DHC Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 20, 2016

Y. Cui
L. Li
J. Wu
Tsinghua University
L. Yiu
Comcast

October 18, 2015

Encryption Mechanism for DHCPv6
draft-cui-dhc-dhcpv6-encryption-04

Abstract

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) enables DHCPv6 servers to configure network parameters dynamically. However, due to the unsecured nature, various critical identifiers used in DHCPv6 are vulnerable to several types of attack. In order to protect the DHCPv6 from passive attack, such as pervasive monitoring attack, this document provides a mechanism to achieve the encryption between the DHCPv6 client and server.

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 20, 2016.

Copyright Notice

Table of Contents

1. Introduction

The Dynamic Host Configuration Protocol for IPv6 [RFC3315] enables DHCPv6 servers to configure network parameters dynamically. Due to the unsecured nature of DHCPv6, the various critical identifiers are vulnerable to several types of attacks, particularly pervasive monitoring (PM) [RFC7258]. [I-D.ietf-dhc-dhcpv6-privacy] analyses the DHCPv6 privacy issues and discusses how various identifiers used in DHCPv6 could become a source for gleaning additional information of an individual. The IETF has expressed strong agreement that PM is an attack that needs to be mitigated where possible in [RFC7258].

Prior work has addressed some aspects of DHCPv6 security, but until now there has been little work to protect the DHCPv6 from passive attack, such as pervasive monitoring attack. Secure DHCPv6 [I-D.ietf-dhc-sedhcpv6] provides the authentication mechanism between DHCPv6 client and server along with the DHCPv6 transaction. However, the DHCPv6 message is still transmitted in clear text and the private information within the DHCPv6 message is not protected from pervasive monitoring. Anonymity profile for DHCP clients [I-D.ietf-dhc-anonymity-profile] provides guidelines on the composition of DHCPv4 or DHCPv6 request to minimize the disclosure of

identifying information. However, anonymity profile limits the use of the certain options and cannot protect all identifiers used in DHCP if new option containing some private information is defined. In addition, the anonymity profile cannot work in some situation where the client wants anonymity to attackers but not to the valid DHCP server. Besides, a separate encryption mechanism such as DTLS is also infeasible for DHCPv6, because the DHCPv6 relay can not recognize the 'secure' DHCPv6 message and may drop the DTLS messages.

The proposed solution provides a mechanism to achieve the encryption between the DHCPv6 client and server in order to protect the DHCPv6 from passive attack, such as pervasive monitoring. Before the DHCPv6 configuration process, the Information-request and Reply messages exchange is used to inform the client of the server's public key. After the public key exchange, the following DHCPv6 messages are encrypted and encapsulated into two newly defined DHCPv6 messages: Encrypted-Query and Encrypted-Response. In this way, the various identifiers contained in DHCPv6 message are protected from passive attack.

2. Requirements Language

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].

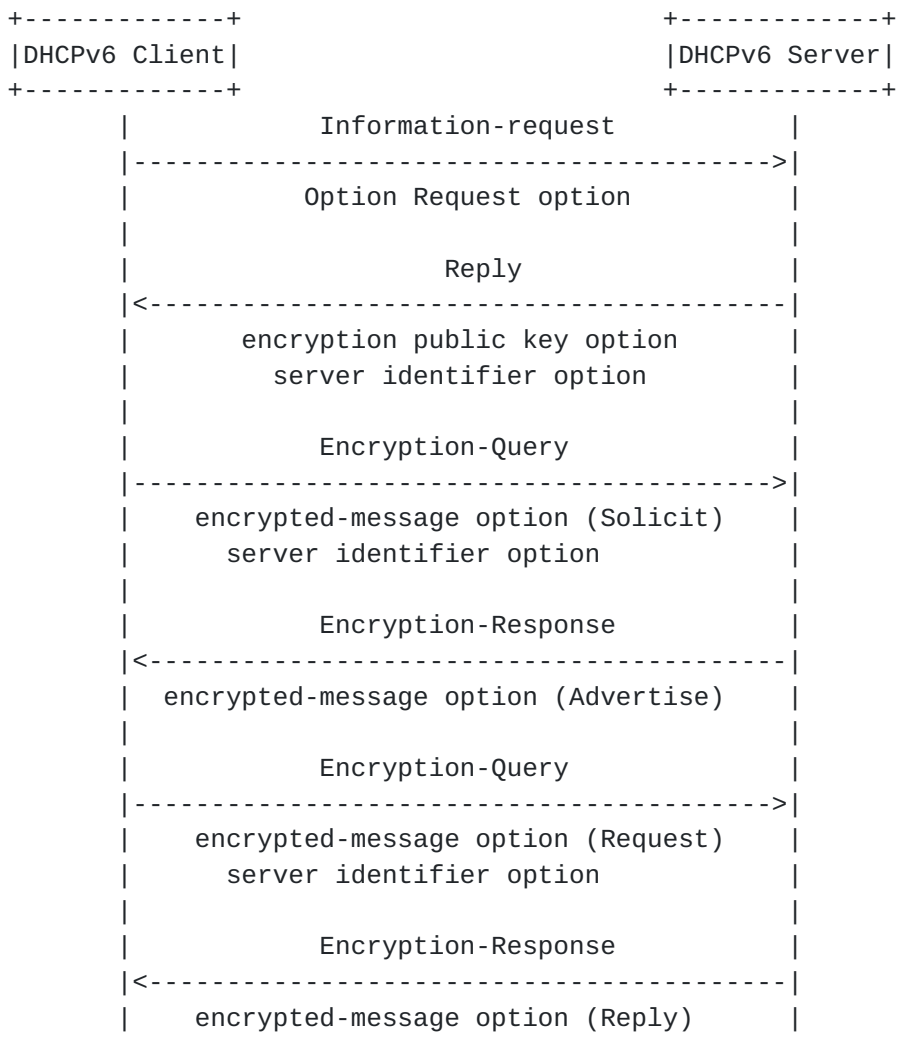
3. Solution Overview

In the proposed solution, the server's public key is communicated to the client before the standard DHCPv6 transactions. Once the client gets notified with the public key, the successive DHCPv6 configuration process can be encrypted with the recipient's public key. The encrypted DHCPv6 messages are put into the newly defined DHCPv6 option: encrypted-message option, and encapsulated into the two new DHCPv6 messages: Encrypted-Query and Encrypted-Response. This mechanism is used for the stateful DHCPv6 process starting with a SOLICIT message and the stateless DHCPv6 process starting with an Information-request message.

This solution is based on the public/private key pairs of the DHCPv6 client and server. The client/server firstly generates a pair of public/private keys. The solution adds the Information-request and Reply messages exchange before the standard DHCPv6 configuration process. The information-request message is used by the client to obtain the server's public key information without having addresses assigned to it. The DHCPv6 client firstly multicasts an Information-request message to DHCPv6 servers. The client MUST request the encryption public key option in the Option Request option. When

receiving the Information-request message with the request for encryption public key, the server sends the Reply message that contains the server's public key option and server identifier option. Upon the receipt of the Reply message, the DHCPv6 client records the server's DUID as well as the corresponding public key. If the client receives multiple Reply messages, the client selects one DHCPv6 server for the following network parameters configuration.

After the server's public key notification, the following DHCPv6 exchanges are encrypted with the recipient's public key and encapsulated into the encrypted-message option. For the stateful/ stateless scenario, the Solicit/Information-request message MUST contain the public key option to communicate the client's public key. The client sends the Encrypted-Query message to server, which carries the server identifier option and the encrypted-message option. The DHCPv6 server replies with the Encrypted-Response message to client, which contains the encrypted-message option. The following figure illustrates the DHCPv6 encryption procedure of the client-server exchanges involving four messages.



DHCPv6 Encryption Procedure

4. Client Behavior

If the client supports the encryption mode, it MUST generate a public/private key pair. For the client supporting the encryption mode, it multicasts the Information-request message to the DHCPv6 servers. The Information-request message MUST NOT include any option which may reveal the private information of the client, such as the client identifier option. The client MUST include an Option Request option to request the encryption public key option.

When the DHCPv6 client receives the Reply messages, the client MUST discard the those that do not contain the encryption public key option or the sever identifier option. Upon the receipt of the Reply message, the DHCPv6 client records the server's DUID as well as the corresponding public key. If the client receives multiple Reply messages, the client selects one DHCPv6 server for the following

network parameters configuration.

Once the server's public key is informed, the DHCPv6 client sends the Encrypted-Query message to the DHCPv6 server. The Encrypted-Query message is constructed with the encrypted-message option and server identifier option. The encrypted-message option contains the DHCPv6 message that is encrypted using the selected server's public key. The server identifier option is externally visible to avoid extra cost by those unselected servers. The Solicit/Information-request message MUST contain the public key option for the client's public key exchange.

For the received Encrypted-Response message, the client extracts the encrypted-message option and decrypts it using its private key to obtain the original DHCPv6 message. Then it handles the message as per [RFC3315]. If the client fails to get the proper parameters from the chosen server, it sends the Encrypted-Query message to another authenticated server for parameters configuration until the client obtains the proper parameters.

5. Relay Agent Behavior

When a DHCPv6 relay agent receives an Encrypted-query or Encrypted-response message, it may not recognize this message. The unknown messages MUST be forwarded as describes in [RFC7283].

When a DHCPv6 relay agent recognizes the Encrypted-query and Encrypted-response messages, it forwards the message according to section 20 of [RFC3315].

6. Server Behavior

When the DHCPv6 server receives the Information-request message with encryption public key option request, it replies the Reply message to the client, which includes the encryption public key option and server identifier option.

Upon the receipt of Encrypted-Query message, the server checks the server identifier option. It decrypts the encrypted-message option using its private key if it is the target server. The DHCPv6 server drops the message that is not for it, thus not paying cost to decrypt the message. If the decrypted message is the Solicit/Information-request message, the server MSUT discard the decrypted message that does not include the encryption public key option. The server is informed of the client's public through the encryption public key option contained in the Solicit/Information-request message.

After the server is informed of the client's public key, the DHCPv6

messages, which is sent from server to client, is encrypted using the client's public key. The encrypted DHCPv6 message is encapsulated into the encrypted-message option. The Encrypted-Response message contains the encrypted-message option.

7. New DHCPv6 Messages

There are two DHCPv6 messages defined: Encrypted-Query and Encrypted-Response. Both DHCPv6 messages defined in this document share the following format:

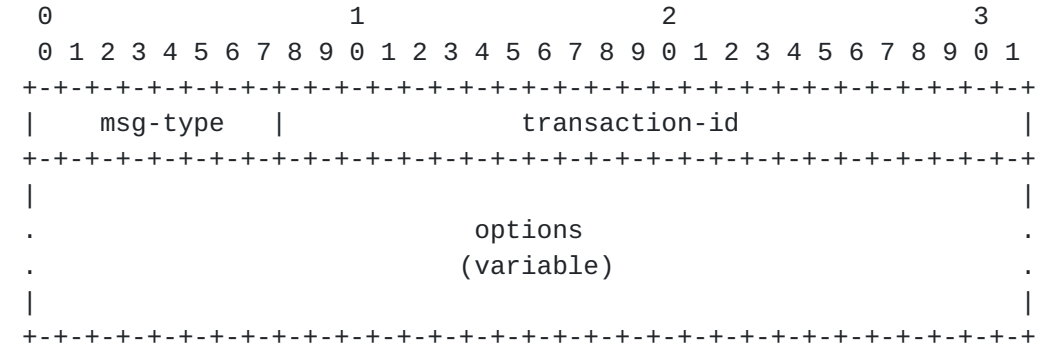


Figure 1: The format of New DHCPv6 Messages

msg-type ENCRYPTED-QUERY (TBA1), ENCRYPTED-RESPONSE (TBA2).

transaction-id The transaction ID for this message exchange.

options Options carried in this message.

8. New DHCPv6 Options

8.1. Encrypted-message Option

The encrypted-message option carries the encrypted DHCPv6 message with the recipient's public key.

The format of the encrypted-message option is:

Figure 2: encrypted-message Option Format

option-code OPTION_ENCRYPTED_MSG (TBA3).

option-len Length of the encrypted DHCPv6 message.

encrypted DHCPv6 message A variable length field containing the encrypted DHCPv6 message sent by the client or server. In Encrypted-Query message, it contains encrypted DHCPv6 message sent by a client. In Encrypted-response message, it contains encrypted DHCPv6 message sent by a server.

8.2. Encryption Public Key Option

The encryption public key option is defined to carry the sender's public key.

The format of the encryption public key option is:

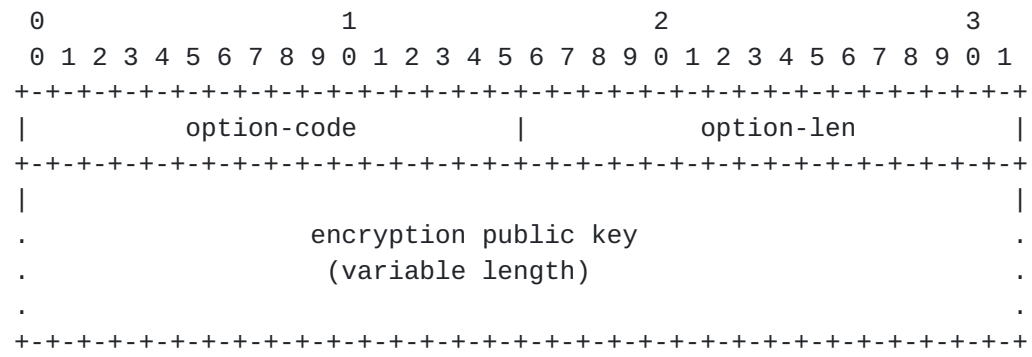


Figure 3: Encryption Public Key Option Format

option-code OPTION_ENCRYPTION_PUBLIC_KEY (TBA4).

option-len Length of the encryption public key.

encryption public key A variable length field containing the

sender's public key. The sender's public key is used for the following messages encryption.

9. Security Considerations

TBD

10. IANA Considerations

There are two new DHCPv6 messages defined and two new DHCPv6 options defined. The IANA is requested to assign values for these two messages and two options.

The two messages are:

- ENCRYPTED-QUERY (TBA1).
- ENCRYPTED-RESPONSE (TBA2).

The two options are:

- OPTION_ENCRYPTED_MSG (TBA3)
- OPTION_ENCRYPTION_PUBLIC_KEY (TBA4)

11. Contributors

The authors would like to thank Bernie Volz, Tomek Mrugalski, Ralph Droms, Randy Bush, Stephen Farrell, Christian Huitema, Nico Williams, Erik Kline, Alan DeKok, Bernard Aboba, Sam Hartman, Qi Sun, Zilong Liu and Cong Liu.

12. References

12.1. 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>.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July 2003, <http://www.rfc-editor.org/info/rfc3315>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <http://www.rfc-editor.org/info/rfc5280>.

[RFC7283] Cui, Y., Sun, Q., and T. Lemon, "Handling Unknown DHCPv6 Messages", RFC 7283, DOI 10.17487/RFC7283, July 2014, <http://www.rfc-editor.org/info/rfc7283>.

[RFC7435] Dukhovni, V., "Opportunistic Security: Some Protection Most of the Time", RFC 7435, DOI 10.17487/RFC7435, December 2014, <http://www.rfc-editor.org/info/rfc7435>.

12.2. Informative References

[I-D.ietf-dhc-anonymity-profile] Huitema, C., Mrugalski, T., and S. Krishnan, "Anonymity profile for DHCP clients", draft-ietf-dhc-anonymity-profile-04 (work in progress), October 2015.

[I-D.ietf-dhc-dhcpv6-privacy] Krishnan, S., Mrugalski, T., and S. Jiang, "Privacy considerations for DHCPv6", draft-ietf-dhc-dhcpv6-privacy-01 (work in progress), August 2015.

[I-D.ietf-dhc-sedhcpv6] Jiang, S., Shen, S., Zhang, D., and T. Jinmei, "Secure DHCPv6", draft-ietf-dhc-sedhcpv6-08 (work in progress), June 2015.

[RFC7258] Farrell, S. and H. Tschofenig, "Pervasive Monitoring Is an Attack", BCP 188, RFC 7258, DOI 10.17487/RFC7258, May 2014, <http://www.rfc-editor.org/info/rfc7258>.

Authors' Addresses

Yong Cui
Tsinghua University
Beijing 100084
P.R.China

Phone: +86-10-6260-3059
Email: yong@csnet1.cs.tsinghua.edu.cn

Lishan Li
Tsinghua University
Beijing 100084
P.R.China

Phone: +86-15201441862
Email: lilishan9248@126.com

Jianping Wu
Tsinghua University
Beijing 100084
P.R.China

Phone: +86-10-6278-5983
Email: jianping@cernet.edu.cn

Yiu Lee
Comcast
Philadelphia 19103
USA

Email: yiu_lee@cable.comcast.com