Secure DHCPv6 with Public Key

Replacement of draft-ietf-dhc-secure-dhcpv6

IETF 89 DHC WG

March 3rd, 2014

Sheng JIANG (Speaker)
Sean SHEN
Dacheng ZHANG (new co-author)

Background

- **“Secure DHCPv6 with Public Key” replaced draft-ietf-dhc-secure-dhcpv6**
  - dropped CGA relevant mechanism, making it general public key based
  - added PKI as an alternative of pre-config, while keeping "a leap of faith" model possible
  - completed timestamp check mechanism
- **Inherited the maturity from old document**
  - Adopted in IETF88
  - Almost ready for WGLC
  - A few detailed technical issues raised in IETF88 and reviewings

The operations of dealing with non-supported algorithms

- **The operations of dealing with non-supported Signature algorithms is as follows:**
  - If the recipient does not support the algorithm used by the sender, it cannot authenticate the message.
  - In this case, the receiver SHOULD reply with a NotSupportAlgorithm status code (TBD4: New status code: indicates the recipient does not support algorithms that sender used)
  - Upon receiving this status code, the sender MAY resend the message protected with the mandatory algorithms
- **Mandatory Algorithms (so any hosts can communicate)**
  - The mandatory algorithm is RSASSA-PKCS1-v1_5
  - The mandatory algorithm is SHA-256

Protections against Resource Exhaustion Attacks

- **The number of cached public keys or unverifiable certificates MUST be limited in order to protect the DHCPv6 server against resource exhaustion attacks.**
- **If the recipient's list that stores public keys or unverifiable certificates in the leap of faith model exceeds, an error FaithListExceed status code** (TBD6: New status code: indicates the recipient‘s list that stores public keys or unverifiable certificates in the leap of faith model currently exceeds) **SHOULD be returned to the sender.**
- **The resource releasing policy against exceeding situations is out of scope.**

Updates in the Operations of Processing Incoming Packets

- **The recipient SHOULD first check the support of algorithms that sender used. If not, an error NotSupportAlgorithm status code** (TBD5: New status code: indicates the recipient does not support the leap of faith model) **should be sent back to the sender, while the message is dropped saliently.**
- **If the sender uses certificate, the recipient SHOULD validate the sender's certificate following the rules defined in [RFC5280]. An implementation may create a local trust certificate record for a verified certificate in order to avoid repeated verification procedure in the future.**

Process upon Receiving a Status Code

- Upon receiving a Reply message with a NotSupportAlgorithm status code, the sender MAY resend the message protected with the mandatory algorithms.
- Upon receiving a Reply message with a NotSupportFaithModel or FaithListExceed status code, the sender is not able to build up the connection with the recipient.
- The sender MAY try to use a verifiable certificate. In the latter case, the sender MAY retry later.

Other Updates

- Clarify that how the two communicating nodes can be securely synchronized is out of scope.

Comments are welcomed!

Ready for WGLC!

Thank You!