DHC Working Group
Internet-Draft
Intended status: Informational
Expires: September 7, 2016

L. Li
Y. Cui
J. Wu
Tsinghua University
S. Jiang
Huawei Technologies Co., Ltd
March 6, 2016

secure DHCPv6 deployment
draft-li-dhc-secure-dhcpv6-deployment-03

Abstract

Secure DHCPv6 provides authentication and encryption mechanisms for DHCPv6. This draft analyses DHCPv6 threat model and provides guideline for secure 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 September 7, 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. Secure DHCPv6 [I-D.ietf-dhc-sedhcpv6] provides authentication and encryption mechanisms for DHCPv6.

This document analyses DHCPv6 threat model and provides some guideline for secure DHCPv6 deployment. For secure DHCPv6 deployment, we mainly consider two different scenarios: roaming client with loose security policy and static client with strict security policy.

2. DHCPv6 Threat Model

DHCPv6 privacy consideration [I-D.ietf-dhc-dhcpv6-privacy] analyses the privacy problem for DHCPv6, listing the various DHCPv6 options containing the privacy information and the possible attacks to DHCPv6.

Most of the privacy considerations for DHCPv6 focus on the client privacy protection. As the public service infrastructures, the privacy protection of the DHCPv6 server and relay agent is less important.

The attack specific to a DHCPv6 client is the possibility of the injection attack, MitM attack, spoofing attack. Because of the above attacks, the client may be configured with the incorrect configuration information, such as invalid IPv6 address. In

addition, the client is also faced up with passive attacks, such as pervasive monitoring. Pervasive monitoring may glean the privacy information of 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.

For the static clients, such as the devices in enterprise network, they are always assumed to connect to exactly one network. The static client can be easily pre-configured with the certificates of the local DHCPv6 servers. According to the pre-configured information, the static client can detect the spoofing attack. The typical attack is MitM attack. An intruder connects to the network and uses DHCP spoofing to install itself as a MitM. Because of the MitM attack, the client's privacy information may be modified or gleaned by the MitM. For the roaming clients, the typical attack is spoofing attack. Because of the rogue server which masquerades as valid server, the client is configured with the incorrect configuration information.

The attack specific to a DHCPv6 server is the possibility of "denial of service" (Dos) attack. Invalid clients may masquerade as valid clients to request IPv6 addresses continually. The attack may cause the exhaustion of valid IPv6 addresses, CPU and network bandwidth. In addition, it also causes problem for the maintenance and management of the large tables on the DHCPv6 servers.

3. Secure DHCPv6 Mechanism Deployment

3.1. Secure DHCPv6 Overview

Secure DHCPv6 [I-D.ietf-dhc-sedhcpv6] provides the authentication and encryption mechanisms for DHCPv6. The Information-request and Reply messages are exchanged to achieve DHCPv6 server authentication. Then the DHCPv6 client authentication is achieved through the first encrypted DHCPv6 message sent from the client to the server, which contains the client's certificate information. Once the mutual authentication, the subsequent DHCPv6 messages are all encrypted with the recipient's public key.

DHCPv6 server authentication protects the DHCPv6 client from injection attack, spoofing attack, and MitM attack. DHCPv6 client authentication protects the DHCPv6 server from Dos attack. DHCPv6 encryption protects DHCPv6 from passive attack, such as pervasive monitoring.

3.2. Secure DHCPv6 Deployment Difficulties

Because of DHCPv6's specific property, the deployment of Secure DHCPv6 mechanism is faced with some specific difficulties. The DHCPv6 server is always assumed to be pre-configured with the trusted clients' certificates or the trusted CAs' certificates to verify the clients' identity. The difficulty of Secure DHCPv6 deployment is that it is hard for the client to verify the server's identity without access to the network. According to the client's capability and security requirement, different schemes for secure DHCPv6 deployment are applied.

3.3. Roaming Client with Loose Security Policy

In the scenario where the DHCPv6 clients are roaming and have loose security requirement, opportunistic security plays a role. Opportunistic security provides DHCPv6 encryption even when the mutual authentication is not available. Based on the roaming client's capability, the DHCPv6 configuration process is either authenticated and encrypted, or non-authenticated and encrypted.

If the client is pre-configured with the trusted servers' certificates or the trusted CAs' certificates, it has the capability to achieve server authentication. If the client is pre-configured with its own CA-signed certificate, it sends the CA-signed certificate to the DHCPv6 server for client authentication. When the client has been pre-configured with these certificate information, the DHCPv6 configuration process is authenticated and encrypted, which protects the DHCPv6 transaction from passive and active attacks.

If the client is not pre-configured with these certificate information, the communication is non-authenticated and encrypted. Non-authenticated and encrypted communication is better than cleartext, which defends against pervasive monitoring and other passive attacks. Although the client is not capable of verifying the server's identity, the client can obtain the server's public key through the server's certificate. For the client authentication, the client can send the self-signed certificate to the server if the client is not configured with the CA-signed certificate. For the DHCPv6 encryption, after the mutual public key communication process, the DHCPv6 message is encrypted with the recipient's public key.

3.4. Static Client with Strict Security Policy

In the scenario where the DHCPv6 clients are static and have strict security requirement, the PKI plays a role. Then the default security policy is that DHCPv6 configuration communication must be

authenticated and encrypted. The static clients, such as the desktop in enterprise network, are pre-configured with the trusted servers' certificates or the trusted CAs' certificates which form the certificate path. Through the pre-configured information, the client has the capability to achieve server authentication locally according to the rule defined in [RFC5280]. For client authentication, the client sends the CA-signed certificate to the server for client authentication. For DHCPv6 encryption, the DHCPv6 message is encrypted with the recipient's public key contained in the certificate.

In some scenarios, the roaming client may also have strict security requirement, such as the byod in enterprise network. Because of the strict security policy, the DHCPv6 configuration process is authenticated and encrypted. Although the roaming client is not pre-configured with the certificates information, the trusted server's certificate and its own certificate can be obtained out of band, such as by scanning a QR code. Through the obtained certificate information, the DHCPv6 client and the DHCPv6 server can achieve the mutual authentication. And then the subsequent DHCPv6 messages are encrypted with the recipient's public key.

4. Security Considerations

Opportunistic encryption is used for secure DHCPv6 deployment in the scenario where the security policy is loose. Downgrade attacks cannot be avoided if nodes can accept the un-authenticated and encrypted DHCPv6 configuration.

5. References

5.1. Normative References

[I-D.ietf-dhc-sedhcpv6]
Jiang, S., Li, L., Cui, Y., Jinmei, T., Lemon, T., and D. Zhang, "Secure DHCPv6", draft-ietf-dhc-sedhcpv6-10 (work in progress), December 2015.

[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.ietf-dhc-dhcpv6-privacy] Krishnan, S., Mrugalski, T., and S. Jiang, "Privacy considerations for DHCPv6", draft-ietf-dhc-dhcpv6-privacy-05 (work in progress), February 2016.

[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: lilishan48@gmail.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

Sheng Jiang
Huawei Technologies Co., Ltd
Q14, Huawei Campus, No.156 Beiqing Road
Hai-Dian District, Beijing, 100095
CN

Email: jiangsheng@huawei.com