Update of Secure DHCPv6 & Secure DHCPv4

draft-ietf-dhc-sedhcpv6
draft-jiang-dhc-sedhcpv4

IETF 93 DHC WG

July, 2015

Sheng JIANG (Speaker)

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**

New comments

- **From Brian Haberman (AD review), Hackathon, Russ Housley & Charlie Kaufman**
- **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**
- **The encoding allows only a single certificate.**
  - Need opinion from DHC
- **A few clarifications and normative language consistent corrections**

New comments (cont.)

- **The long message will cause fragmentation, difficult for a server to protect itself from state exhaustion denial of service attacks while accepting fragmented datagrams**
  - General issue for UDP fragmentation, not Secure DHCPv6 specific
  - Will add new text in security consideration session to mention it
- **Have a single algorithm identifier that specifies both the hash and the public key signature algorithm rather than separate identifiers for the two**
  - Need opinion from 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

Update on Secure DHCPv4 01 Version

- **Removed the special design of 8-bit type + 16-bit length**
  - Applied multiple instances of the same option are generated according to [RFC3396], when the option exceeds 255 octets in size (the maximum size of a single option)
- **Latest modifications on Secure DHCPv6 have also applied to Secure DHCPv4 (01 version)**
  - The authors plan to apply any correspondent modifications on Secure DHCPv4 in the future, too

Comments are welcomed!

WG Adoption for Secure DHCPv4?

Thank You!