Update of Secure DHCPv6

draft-ietf-dhc-sedhcpv6

IETF 93 DHC WG

July, 2015

Dacheng Zhang(Speaker)

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**
  - 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 Update

- **“Secure DHCPv6” is requested for publication recently**
  - 07 & 08 version is mainly for AD review by Ted Lemon
  - 08 (June): clarified what the client and the server should do if it receives a message using unsupported algorithm; refined the error code treatment regarding to AuthenticationFail and TimestampFail; added consideration on how to reduce the DoS attack when using TOFU;
  - 07 (March): removed the deployment consideration section; instead, described more straightforward use cases with TOFU in the overview section, and clarified how the public keys would be stored at the recipient when TOFU is used. The overview section also clarified the integration of PKI or other similar infrastructure is an open issue.
- **There are some latest review comments on Secure DHCPv6, from AD review and Security review**

- **Timestamp format – does not match the NTP document in terms of time formats**
  - Adopt SeND format
- **Security Terms**
  - "public key signatures" ->"digital signatures“
  - “Certificate Authority” -> “Certification Authority”
- **Server replies should be in the same algorithms that client use**
- **A few clarifications and normative language consistent corrections**
- **The encoding allows only a single certificate.**
  - OK, will discuss with DHC.

- **The long message will cause fragmentation, difficult for a server to protect itself from state exhaustion denial of service attacks while accepting fragmented datagrams**
  - It is a open issue. General to all the scenarios where fragmentation exists
- **Have a single algorithm identifier that specifies both the hash and the public key signature algorithm rather than separate identifiers for the two**
  - OK, will discuss with DHC.
- **Challenges in the usage of timestamp**
- **New round of discussion in the limitation of PKI / leap of faith**
  - Client could validate certificate only under restricted condition

Thank You!