Secure DHCPv6 Deployment

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

Presenter: Ted Lemon

Motivation

- Secure DHCPv6
  - Aim at scenario where clients and servers are pre-configured with trusted certificates info, such as enterprise network
  - However, more widely applicable with integration of generic PKI is subject to future study and out of scope
- The document analyzes DHCPv6 threat model and provides guideline for secure DHCPv6 deployment

DHCPv6 Threat Model

- DHCPv6 client
  - Attack
    - MitM attack, spoofing attack, pervasive monitoring attack
    - Difference between static client and roaming client
      - Compared with roaming client, static client is easy to detect spoofing attack according to local trusted certificates info
  - Result
    - Client may be configured with incorrect parameters
    - Client's privacy information may be gleaned, which is used to find location information, previously visited networks…

DHCPv6 Threat Model

- DHCPv6 server
  - Attack: Dos attack
  - Result
    - Exhaustion of valid IPv6 addresses, CPU and network bandwidth
    - Maintenance and management of the large tables on the DHCPv6 servers

Secure DHCPv6 Deployment

- Roaming client with Loose security policy
  - Opportunistic security plays a role
  - Example: laptop in coffee room
  - Accept non-authenticated and encrypted communication
- Static client with strict security policy
  - PKI plays a role
  - Example: desktop in enterprise network
  - Authenticated and encrypted communication

Update after IETF94

- Change scenario classification method
  - Enterprise network with strict security policy → Static client with strict security policy
  - Coffee room with loose security policy → Roaming client with loose security policy
- Add difference between static client and roaming client in threat model
- Add security consideration
  - Downgrade attacks cannot be avoided if non-authenticated and encrypted DHCPv6 configuration can be accepted

Next Step

- Move forward?
- Thanks!