Secure DHCPv6 Using CGA

draft-ietf-dhc-secure-dhcpv6-032

IETF 81 DHC WG

July 29, 2011

Sheng JIANG (Speaker, Huawei)
Gang CHEN (China Mobile)

- **Adopted as DHC WG document March 2010**
  - Has updated 3 times with minor modifications.
- **Recent added some more security Considerations**
  - Without other pre-configured security mechanism, like pre-notified DHCPv6 server address, using host-based CGA by DHCPv6 servers could not prevent attacks claiming to be a DHCPv6 server.
    - **CGAs of DHCPv6 servers may be pre-notified to hosts**
  - Link-local CGAs are more vulnerable because the same prefix is used by all IPv6 nodes. Therefore, when link-local CGAs are used by the DHCPv6 clients, it is recommended to use a slightly higher Sec value

New Secure Consideration (cont.)

- Impacts of collision attacks on current uses of CGAs are analyzed in [RFC4982]. CGAs do not provide non-repudiation features. Therefore, as [RFC4982] points out CGA-based protocols, including Secure DHCPv6 defined in this document, are not affected by collision attacks on hash functions.
- [RFC6273] has analyzed possible threats to the hash algorithms used in SEND. Since the Secure DHCPv6 defined in this document uses the same hash algorithms in similar way like SEND (except that Secure DHCPv6 has not used PKIX Certificate), analysis results could be applied as well:
  - Current attacks on hash functions do not constitute any practical threat to the digital signatures used in the RSA signature in Secure DHCPv6.
  - Attacks on CGAs, as described in [RFC4982], will compromise the security of Secure DHCPv6 and they need to be addressed by encoding the hash algorithm information into the CGA as specified in [RFC4982].

Comments are welcomed!

Ready for WGLC!

Thank You!