorithm will normally result in assigning the same IPv6 address as in the previous session, except under exceptional circumstances such as resetting the "secret key" used in [RFC7217].

3. Considerations on IPv6 address assignment

Several IPv6 address assignment methods have been defined over time. We review here these methods in light of link layer address randomization, using the same nomenclature as [I-D.ietf-6man-ipv6-address-generation-privacy].

3.1. IEEE-identifier-based IIDs

IEEE-identifier-based IIDs could be derived from randomized link layer ID, using the algorithm specified in Appendix A of [RFC4291].

If the IIDs are constructed using the random link layer addresses, and if the random link layer addresses are constructed using the algorithm specified in Section 2.1, then the issues described in section 3 of [I-D.ietf-6man-ipv6-address-generation-privacy] are somewhat mitigated, but many concerns remain. The correlation over time still be possible for the lifetime of the link layer address, and the location tracking will only be mitigated if link layer addresses do change with location.

In addition to the lifetime and location tracking concerns, there is also a "scope" issue with IEEE-identifier-based IIDs. The practice will export the link-layer address value to all places where the IPv6

address is used. This increase the potential "surface" for privacy attacks, and is not desirable.

There is a small probability of collision between IIDs derived from random link layer addresses and IIDs obtained through the sematically opaque, cryptographically generated, or temporary assignment methods. The "u" bit is set to global for globally assigned link layer addresses, but set to "local" for both random link layer addresses and for IIDs derived through some random process. The collision risk is however very small, and may not be a practical concern.

3.2. Static, manually configured IIDs

Because static, manually configured IIDs are stable, both correlation and location tracking are possible for the life of the address. Using randomized link-local addresses doesn't change that.

In practice, static assignment and link-layer address randomization address different scenarios. Static assignments are typically used for static hosts, while randomization is typically used for mobile hosts.

3.3. Constant, semantically opaque IIDs

This address assignment method allows correlation and location tracking because the IID is constant across IPv6 links and time. Using randomized link-local addresses doesn't change that. In fact, the constant values allow for correlation between the random link-local address and the host's identity, removing most of privacy value of random link-layer addresses.

Section 4.3 of [I-D.ietf-6man-ipv6-address-generation-privacy] addresses the general case of systems generating constant IID using the algorithms specified in [RFC4941], mentioning the implementation of this algorithm in Windows. Tests on the Windows platform show that the "constant" IIDs do in fact change if the link layer address is changed to a random value, and thus do in fact preserve the privacy value of random link-layer addresses.

3.4. Stable, semantically opaque IIDs

[RFC7217] specifies an algorithm that generates, for each network interface, a unique random IID per IPv6 link. The privacy properties of that algorithm depends on the specific source of the "Net_Iface" chosen by the implementer.

Most sources for the Net_IFace parameter listed in Appendix A of [RFC7217] will result in stable identifiers, independent of the link-

layer address. This will enable tracking over time of a host that repeatedly visits the same location, despite any attempts by the host to use different random link-layer address values. In fact, the stable IIDs will enable correlation of different link-layer addresses to the same host identity.

Tracking over time is prevented if the Net_IFace parameter is set to the current link layer address. In that case, the stable addresses will have exactly the same lifetime as the link-layer identifiers. This SHOULD be the default solution for mobile hosts.

Some hosts are static by nature. This is for example the case of servers. For such hosts, address stability is probably more important than preventing tracking over time. Such hosts should probably not attempt to configure random link layer addresses. They MAY want use a more stable sources for the Net_IFace than the link address programmed in the network interface card, as explained in [RFC7217].

3.5. Temporary IIDs

As stated in [I-D.ietf-6man-ipv6-address-generation-privacy], "a host that uses only a temporary address mitigates all four threats. Its activities may only be correlated for the lifetime a single temporary address." There is however a condition. If the lifetime of the temporary address exceeds the lifetime of the random link layer address, then correlation of successive link-layer addresses become possible, effectively enabling a form of tracking.

If a host uses both temporary and stable addresses, the privacy properties are those of the particular stable addresses. This is also true is a host uses temporary addresses and configure but doen't use a stable address. The address configuration will require performing duplicate address detection, generating at least a few packets on the local links. Observing this packets, an on-link attacker can correlate the link-layer address with the stable address. If the stable address includes a constant identifier, then the benefits of using rnadom link-local addresses will be negated.

3.6. DHCPv6 generation of IIDs

When using DHCPv6 in conjunction with random link layer addresses, implementers SHOULD follow the recommendations of [I-D.ietf-dhc-anonymity-profile].

3.7. Transition/co-existence technologies

Transition technologies typically embed an IPv4 address in a specifically formatted IPv6 address. Tracking over time becomes possible if the IPv4 address has a longer lifetime than the random link-layer address.

To mitigate the potential tracking issues with embedded IPv4 addresses, hosts using random link-local addresses SHOULD implement the DHCPv4 profile specified in [I-D.ietf-dhc-anonymity-profile].

4. Security Considerations

This whole document concerns the privacy and security properties of different IPv6 address generation mechanisms.

5. IANA Considerations

This draft does not require any IANA action.

6. Acknowledgments

The inspiration for this draft came from the authors of [I-D.ietf-6man-ipv6-address-generation-privacy], Alissa Cooper, Fernando Gont, and Dave Thaler.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, September 2007.

[RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, April 2014.

7.2. Informative References

[CNBC] Weston, G., Greenwald, G., and R. Gallagher, "CBC News: CSEC used airport Wi-Fi to track Canadian travellers", Jan 2014, <http://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881>.

[I-D.ietf-6man-ipv6-address-generation-privacy] Cooper, A., Gont, F., and D. Thaler, "Privacy Considerations for IPv6 Address Generation Mechanisms", draft-ietf-6man-ipv6-address-generation-privacy-07 (work in progress), June 2015.

[I-D.ietf-dhc-anonymity-profile] Huitema, C., Mrugalski, T., and S. Krishnan, "Anonymity profile for DHCP clients", draft-ietf-dhc-anonymity-profile-00 (work in progress), May 2015.

[IETFMACRandom] Zuniga, JC., "MAC Privacy", November 2014, <http://www.ietf.org/blog/2014/11/mac-privacy/>.

Author's Address

Christian Huitema
Microsoft
Redmond, WA 98052
U.S.A.

Email: huitema@microsoft.com