Secure DHCPv6

draft-ietf-dhc-sedhcpv6-13

Presenter: Ted Lemon
Secure DHCPv6 Overview

Client verifies server’s identity

After server authentication, first message sent from client (such as Solicit) contains client’s certificate information

DHCPv6 Client

Information-request

Reply

Certificate option
Signature option
Increasing-number option
Server Identifier option

Encryption-Query

Encrypted-message option
Server Identifier option

Encryption-Response

Encrypted-message option

Server Authentication

Encrypted DHCPv6 Configuration

...
Comments from Stephen Farrell

• It is something where we should be able to make progress and this is getting there
• Why TOFU is out of scope and whether requiring certificate is a good idea?
  – Add opportunistic security for deployment
  – Provide encryption in all case
  – Provide authentication based either on pre-sharing of authorized certificates, or else using trust-on-first-use
Comments from Stephen Farrell

• The client authentication is optional
  – For cases like hotspot or home network, no need for client authentication
  – For cases like data center, client authentication needed

• Add scenario where hash and signature algorithms cannot be separated
Comment from Stephen Farrell

• Add the comparison with related works
  – RFC7824 (Privacy consideration for DHCPv6)
  – RFC7844 (Anonymity Profiles for DHCP clients)

• supply the encryption text format
  – Add reference of RFC5652 (cryptographic message syntax)
Additional Revision

• Change Timestamp option into Increasing-number option for replay attack detection
  – Increasing-number is easy to check compared with Timestamp
  – Client and Server have one stable stored number for increasing-number check
  – Timestamp is one of the possible implementation choice
Additional Revision

• Add the consideration where multiple DHCPv6 servers share one common cert
  – Caused change: Encrypted-Query message contains Server Identifier option when if it is in the original message to avoid the extra decryption for servers not for it
  – Compatible with server selection method in RFC3315 by sharing one common cert
Additional Revision

• Add the statement that Encrypted-Query and Encrypted-Response messages can only contain certain options: Server Identifier option and Encrypted-message option

• Add the relay agent cache function for the quick response when there is no authenticated server
Additional Revision

- The Reply message with error status code may contain client identifier option, then the client's privacy information may be disclosed
  - Possible solution: encrypt the Reply message
  - Encrypt the Reply message with the mandatory algorithm If the error is AlgorithmNotSupportedException
Next Step

• Next Step?
• Thanks!