Network Working Group
Internet-Draft
Intended status: Informational
Expires: April 4, 2016

D. Thaler
Microsoft

October 2, 2015

Privacy Considerations for IPv6 over Networks of Resource-Constrained Nodes
draft-thaler-6lo-privacy-considerations-01

Abstract

This document discusses how a number of privacy threats apply to technologies designed for IPv6 over networks of resource-constrained nodes, and provides advice to protocol designers on how to address such threats in IPv6-over-foo adaptation layer specifcations.

Table of Contents

1. Introduction

RFC 6973 [RFC6973] discusses privacy considerations for Internet protocols, and Section 5.2 in particular covers a number of privacy-specific threats. In the context of IPv6 addresses, Section 3 of [I-D.ietf-6man-ipv6-address-generation-privacy] provides further elaboration on the applicability of the privacy threats.

When interface identifiers (IIDs) are generated without sufficient entropy compared to the link lifetime, devices and users can become vulnerable to the various threats discussed there, including:

- Correlation of activities over time, if the same identifier is used for Internet traffic over period of time

- Location tracking, if the same interface identifier is used with different prefixes as a device moves between different networks

- Device-specific vulnerability exploitation, if the identifier helps identify a vendor or version or protocol and hence suggests what types of attacks to try

- Address scanning, which enables all of the above attacks by off-link attackers.

Typically "enough" bits of entropy means at least 46 bits (see Section 2 for why); ideally all 64 bits of the IID should be used, although historically some bits have been excluded for reasons discussed in [RFC7421].

For these reasons, [I-D.ietf-6man-default-iids] recommends using the address generation scheme in [RFC7217], rather than addresses generated from a fixed IEEE identifier.

Furthermore, to mitigate the threat of correlation of activities over time on long-lived links, [RFC4941] specifies the notion of a "temporary" address to be used for transport sessions (typically locally-initiated outbound traffic to the Internet) that should not be linkable to a more permanent identifier such as a DNS name, user name, or stable hardware address. Indeed, the default address selection rules [RFC6724] now prefer temporary addresses by default for outgoing connections. If a device needs to simultaneously support unlinkable traffic as well as traffic that is linkable to such a stable identifier, this necessitates supporting simultaneous use of multiple addresses per device.

2. Amount of Entropy Needed

In terms of privacy threats discussed in [I-D.ietf-6man-ipv6-address-generation-privacy], the one with the need for the most entropy is address scans. To mitigate address scans, one needs enough entropy to make the probability of a successful address probe be negligible. Typically this is measured in the length of time it would take to have a 50% probability of getting at least one hit. Address scans often rely on sending a packet such as a TCP SYN or ICMP Echo Request, and determining whether the reply is an ICMP unreachable error (if no host exists) or a TCP response or ICMP Echo Reply (if a host exists), or neither in which case nothing is known for certain.

Many privacy-sensitive devices support a "stealth mode" as discussed in Section 5 of [RFC7288] whereby they will not send a TCP RST or ICMP Echo Reply. In such cases, and when the device does not listen on a well-known TCP port known to the scanner, the effectiveness of an address scan is limited by the ability to get ICMP unreachable errors, since the attacker can only infer the presence of a host based on the absense of an ICMP unreachable error.

Generation of ICMP unreachable errors is typically rate limited to 2 per second (the default in routers such as Cisco routers running IOS 12.0 or later). Such a rate results in taking about a year to completely scan 26 bits of space.

The actual math is as follows. Let 2^N be the number of devices on the subnet. Let 2^M be the size of the space to scan (i.e., M bits of entropy). Let S be the number of scan attempts. The formula for a 50% chance of getting at least one hit in S attempts is: P(at least one success) = 1 - (1 - 2^N/2^M)^S = 1/2. Assuming 2^M >> S, this simplifies to: S * 2^N/2^M = 1/2, giving S = 2^(M-N-1), or M = N + 1 + log_2(S). Using a scan rate of 2 per second, this results in the following rule of thumb:

Bits of entropy needed = log_2(# devices per link) + log_2(seconds of link lifetime) + 2

For example, for a network with at most 2^16 devices on the same subnet, and the average lifetime of a device being 4 years (2^28 seconds) or less, this results in a need for at least 46 bits of entropy (16+28+2) so that an address scan would need to be sustained for longer than the lifetime of devices to have a 50% chance of getting a hit.

Although 46 bits of entropy may be enough to provide privacy in such cases, 59 or more bits of entropy would be needed if addresses are used to provide security against attacks such as spoofing, as CGAs [RFC3972] and HBAs [RFC5535] do, since attacks are not limited by ICMP rate limiting but by the processing power of the attacker. See those RFCs for more discussion.

If, on the other hand, the devices being scanned for do not implement a "stealth mode", but respond with TCP RST or ICMP Echo Reply packets, then the address scan is not limited by the ICMP unreachable rate limit in routers, since the attacker can determine the presence of a host without them. In such cases, more bits of entropy would be needed to provide the same level of protection.

3. Potential Approaches

The table below shows the number of bits of entropy currently available in various technologies:

Technology	Reference	Bits of Entropy
802.15.4	[RFC4944]	16+ or any EUI-64
Bluetooth LE	[I-D.ietf-6lo-btle]	48
DECT ULE	[I-D.ietf-6lo-dect-ule]	40 or any EUI-48
MS/TP	[I-D.ietf-6lo-6lobac]	8 or 64
ITU-T G.9959	[RFC7428]	8
NFC	[I-D.ietf-6lo-nfc]	6 or ???

Such technologies generally support either IEEE identifiers or so called "Short Addresses", or both, as link layer addresses. We discuss each in turn.

3.1. IEEE-Identifier-Based Addresses

Some technologies allow the use of IEEE EUI-48 or EUI-64 identifiers, or allow using an arbitrary 64-bit identifier. Using such an identifier to construct IPv6 addresses makes it easy to use the normal LOWPAN_IPHC encoding with stateless compression, allowing such IPv6 addresses to be fully elided in common cases.

Interfaces identifiers formed from IEEE identifiers can have insufficient entropy unless the IEEE identifier itself has sufficient entropy, and enough bits of entropy are carried over into the IPv6 address to sufficiently mitigate the threats. Privacy threats other than "Correlation over time" can be mitigated using per-network randomized IEEE identifiers with 46 or more bits of entropy. A number of such proposals can be found at <https://mentor.ieee.org/privecsg/documents>, and Section 10.8 of [BTCorev4.1] specifies one for Bluetooth. Using IPv6 addresses derived from such IEEE identifiers would be roughly equivalent to those specified in [RFC7217].

Correlation over time can be mitigated if the IEEE identifier itself changes often enough, such as each time the link is established, if the link lifetime is short. For further discussion, see [I-D.huitema-6man-random-addresses].

Another potential concern is that of efficiency, such as avoiding DAD all together when IPv6 addresses are IEEE-identifier-based. Appendix A of [RFC4429] provides an analysis of address collision probability based on the number of bits of entropy. A simple web search on "duplicate MAC addresses" will show that collisions do happen with MAC addresses, and thus based on the analysis in [RFC4429], using sufficient bits of entropy in random addresses can provide greater protection against collision than using MAC addresses.

3.2. Short Addresses

An IPv6 interface identifier formed from a "Short Address" and a set of well-known constant bits (such as padding with 0's) lacks sufficient entropy to mitigate address scanning unless the link lifetime is extremely short. Furthermore, an adversary could also use statisical methods to determine the size of the L2 address space and thereby make some inference regarding the underlying technology on a given link, and target further attacks accordingly.

When Short Addresses are desired on links that are not guaranteed to have a short enough lifetime, the mechanism for constructing an IPv6 interface identifier from a Short Address could be designed to

sufficiently mitigate the problem. For example, if all nodes on a given L2 network have a shared secret (such as the key needed to get on the layer-2 network), the 64-bit IID might be generated using a one-way hash that includes (at least) the shared secret together with the Short Address. The use of such a hash would result in the IIDs being spread out among the full range of IID address space, thus mitigating address scans, while still allowing full stateless compression/elision.

For long-lived links, "temporary" addresses might even be generated in the same way by (for example) also including in the hash the Version Number from the Authoritative Border Router Option (ABDO) if any. This would allow changing temporary addresses whenever the Version Number is changed, even if the set of prefix or context information is unchanged.

In summary, any specification using Short Addresses should carefully construct an IID generation mechanism so as to provide sufficient entropy compared to the link lifetime.

4. Recommendations

The following are recommended for adaptation layer specifications:

- Security (privacy) sections should say how address scans are mitigated. An address scan might be mitigated by having a link always be short-lived, or might be mitigated by having a large number of bits of entropy, or some combination. Thus, a specification should explain what the maximum lifetime of a link is in practice, and show how the number of bits of entropy is sufficient given that lifetime.

- Technologies must define a way to include sufficient bits of entropy in the IPv6 interface identifier, based on the maximum link lifetime. Specifying that a random EUI-48 or EUI-64 can be used is one easy way to do so, for technologies that support such identifiers.

- Specifications should not simply construct an IPv6 interface identifier by padding a short address with a set of other well-known constant bits, unless the link lifetime is guaranteed to be extremely short.

- Specifications should make sure that an IPv6 address can change over long periods of time. For example, the interface identifier might change each time a device connects to the network (if connections are short), or might change each day (if connections can be long). This is necessary to mitigate correction over time.

- o If a device can roam between networks, and more than a few bits of entropy exist in the IPv6 interface identifier, then make sure that the interface identifier can vary per network as the device roams. This is necessary to mitigate location tracking.

5. IANA Considerations

This document has no actions for IANA.

6. Security Considerations

This entire document is about security considerations and how to specify possible mitigations.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <http://www.rfc-editor.org/info/rfc2119>.

7.2. Informative References

[RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, DOI 10.17487/RFC3972, March 2005, <http://www.rfc-editor.org/info/rfc3972>.

[RFC4429] Moore, N., "Optimistic Duplicate Address Detection (DAD) for IPv6", RFC 4429, DOI 10.17487/RFC4429, April 2006, <http://www.rfc-editor.org/info/rfc4429>.

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, DOI 10.17487/RFC4941, September 2007, <http://www.rfc-editor.org/info/rfc4941>.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, DOI 10.17487/RFC4944, September 2007, <http://www.rfc-editor.org/info/rfc4944>.

[RFC5535] Bagnulo, M., "Hash-Based Addresses (HBA)", RFC 5535, DOI 10.17487/RFC5535, June 2009, <http://www.rfc-editor.org/info/rfc5535>.

[RFC6724] Thaler, D., Ed., Draves, R., Matsumoto, A., and T. Chown, "Default Address Selection for Internet Protocol Version 6 (IPv6)", RFC 6724, DOI 10.17487/RFC6724, September 2012, <http://www.rfc-editor.org/info/rfc6724>.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, DOI 10.17487/RFC6973, July 2013, <http://www.rfc-editor.org/info/rfc6973>.

[RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/RFC7217, April 2014, <http://www.rfc-editor.org/info/rfc7217>.

[RFC7288] Thaler, D., "Reflections on Host Firewalls", RFC 7288, DOI 10.17487/RFC7288, June 2014, <http://www.rfc-editor.org/info/rfc7288>.

[RFC7421] Carpenter, B., Ed., Chown, T., Gont, F., Jiang, S., Petrescu, A., and A. Yourtchenko, "Analysis of the 64-bit Boundary in IPv6 Addressing", RFC 7421, DOI 10.17487/RFC7421, January 2015, <http://www.rfc-editor.org/info/rfc7421>.

[RFC7428] Brandt, A. and J. Buron, "Transmission of IPv6 Packets over ITU-T G.9959 Networks", RFC 7428, DOI 10.17487/RFC7428, February 2015, <http://www.rfc-editor.org/info/rfc7428>.

[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-08 (work in progress), September 2015.

[I-D.ietf-6man-default-iids] Gont, F., Cooper, A., Thaler, D., and S. LIU, "Recommendation on Stable IPv6 Interface Identifiers", draft-ietf-6man-default-iids-07 (work in progress), August 2015.

[I-D.ietf-6lo-6lobac] Lynn, K., Martocci, J., Neilson, C., and S. Donaldson, "Transmission of IPv6 over MS/TP Networks", draft-ietf-6lo-6lobac-02 (work in progress), July 2015.

[I-D.ietf-6lo-btle]
Nieminen, J., Savolainen, T., Isomaki, M., Patil, B., Shelby, Z., and C. Gomez, "IPv6 over BLUETOOTH(R) Low Energy", draft-ietf-6lo-btle-17 (work in progress), August 2015.

[I-D.ietf-6lo-dect-ule]
Mariager, P., Petersen, J., Shelby, Z., Logt, M., and D. Barthel, "Transmission of IPv6 Packets over DECT Ultra Low Energy", draft-ietf-6lo-dect-ule-03 (work in progress), September 2015.

[I-D.ietf-6lo-nfc]
Youn, J. and Y. Hong, "Transmission of IPv6 Packets over Near Field Communication", draft-ietf-6lo-nfc-01 (work in progress), July 2015.

[I-D.huitema-6man-random-addresses]
Huitema, C., "Implications of Randomized Link Layers Addresses for IPv6 Address Assignment", draft-huitema-6man-random-addresses-02 (work in progress), August 2015.

[BTCorev4.1]
Bluetooth Special Interest Group, "Bluetooth Core Specification Version 4.1", December 2013, <https://www.bluetooth.org/DocMan/handlers/DownloadDoc.ashx?doc_id=282159>.

Author's Address

Dave Thaler
Microsoft
One Microsoft Way
Redmond, WA 98052
USA

Email: dthaler@microsoft.com