

Secure DHCPv6 with Public Key

draft-jiang-dhc-sedhcpv6-02
Replacement of draft-ietf-dhc-secure-dhcpv6

IETF 88 DHC WG

November 5th, 2013

Sheng JIANG (Speaker)

Sean SHEN

Background

- **It is actually the replacement of draft-ietf-dhc-secure-dhcpv6**
 - draft-ietf-dhc-secure-dhcpv6 “Secure DHCPv6 Using CGA” reached IESG and dead because of consideration regarding to CGA
 - The use of CGAs in this situation (1) isn't really how they were intended to be used and (2) probably doesn't add any value over a regular public key signature
- **A suggestion from IESG is to make another public key based security solution, while DHCPv6 needs another security mechanism beyond symmetric key pair**
- **The new draft-jiang-dhc-sedhcpv6**
 - dropped CGA relevant mechanism, making it general public key based
 - added PKI/Certificate as an alternative of pre-config, while keeping "a leap of faith" model possible
 - completed timestamp check mechanism

Secure DHCPv6 Overview

- **A Sender MUST have a public/private key pair in order to create Secure DHCPv6 messages**
 - The authority of the sender may depend on pre-configuration mechanism or PKI, or a leap of faith model
 - By combining with the signatures, sender identity can be verified and messages protected
- **This document introduce a public key, a certificate and a signature options with a corresponding verification mechanism**
 - Timestamp is integrated into signature options
 - Support for algorithm agility by notification model

Process Rules on Recipient

- **Secure DHCPv6 Message Validation**

- discard the message if the Signature option is absent, or both the Public Key and Certificate option is absent, or both are presented
- except for Relay-forward and Relay-reply Messages

- **Check the authority of sender first, by**

- finding a match public key from the local trust public key list, which is pre-configured or recorded from previous communications
- or validating the sender's certificate following the rules defined in [RFC5280]
- or the receiver MAY choose to further process the message from an unauthorized sender so that a leap of faith may be built up

- **Verify the Signature and check timestamp**

- for authentication, message integrity and anti-replay

Processing Rules of Relay Agent

- **There is nothing more the relay agents have to do to support Secure DHCPv6 beyond RFC3315**
 - According to review comments, verifying the bypass messages client-to-server or server-to-client, or protection between relay agent and server are removed in 02 version
- **By current definition in this document, relay agents MUST NOT add any secure DHCPv6 options**

Comments are welcomed!

In WG Adoption Call

(Oct. 17 ~ Nov. 11)

Thank You!