DHC Working Group
Internet-Draft
Intended status: Informational
Expires: April 11, 2016

L. Li
Y. Cui
J. Wu
Tsinghua University
October 9, 2015

Opportunistic Security for DHCPv6
draft-li-dhc-secure-dhcpv6-deployment-00

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 analysis the DHCPv6 threat model and various key management schemes for DHCPv6 deployment, and recommend the opportunistic security for DHCPv6 deployment.

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 mechanism 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 such as the key management is still not specified.

This document analyses the DHCPv6 threat model and the two secure DHCPv6 mechanisms deployment schemes: TOFU and PKI, which are suitable for different DHCPv6 security requirement. In order to meet the requirement of the different DHCPv6 security service, we recommend the opportunistic security for DHCPv6 deployment.

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. DHCPv6 threat model

Most of the privacy consideration for DHCPv6 focuses 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, which lists 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 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 the address resources for DHCPv6 server.

4. Secure DHCPv6 mechanisms deployment

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. For the secure DHCPv6 mechanism deployment, the DHCPv6 server is always considered to have connectivity to authorized CA and verify 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. How to deploy secure DHCPv6 mechanisms is based on the DHCPv6 security requirement and the client capability.

TOFU MAY play a role in the scenario where the DHCPv6 client is mobile and connects to random networks such as public coffee shops. In such scenario, the secure policy is loss and the DHCPv6 client MAY 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 is conflicts with 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 attacks without the validation of the conflicted public key.

In the scenario where the tight security policy is required and the client are stable terminal devices, the PKI model MAY play 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 preconfigured information. The client is preconfigured the trusted relationship between the DHCPv6 client and server, or one or multiple CA certificates, which form the certificate path. The PKI model achieve the authentication of the certificate all the time, which improve the security performance. However, without the preconfigured information, the DHCPv6 communication will fail. And it also brings the deployment difficulties.

5. Opportunistic security for DHCP

TOFU and PKI model are all comprehensive security protection against both passive and active attacks. If the authentication fails, the DHCPv6 transaction is clear text without any protection. For DHCPv6 service, the client is always cannot authenticate the server without access to network. So we propose the opportunistic security [RFC7435] for DHCPv6, which aims to achieve the maximum protection that is available.

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 authentication information, such as one or multiple CA certificate which forms the certification path. Through the pre-configured CA certificate, the server's identity is verified according to the rule defined in [RFC5280]. When the client is not pre-configured the server authentication information, the client has no capability to verify the server's identity. If the server is authenticated and the public keys are exchanged, the communication is authenticated and encrypted, which protects the DHCPv6 transaction from passive and active attacks. If the server is not authenticated and the public keys are exchanged, the communication is not authenticated but encrypted, which protects the DHCPv6 transaction from passive attacks, such as pervasive monitoring attack. And encryption without authentication is better than clear text. If the server is not authenticated and the public keys are also not exchanged, 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 always 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 MAY NOT be preconfigured the authentication information, such as the trusted relationship between the server and client, or the trusted CA certificates. It is difficult for the client to verify the server's certificate without access to the network. 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.

6. Security Considerations

TBD

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>.

[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>.

7.2. Informative References

[I-D.cui-dhc-dhcpv6-encryption]
Cui, Y., Li, L., Wu, J., and Y. Lee, "Authentication and Encryption Mechanism for DHCPv6", draft-cui-dhc-dhcpv6-encryption-03 (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.

[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