DHC Working Group
Internet-Draft
Intended status: Standards Track
Expires: March 2, 2016

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

August 30, 2015

Authentication and Encryption Mechanism for DHCPv6
draft-cui-dhc-dhcpv6-encryption-03

Abstract

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) enables DHCPv6 servers to configure network parameters. However, due to the unsecured nature, various critical identifiers used in DHCPv6 are vulnerable to several types of attacks, particularly pervasive monitoring. This document provides a mechanism to secure DHCPv6 messages, which achieves the server authentication and encryption between the DHCPv6 client and server.

Table of Contents

1. Introduction

The Dynamic Host Configuration Protocol for IPv6 [RFC3315] enables DHCPv6 servers to configure network parameters dynamically. [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. Due to the unsecured nature of DHCPv6, the various critical identifiers are vulnerable to several types of attacks, particularly pervasive monitoring [RFC7258].

Prior work has addressed some aspects of DHCPv6 security, but until now there has been little work on privacy between a DHCPv6 client and server. 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. The IETF has expressed strong agreement that PM is an attack that needs to be mitigated where possible. 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 the 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 clients want anonymity to attackers but not to the valid DHCP server. In addition, 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 achieves the server authentication and encryption between DHCPv6 client and server. The DHCPv6 server authentication is achieved before the DHCPv6 configuration process. The Information-request and Reply message exchange is used to contain the server's certificate. After the server authentication, the following DHCPv6 messages are encrypted and encapsulated into two newly defined DHCPv6 messages: Encrypted-Query and Encrypted-Response. In this way, identifiers including the entity's DUID are protected.

The proposed secure mechanism can provide the following functions to improve security of DHCPv6:

- o authenticate the DHCPv6 server.

- o Encrypt the DHCPv6 configuration messages between DHCPv6 client and server once the public keys exchange is completed.

- o Anti-replay protection based on timestamps.

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

This solution proposes the server authentication before the standard DHCPv6 transactions; Once the authentication, the following DHCPv6 messages are encrypted with the recipient's public key. The encrypted DHCPv6 messages are put into the newly defined Encrypted-Message option, and encapsulated into Encrypted-Query and Encrypted-Response DHCPv6 messages that are defined in this document. The proposed mechanism is used for the stateful DHCPv6 session starting with a SOLICIT message and the stateless DHCPv6 session starting with an Information-Request message.

This solution is based on the public/private key pairs of the DHCPv6 client and server. The server and client firstly generate a pair of public/private keys. The server SHOULD acquire a public key certificate from the CA that signs the public key. A trust

relationship for a certificate could be established by TOFU with option of other stronger mechanism depending on the application need. TOFU can be used by a client to authenticate a server and its message in default without a pre-established trust relationship between the client and the server.

The solution adds a two-way communication before the standard DHCPv6 configuration process. The DHCPv6 client firstly multicasts an Information-request message to the DHCPv6 servers. The Information-request message is RECOMMENDED to contain no options, so that it reveals no private information of the client. When receiving the Information-Request message, the server replies the Reply message that contains the server's certificate, timestamp, signature and DUID. Upon the receipt of the Reply message, the DHCPv6 client verifies the identity of the DHCPv6 server and checks the timestamp. If the validation and timestamp check are successful, the client gets the server's DUID as well as the public key from the certificate. For the authenticated servers, the client selects one DHCPv6 server for network parameters configuration.

After the server authentication, the following DHCPv6 messages 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, the timestamp option and the signature option for client's public key exchange. The client sends the Encrypted-Query message to server, which carries the server identifier option and an Encrypted-Message option. The DHCPv6 server sends the Encrypted-Response message to client which contains the Encrypted-Message option. The following figure shows the DHCPv6 authentication and encryption procedure for the client-server exchanges involving four messages.

[RFC7283] enables relays to support the newly defined DHCPv6 messages without any change.

```
           +-------------+                          +-------------+
           |DHCPv6 Client|                          |DHCPv6 Server|
           +-------------+                          +-------------+
                  |            Information-Request          |
                  |---------------------------------------->|
                  |                                         |
                  |                    Reply                |
                  |<----------------------------------------|
                  |  certificate option   signature option  |
                  |            timestamp option             |
                  |         server identifier option        |
                  |                                         |
                  |            Encryption-Query             |
                  |---------------------------------------->|
                  |    Encrypted-Message option (Solicit)   |
                  |      server identifier option           |
                  |                                         |
                  |            Encryption-Query             |
                  |<----------------------------------------|
                  |  Encrypted-Message option (Advertise)   |
                  |                                         |
                  |            Encryption-Query             |
                  |---------------------------------------->|
                  |    Encrypted-Message option (Request)   |
                  |      server identifier option           |
                  |                                         |
                  |            Encryption-Query             |
                  |<----------------------------------------|
                  |    Encrypted-Message option (Reply)     |

              DHCPv6 Authentication and Encryption Procedure
```

4. Client Behavior

If the client supports the secure mode, it MUST generate a public/private key pair. For the client supporting the secure mode, it multicasts the Information-Request message to the DHCPv6 servers. To protect the client's privacy, the Information-Request message is RECOMMENDED to reveal no private information to the server. To provide a "dummy" Encryption-Request message, it is RECOMMENDED to send the Encryption-Request message with no option.

When the DHCPv6 client receives the Reply message, it validates the server's identity and checks the timestamp. The server's authentication could be established by TOFU with option of other stronger mechanism depending on the application need. TOFU calls for accepting and storing a certificate associated with an asserted identity, without authenticating that assertion. The client creates

a local trusted certificate record list for the verified certificate and the corresponding server identifier. A certificated that finds a match in the local trust certificate list is treated as verified. The timestamp is checked according to the rule defined in [I-D.ietf-dhc-sedhcpv6]. For the authenticated servers, the client selects one DHCPv6 server for network parameters configuration. And the following DHCPv6 message is encrypted using the elected server's public key.

Once the public keys exchange is completed, the DHCPv6 messages sent from client to server are encrypted using the public key retrieved from the server's certificate. The encrypted DHCPv6 message is encapsulated into the Encrypted-Message option. The Encrypted-Query message is constructed with the Encrypted-Message option and server identifier option. The server identifier option is externally visible to avoid extra cost by those unselected servers. If the client fails to get the proper parameters from the chosen server, it will send the Information-Query message to other authenticated servers for IPv6 configuration. The Solicit message MUST contain the public key option, the timestamp option and the signature option for client's public key exchange. The selected server is informed of the client's public key through the Solicit message which is decrypted from the Encrypted-Message option.

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 will send the Encrypted-Query message to other authenticated server for parameters configuration until the client obtains the proper parameters.

5. Server Behavior

When the DHCPv6 server receives the Information-Request message, it replies the Reply message to the client, which includes the server's digital signature, certificate, timestamp and server identifier.

On the receipt of Encrypted-Query message, the server checks the visible server identifier option. It decrypts the Encrypted-Message option using its private key if it is the target server. The DHCPv6 server drops the messages that are not for it, thus not paying cost to decrypt the message. If the decrypted message is the Solicit message, the server checks the timestamp and the signature. If the check succeeds, the server is informed of the client's public key through the contained public key option.

The DHCPv6 messages, which is sent from server to client, is

encrypted using the public key from the client's certificate. The encrypted DHCPv6 message is encapsulated into the Encrypted-Message option. The Encrypted-Response message contains the Encrypted-Message option.

6. New DHCPv6 Messages

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

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    msg-type   |               transaction-id                  |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
.                            options                            .
.                           (variable)                          .
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

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.

7. New DHCPv6 Options

The Encrypted-Message option are defined, which carries the DHCPv6 message that is encrypted with the recipient's public key.

The format of the DHCPv4 Message option is:

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |          option-code          |           option-len          |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                                                               |
    .                  encrypted DHCPv6 message                     .
    .                                                               .
    .                                                               .
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2: Encrypted-Message Option Format

option-code OPTION_Encrypted_MSG (TBA3).

option-len Length of the encrypted DHCPv6 message.

encrypted DHCPv6 message The encrypted DHCPv6 message sent by the client or the server. In a Encrypted-Query message, it contains encrypted DHCPv6 message sent by a client. An Encrypted-response message contains encrypted DHCPv6 message sent by a server in response to a client.

8. Security Considerations

TBD

9. IANA Considerations

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

The two messages are:

- o Encrypted-Query message (TBA1).
- o Encrypted-Response message (TBA2).

The one option is:

- o Encrypted-Message option (TBA3).

10. Contributors

The authors would like to thank Bernie Volz, Ralph Droms, Yiu Lee, Tomek Mrugalski, Fred Baker, Qi Sun, Zilong Liu, Cong Liu.

11. References

11.1. Normative References

[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.

[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>.

11.2. 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-02 (work in progress), August 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.

[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