dhc
Internet-Draft
Updates: 3315 (if approved)
Intended status: Standards Track
Expires: September 10, 2015

T. Mrugalski
ISC
S. Krishnan
Ericsson

March 9, 2015

Mitigation of Privacy Concerns in DHCPv6
draft-mrugalski-dhc-dhcpv6-privacy-mitigation-00

Abstract

There is work ongoing in the dhc working group that discusses the various identifiers used by DHCPv6 and the potential privacy implications. This draft explores several migitation techniques that could be used to address the privacy issues in DHCPv6. This draft is expected to evolve significantly over time, but the ultimate goal is to standardize mitigation techniques the DHC working group considers useful.

Status of This Memo

This Internet-Draft will expire on September 10, 2015.

Copyright Notice

Table of Contents

1. Introduction

DHCPv6 [RFC3315] is a protocol that is used to provide addressing and configuration information to IPv6 hosts. The DHCPv6 protocol uses several identifiers that could become a source for gleaning additional information about the IPv6 host. This information may include device type, operating system information, location(s) that the device may have previously visited, etc. [I-D.ietf-dhc-dhcpv6-privacy] discusses the various identifiers used by DHCPv6 and the potential privacy issues [RFC6973]. This document proposes

2. Terminology

This document uses the term "Stable identifier" as defined in [I-D.ietf-dhc-dhcpv6-privacy]

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 [RFC2119]. When these words are not in ALL CAPS (such as "should" or "Should"), they have their usual English meanings, and are not to be interpreted as [RFC2119] key words.

3. Client Mitigation Techniques

3.1. Not disclose the desire for privacy

A naive approach to privacy would be to simply disclose the desire to protect one's privacy, e.g. by sending requests for temporary addresses or defining a new type of temporary DUID that would be changing over time. This is not workable in a large number of cases as it is possible that the network operator (or other entities that have access to the operator's network) might be actively participating in surveillance and anti-privacy, willingly or not. Simply revealing the desire for privacy, could cause the attacker to react by triggering additional surveillance or monitoring mechanisms. Therefore we feel that it is preferable to not disclose one's desire for privacy. This preference leads to some important implications. In particular, we make an effort to make the mitigation techniques difficult to distinguish from regular client behaviors, if at all possible.

3.2. Use randomized DUIDs

One of the primary privacy concerns is that a client is disclosing a stable identifier (the DUID) that can be use for tracking and profiling. The most common way of disclosing client's MAC/hardware address in DHCPv6 is to use DUID type LLT (link-layer with time) or LL (link-layer). Another DUID of type UUID is also bad in this regard, as its the UUID may contain additional information about the device it is tied to.

Discussion: As stated in Section 3.1, the desire for privacy should not be explicitly advertised. Therefore a new DUID type is not recommended here.

PROPOSAL: The clients that want to protect their privacy SHOULD generate a new randomized DUID-LLT every time they attach to a new link or detect a possible link change event. The exact details are left up to implementors, but there are several factors should be taken into consideration. The DUID type SHOULD be set to 1 (DUID-LLT). Hardware type SHOULD be set appropriately to the hardware type. Time MAY be set to current time, but this will reveal the fact that the DUID is newly generated. Implementors interested in hiding

this fact MAY use a time stamp from the past. e.g. a random timestamp from the previous year could be a good value. In the most common cases the link-layer address is based on MAC. The first three octets are composed of the OUI (Organizationally Unique Identifier) that is expected to have a value assigned to a real organization. See [IEEE-OUI] for currently assigned values. Using a value that is unassigned may disclose the fact that a DUID is randomized. Using a value that belongs to a third party may have legal implications.

3.3. Do not send Confirm messages

The [RFC3315] requires clients to send a Confirm message when they attach to a new link to verify whether the addressing and configuration information they previously received is still valid. When these clients send Confirm messages, they include any IAs assigned to the interface that may have moved to a new link, along with the addresses associated with those IAs. By examining the addresses in the Confirm message an attacker can trivially identify the previous point(s) of attachment.

PROPOSAL: Clients interested in protecting their privacy SHOULD NOT send Confirm messages and instead directly try to acquire addresses on the new link.

3.4. Obtain temporary addresses

[RFC3315] defines a special container (IA_TA) for requesting temporary addresses. This is a good mechanism in principle, but there are a number of issues associated with it. First, this is not widely used feature, so clients depending solely on temporary addresses may lock themselves out of service. Secondly, [RFC3315] does not specify any renewal mechanisms for temporary addresses. Therefore support for renewing temporary addresses may vary between server implementations, including not being supported at all. Finally, by requesting temporary addresses a client reveals its desire for privacy and potentially risks countermeasures as described in Section 3.1.

PROPOSAL: Clients interested in their privacy SHOULD not use IA_TA. They should simply send an IA_NA with a randomized IAID. This, along with the mitigation technique discussed in Section 3.2, will ensure that a client will get a new address that can be renewed and can be used as long as needed. To get a new address, it can send Request message with a new randomized IAID before releasing the other one. This will cause the server to assign a new address, as it still has a valid lease for the old IAID value. Once a new address is assigned, the address obtained using the older IAID value can be released safely, using the Release message or it may simply be allowed to time out.

This proposal may not work if the server enforces specific policies, e.g. only one address per client. If client does not succeed in receiving a second address using a new IAID, it may release the first one (using an old IAID) and then retry asking for a new address.

From the Operating System perspective, addresses obtained using this technique SHOULD be treated as temporary as specified in [RFC4941].

3.5. Do not request the FQDN Option

A typical client uses FQDN option, defined in [RFC4704] to negotiate with a server the DNS entries that should be updated. In the process, the client typically reveals its hostname and possibly its home domain. Server, depending on configured policies, may accept or override the name with network specific information.

PROPOSAL: Clients SHOULD avoid disclosing their hostnames, as the hostnames may contain personally identifying information (e.g. "Tomek's laptop"). Even if the hostname does not contain personally identifying information, it can still be used as a stable identifier for tracking. Therefore a client SHOULD not send FQDN option at all. This ensures that the host does not expose a stable identifier, but also implies that the host will not have a resolvable DNS name. Should DNS name be useful, a client SHOULD send a randomly generated hostname, consisting of a single label. The server is expected to append the domain name and return FQDN to the client. Client can then use this FQDN as its temporary hostname that will be discarded once its location changes or the client chooses to assume a new identity.

3.6. Randomize ordering of Options in messages and in the ORO

A DHCPv6 client may reveal other types of information, besides unique identifiers. There are many ways a DHCPv6 client can perform certain actions and the specifics can be used to fingerprint the client. This may not reveal the identity of a client, but may provide

additional information, such as the device type, vendor type or OS type and in some cases specific version.

One specific method used for fingerprinting utilizes the order in which options are included in the message. Another related technique utilizes the order in which option codes are included in an ORO (Option Request Option).

PROPOSAL: The client willing to protect its privacy SHOULD randomize options order before sending any DHCPv6 message. Such a client SHOULD also randomly shuffle the option codes order in ORO.

3.7. Anonymous Information-Request

According to [RFC3315], a DHCPv6 client typically includes its client identifier in most of the messages it sends. There is one exception, however. Client is allowed to omit its client identifier when sending Information-Request.

PROPOSAL: When using stateless DHCPv6, clients wanting to protect their privacy SHOULD not include client identifiers in their Information-Request messages. This will prevent the server from specifying client-specific options if it is configured to do so, but the need for anonymity precludes such options anyway.

4. Server Mitigation Techniques

TODO: - don't send GEOLOCATION options to anyone who asks (preferably don't sent that option at all); - if running on mobile device, possibly change its server-id when its link flips; - don't send FQDN options if you don't intend to do actual DNS Updates; -

5. Security Considerations

The use of randomized DUIDs and IAIDs allows malicious clients to exhaust address and prefix pools on DHCPv6 servers by simply requesting more and more addresses/prefixes. This attack is certainly possible already in today's networks, but this document provides a *legitimate* use case for random DUIDs and IAIDs making countermeasures more difficult. In addition to exhausting configured address and prefix pools, these clients may also cause increased state (and hence resource utilization) on the DHCPv6 servers.

6. Privacy Considerations

This document at its entirety discusses privacy considerations in DHCPv6. As such, no separate section about this is needed.

7. IANA Considerations

This draft does not request any IANA action.

8. Acknowledgements

The authors would like to thanks the valuable comments made by Stephen Farrell, Ted Lemon, Ines Robles, Russ White, Christian Schaefer and other members of DHC WG.

This document was produced using the xml2rfc tool [RFC2629].

9. References

9.1. Normative References

[I-D.ietf-dhc-dhcpv6-privacy]
Krishnan, S., Mrugalski, T., and S. Jiang, "Privacy considerations for DHCPv6", draft-ietf-dhc-dhcpv6-privacy-00 (work in progress), February 2015.

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

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

9.2. Informative References

[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-03 (work in progress), January 2015.

[IEEE-OUI]
IEEE, "Organizationally Unique Identifiers http://www.ieee.org/netstorage/standards/oui.txt", .

[RFC2629] Rose, M., "Writing I-Ds and RFCs using XML", RFC 2629, June 1999.

[RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, December 2003.

[RFC4580] Volz, B., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Subscriber-ID Option", RFC 4580, June 2006.

[RFC4649] Volz, B., "Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Relay Agent Remote-ID Option", RFC 4649, August 2006.

[RFC4704] Volz, B., "The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Client Fully Qualified Domain Name (FQDN) Option", RFC 4704, October 2006.

[RFC4776] Schulzrinne, H., "Dynamic Host Configuration Protocol (DHCPv4 and DHCPv6) Option for Civic Addresses Configuration Information", RFC 4776, November 2006.

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

[RFC5007] Brzozowski, J., Kinnear, K., Volz, B., and S. Zeng, "DHCPv6 Leasequery", RFC 5007, September 2007.

[RFC5460] Stapp, M., "DHCPv6 Bulk Leasequery", RFC 5460, February 2009.

[RFC5970] Huth, T., Freimann, J., Zimmer, V., and D. Thaler, "DHCPv6 Options for Network Boot", RFC 5970, September 2010.

[RFC6225] Polk, J., Linsner, M., Thomson, M., and B. Aboba, "Dynamic Host Configuration Protocol Options for Coordinate-Based Location Configuration Information", RFC 6225, July 2011.

[RFC6355] Narten, T. and J. Johnson, "Definition of the UUID-Based DHCPv6 Unique Identifier (DUID-UUID)", RFC 6355, August 2011.

[RFC6939] Halwasia, G., Bhandari, S., and W. Dec, "Client Link-Layer Address Option in DHCPv6", RFC 6939, May 2013.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, July 2013.

Authors' Addresses

Tomek Mrugalski
Internet Systems Consortium, Inc.
950 Charter Street
Redwood City, CA 94063
USA

Email: tomasz.mrugalski@gmail.com

Suresh Krishnan
Ericsson
8400 Decarie Blvd.
Town of Mount Royal, QC
Canada

Phone: +1 514 345 7900 x42871
Email: suresh.krishnan@ericsson.com