6tisch
Internet-Draft
Intended status: Informational
Expires: April 30, 2015

R. Struik
Struik Security Consultancy

October 27, 2014

Observations about IPv6 Addressing
draft-struik-6lo-on-ipv6-addressing-00

Abstract

This document contains some observations on IPv6 addressing.

Requirements Language

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

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 April 30, 2015.

Copyright Notice

Table of Contents

1. Opaque identifiers

RFC7217 [RFC7217] describes a mechanism for generating opaque interface identifiers and argues that these identifiers improve security and privacy of IPv6 addresses, when compared to using modified EUI-64 address formats. The main case presented in that document is that using opaque interface identifiers, rather than fixed hardware device identifiers, thwarts attempts at correlating of host activities over time, tracking across multiple networks, and pinpointing devices that may exhibit known vulnerabilities.

There are also some down sides to adopting this opaque identifier format:

1. Use of opaque identifiers does not preclude traceability on layer 2. While this is an obvious remark, the reverse also seems to hold: if Layer 2 MAC addresses would be randomized (see, e.g., discussion on MAC address randomization at IETF-90), then derivation of IPv6 addresses using those randomized MAC adddreses (rather than the EUI-64 hardware address) would certainly serve the same purpose as the technique in RFC 7217. Moreover, IPv6 opaque addresses may trickle down to Layer 2, by deriving the randomized MAC address from the interface identifier (assumed to be at least 64-bit long). This would allow constrained nodes to derive compression benefits that would not be available if one would cut the ties between Layer 2 and Layer 3 address formats. As such, this would benefit "constrained cluster" specifications, such as RFC6282, RFC4944, and RFC 6755.

2. The algorithm in RFC 7217 for generating opaque interface identifiers RID depends on an intra-device secret key (secret_key), and some public parameters (Prefix, Net_Iface, Network_ID) and takes the form RID:=F(key, public parameters). It is noted that F() MUST be difficult to reverse, MUST not be computable without knowledge of the secret key, and should not

leak the secret key given a number of samples F(key,public parms), where parms are under the control of an adversary. The output should be at least 64 bits (and, in practice, mostly is). While the specification suggests that the secret key should, indeed, be kept secret, the specification seems to allow administrator access and depends on trustworthy bootstrapping. Since it cannot be verified outside the device whether the quantity RID and the opaque interface identifier were indeed generated as specified with a secret key unknown to any outside device, this leaves this technique open to "Big Brother"-esque manipulation. Indeed, it is not hard to see (inspired by [Surveillance]) that one could field devices, where device-internal private information could be leaked via the opaque interface identifier, no matter the good intentions: the supposedly opaque interface identifier simply serves as a so-called subliminal channel. This subliminal channel cannot be detected without close examination of the entire device implementation.

2. Security Considerations

This note illustrates that privacy is a system issue and illustrates examples where the opaque interface identifier could be turned into a subliminal channel for releasing secret information to a Big Brother agent, without means for detecting this.

3. IANA Considerations

There is no IANA action required for this document.

4. Acknowledgments

Kudos to Edward Snowden for introducing fascinating technical problems to the paranoid.

5. Normative References

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

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

[RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, March 2005.

[RFC6282] Hui, J. and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks", RFC 6282, September 2011.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, September 2007.

[RFC6755] Campbell, B. and H. Tschofenig, "An IETF URN Sub-Namespace for OAuth", RFC 6755, October 2012.

[I-D.ietf-6man-default-iids]
Gont, F., Cooper, A., Thaler, D., and W. Will, "Recommendation on Stable IPv6 Interface Identifiers", draft-ietf-6man-default-iids-01 (work in progress), October 2014.

[I-D.ietf-6man-why64]
Carpenter, B., Chown, T., Gont, F., Jiang, S., Petrescu, A., and A. Yourtchenko, "Analysis of the 64-bit Boundary in IPv6 Addressing", draft-ietf-6man-why64-07 (work in progress), October 2014.

[I-D.sarikaya-6lo-cga-nd]
Sarikaya, B. and F. Xia, "Lightweight and Secure Neighbor Discovery for Low-power and Lossy Networks", draft-sarikaya-6lo-cga-nd-01 (work in progress), October 2014.

[Surveillance]
Mihir Bellare, Kenneth G. Paterson, Phillip Rogaway, "Security of Symmetric Encryption Against Mass-Surveillance", CRYPTO 2014, IACR, August 2014.

Author’s Address

Rene Struik
Struik Security Consultancy

Email: rstruik.ext@gmail.com