Secure DHCPv6

draft-ietf-dhc-sedhcpv6-09

Ted Lemon, Randy Bush
Sheng Jiang, Sean Shen, Dacheng Zhang, Tatuya Jinmei
Lishan Li, Yong Cui, Yiu Lee, Jianping Wu
Bernie Volz, Tomek Mrugalski
Motivation

• Current secure DHCPv6 drafts
  • Secure DHCPv6: DHCPv6 authentication of server and client
  • DHCPv6 Encryption: DHCPv6 encryption between client and server
    • Protect DHCPv6 from passive attack, such as pervasive monitoring attack
    • IETF has expressed that PM attack should be mitigated where possible

• If two drafts: Vendors may implement authentication but ignore encryption

• The document merges the two drafts and achieves the DHCPv6 authentication and encryption
Opportunistic Security for DHCPv6

• Opportunistic security for DHCPv6
  • Provide privacy protection as much as possible
  • Encryption even when the authentication is not available

• Default OS policy
  • Authentication available
    • Authenticated and encrypted communication
  • Authentication not available but public keys exchange
    • Non-authenticated and encrypted communication
Opportunistic Security for DHCPv6

- Scenario: strict security policy
  - Scenario: enterprise network where security policy is strict
  - Local explicit security policy: authentication and encryption all needed
  - Local explicit security policy supersedes the default OS policy
  - DHCPv6 configuration process must be authenticated and encrypted
Secure DHCPv6 Overview

Client verify identity of server if pre-configured the trusted CA certs or server’s certs
Client is informed of the server’s public key in cert if no capability to verify server’s identity
Client encrypts message with server’s public key
Solicit message contains client’s cert

DHCPv6 Client

Information-request
Reply
certificate option
timestamp option
signature option
server identifier option

DHCPv6 Server

Encrypted-Query
encrypted-message option (Solicit)
server identifier option

Encryption-Response
encrypted-message option (Advertise)

Server authentication/public key communication

Encrypted DHCPv6 configuration
Format of Encrypted Message

<table>
<thead>
<tr>
<th>message-type</th>
<th>transaction-id</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>encrypted-message option</td>
</tr>
<tr>
<td></td>
<td>encrypted message</td>
</tr>
<tr>
<td></td>
<td>encapsulated in encrypted-message option</td>
</tr>
<tr>
<td></td>
<td>encrypted with recipient’s public key</td>
</tr>
<tr>
<td></td>
<td>DHCPv6 message</td>
</tr>
</tbody>
</table>
New Defined Options and Messages

• Five new DHCPv6 options
  • certificate option: sender’s certificate
  • public key option: sender’s public key
  • signature option: signature signed by the private key
  • timestamp option: sender’s current time
  • encrypted-message option: encrypted DHCPv6 message

• Two new DHCPv6 messages
  • Encrypted-Query message: from client to server
    • encrypted-message option
  • Encrypted-Response message: from server to client
    • encrypted-message option, server identifier option
Companion document

• Secure DHCPv6 deployment
  • Threat Model
  • Deployment Consideration
Next Step

• Any Comments?
• Thanks!