Secure DHCPv6 Deployment

draft-li-dhc-secure-dhcpv6-deployment-01

Presenter: Lishan Li
Motivation

• Secure DHCPv6 has provided the authentication and encryption mechanism for DHCPv6
• How to deploy secure DHCPv6 in real scenarios?
• The document analysis the DHCPv6 threat model and provides the guideline for secure DHCPv6 deployment
DHCPv6 Threat Model

• DHCPv6 client
  • Attack: Injection attack, spoofing attack, rogue server
  • Result: Client may be configured with the incorrect information, such as unavailable address

• DHCPv6 message content:
  • Attack: Pervasive monitoring attack, MitM attack
  • Result: Glean the privacy information to find location information and so on

• DHCPv6 server:
  • Attack: Dos Attack
  • Result: Maintenance and management for the large tables in DHCPv6 server
Secure DHCPv6 deployment

- Scenario: enterprise network, clients are stable terminals
- Security requirement: authentication and encryption all;
- Deployment:
  - Local strict security policy: must authentication and encryption;
  - Server authentication:
    - Client pre-configured the trusted server’s cert, or the trusted CA certificates;
    - Capability to verify server’s identity;
  - Client authentication:
    - Client is pre-configured its certificate, which is sent to server for authentication;
  - DHCPv6 Encryption
    - Encrypted with the public key contained in the cert;
Secure DHCPv6 deployment

• Scenario: public coffee shop, clients are mobile terminals
• Deployment:
  • Server authentication:
    • Client is not pre-configured the trusted server’s certificate, or the trusted CA certificates;
    • No capability to verify the server’s identity, but is informed of server’s public key;
  • Client authentication:
    • Client sends its public key to server;
  • DHCPv6 encryption:
    • If public keys are exchanged, then non-authenticated but encrypted communication;
Next Step

- Advanced?
- Thanks!