Clarifications on DHCPv6 Authentication <draft-jinmei-dhc-dhcpv6-clarify-auth-00.txt>

Tatuya Jinmei

Toshiba Corporation/The KAME Project

Background

- Draft contains various issues
  - based on implementation experiences
  - some may require clarifications/changes in the base spec
- Goal of the document
  - provide a base of discussion
  - to be a source of revising the original spec
- In this presentation
  - concentrate on some major issues

Usage for Information-Request

- Contradiction between 3315 and 3736
  - RFC3315: Info-req usage depends on Solicit/Adv. exchanges
  - RFC3376: the stateless subset can use authentication within itself
- Proposal:
  - separate the usage for Info-req from that for "stateful"
    - including key management
  - allow reusing the same key for multiple exchanges
- Discussion:
  - it may be better to keep the server stateless
  - allow the two choices?

Possibility of DoS Attack

- Issue: the current spec can cause a DoS
  - RFC3315: client MUST restart DHCP on failure of validation
  - => attacker can break a session simply by sending a bogus message
- Possible Resolution:
  - do not immediately restart the session
    - wait a while for a valid reply
  - need to be discussed more
    - good idea in the first place?
    - wait period?
    - Info-req case?

Inconsistent Behavior for Unauth Messages

- RFC3315 Section 21.4.2
  - MAC mismatch -> MUST discard the message
- RFC3315 Section 21.4.4.2
  - allow the client to accept Advertise that fails to pass validation
    - even if MAC mismatch -> accept Advertise?
- Discussion:
  - is there a valid reason for the latter?
  - if not, it should make sense to discard such messages in any case

Other Miscellaneous Issues

- Lack of Authentication from Client
  - what the server should do when the client does not include auth info?
  - => need more discussion
    - depending on the previous issue
    - may differ for Info-Req
- Behavior against a replay attack
  - => should discard if replay is detected
- Definition of "Unauthenticated Messages"
  - => undefined term, need a clear definition
- Key Consistency
  - => wording issue

Proposed Next Steps

- Make sure if any of the issues/resolutions are valid
  - comments are appreciated
- Assuming they are,
  - revise it as a wg document
  - target:
    - a separate RFC? (BCP/PS?)
    - wait for revising the base spec and merge into it?