DHC Working Group
Internet-Draft
Intended status: Informational
Expires: April 21, 2016

L. Li
Y. Cui
J. Wu
Tsinghua University

October 19, 2015

# Opportunistic Security for DHCPv6
# draft-li-dhc-secure-dhcpv6-deployment-01

## Abstract

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6) enables DHCPv6 servers to configure network parameters. To secure DHCPv6, the authentication and encryption mechanisms are proposed to protect the DHCPv6 privacy information. However, how to deploy the secure DHCPv6 mechanisms for DHCPv6 is not specified. This draft analyses the DHCPv6 threat model and recommend the opportunistic security mechanism for DHCPv6 deployment.

## 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 21, 2016.

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 in DHCPv6 are vulnerable to several types of attacks, such as pervasive monitoring and spoofing attack. Currently, there have been some proposed mechanisms to secure DHCPv6. Secure DHCPv6 [I-D.ietf-dhc-sedhcpv6] provides the authentication mechanism between DHCPv6 client and server along with the DHCPv6 transaction. [I-D.cui-dhc-dhcpv6-encryption] proposes the DHCPv6 encryption mechanism between the DHCPv6 client and server. However, how to deploy the proposed secure DHCPv6 mechanisms is still not specified.

This document analyses the DHCPv6 threat model and recommends the opportunistic security mechanism for secure DHCPv6 mechanisms deployment to support the incremental deployment. For the DHCPv6 authentication deployment, we analysis two deployment schemes: TOFU and PKI, which are suitable for different DHCPv6 security requirements.

## 2. DHCPv6 threat model

Most of the privacy considerations for DHCPv6 focus on the client privacy protection. As the public service infrastructure, the privacy protection of DHCPv6 server and relay agent is less important. DHCPv6 privacy consideration [I-D.ietf-dhc-dhcpv6-privacy] analyses the privacy problem for DHCPv6

client, listing the various DHCPv6 options containing the privacy information and the possible attack to the DHCPv6 client. The attack specific to a DHCPv6 client is the possibility of the "rogue" server, which may provide the incorrect information to the client. In addition, the client is also faced up with the pervasive monitoring attack. Pervasive monitoring may gleans the privacy information about the IPv6 host, which is used to find location information, previously visited networks and so on. [RFC7258] claims that pervasive monitoring should be mitigated in the design of IETF protocols, where possible.

The attack specific to a DHCPv6 server is the possibility of the invalid client masquerading as a valid client, which may cause the consuming to address resources configured on a DHCPv6 server.

## 3. Secure DHCPv6 mechanisms deployment

### 3.1. Secure DHCPv6 Mechanism Deployment Difficulties

Because of the DHCPv6 property, secure DHCPv6 mechanisms deployment has some specific difficulties. For the secure DHCPv6 mechanisms deployment, the DHCPv6 server is always assumed to have connectivity to authorized CA and verifies the client's certificate. The difficulty for the deployment is that the client is difficult to verify the server's identity without access to network. When the client is pre-configured with the server authentication information, such as one or multiple CA certificates that form the certification path, the server's identity is verified through the pre-configured server authentication information. When the client is not pre-configured with the server authentication information, the client has no capability to verify the server's identity. In the scenario where the DHCPv6 client is mobile and connects to random networks, the client cannot always get pre-configured with the authentication information.

### 3.2. Opportunistic security for DHCP

There have been some proposed secure DHCPv6 mechanisms. Secure DHCPv6 [I-D.ietf-dhc-sedhcpv6] provides the authentication mechanism between DHCPv6 client and server along with the DHCPv6 transaction. [I-D.cui-dhc-dhcpv6-encryption] proposes the DHCPv6 encryption mechanism between the DHCPv6 client and server. The use of secure DHCPv6 protects DHCPv6 from active attack, such as spoofing attack. The use of DHCPv6 encryption defends DHCPv6 against pervasive monitoring and other passive attacks.

In order to achieve the maximum protection that is available, we recommend the opportunistic security for DHCPv6. Opportunistic

security for DHCPv6 use encryption even when authentication is not available. Based on the DHCPv6 security requirement and the client capability, the incremental deployment is supported. When the client is pre-configured the server configuration information, it has the capability to authenticate the server. When the client has capability to authenticate the server, the client is secure enabled. The communication is authenticated and encrypted, which protects the DHCPv6 transaction from passive and active attacks. When the client has no capability to authenticate the server, but is informed of the server's public key, the client is encrypted enabled. The communication is then not authenticated but encrypted, which protects the DHCPv6 transaction from passive attacks, such as pervasive monitoring attack. If the client has no capability to authenticate the server and does not know the server's public key, clear text is used as the baseline communication security policy.

In the scenario where the tight security policy is required, such as the enterprise networks, the authentication and encryption are both required. Opportunistic security can coexist with the explicit and never preempt the explicit security policies. For example, the enterprise's explicit policy is that authenticated and encrypted communication is required, which covers the default opportunistic security policy.

In the scenario where the security policy is loss, the DHCPv6 server is not pre-configured with the authentication information, such as the trusted CA certificates. So the server authentication is optional in order to not impede the following DHCPv6 communication. After the public keys exchange, the non-authenticated encryption communication is applied to avoid the passive attack. In this way, the DHCPv6 message content is protected from the pervasive monitoring.

### 3.3. DHCPv6 authentication deployment

According to the different DHCPv6 security requirement and client pre-configured information, different schemes for DHCPv6 authentication deployment is used. we analysis two deployment schemes: TOFU and PKI, which are suitable for different DHCPv6 security requirements.

#### 3.3.1. TOFU for DHCPv6 authentication deployment

TOFU plays a role in the scenario where the DHCPv6 client is mobile and connects to random networks. In such scenario, the secure policy is loss and the DHCPv6 client is not previously establish the trusted relationship between the DHCPv6 server and client. The TOFU model assumes that an authenticated public key obtained on first contact is

good enough to secure future communication. In addition, for the subsequent connections, if the received public key conflicts to the cached key, the user may change the current cached kay without any validation.

TOFU-based authentication has a clear improvement over completely insecure protocols, and it is also low-cost and simple to deploy. However, TOFU-based authentication make it difficult to distinguish rouge DHCPv6 servers by accepting any key on the initial connection. And it also has no protection against MitM (Man in the Middle) attacks without the validation of the conflicted public key.

### 3.3.2. PKI for DHCPv6 authentication deployment

In the scenario where the tight security policy is required and the client are stable terminal devices, the PKI model plays a role to verify the certificate and perform the authentication. The client validates the server's certificate locally according to the rule defined in [RFC5280] through the pre-configured information. The client is pre-configured with the trusted relationship between the DHCPv6 client and server, or one or multiple CA certificates, which form the certificate path.

The PKI model achieves the authentication of the certificate all the time, which improves the security performance. However, without the pre-configured information, the DHCPv6 communication will fail. And it also brings the deployment difficulties.

## 4. Security Considerations

TBD

## 5. References

### 5.1. Normative References

[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>.

[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>.

## 5.2. Informative References

[I-D.cui-dhc-dhcpv6-encryption]
Cui, Y., Li, L., Wu, J., and Y. Lee, "Encryption Mechanism for DHCPv6", draft-cui-dhc-dhcpv6-encryption-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

Lishan Li
Tsinghua University
Beijing  100084
P.R.China

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

Yong Cui
Tsinghua University
Beijing  100084
P.R.China

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

Jianping Wu
Tsinghua University
Beijing  100084
P.R.China

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