Split Scenario Bootstrapping

MIP6 WG, IETF 69

Vijay Devarapalli (vijay.devarapalli@azairenet.com)
James Kempf (kempf@docomolabs-usa.com)
Gerardo Giaretta (gerardog@qualcomm.com)

Status

- Version 07 just submitted
- Currently with the IESG
- IETF last call and IESG comments addressed
- Substantial number of changes since last IETF meeting in March

Use of Anycast-based HA assignment

- Security review indicated that this changes RFC 4306 recommended behavior
  - The IKE_SA_INIT response comes back from a unicast address when the request was sent to an anycast address
- Security AD wanted to see this standardized separately since it could be applied elsewhere too
- Removed from the document
  - May be standardized separately
- An issue still exists
  - Firewall may block a response coming back from a unicast address
  - But this becomes an issue for any usage of anycast address

Use of PKI

- Security review indicated that the use of PKI and verifying the certificates underspecified
- Some considerations
  - The MN identity in the IDi payload MUST correspond to identity in the certificate obtained by the HA
  - MN identity in IDi payload is used by the HA to lookup the policy and the certificate that corresponds to the mobile node
  - If IDi contains home address, then it MUST match iPAddress field in the SubjectAltName extension in the certificate
- Some of this is already specified in RFC 4877
- Added references to PKI4IPsec (draft-ietf-pki4ipsec-ikecert-profile-12.txt)

Home Agents not responding to IKE_SA_INIT

- MN behavior when HA does not respond to IKE_SA_INIT or if authentication fails
  - MN should try other home agents on the HA list
  - Try again after a period of time if no home agent responds
    - Timer configurable on the mobile node
  - If authentication fails with all home agents, it is an unrecoverable error on the MN

Format of MIP6_HOME_PREFIX attribute

- The format the MIP6_HOME_PREFIX attribute had many mistakes
  - An attribute in the CFG_REQ and CFG_REP payloads
  - Used to deliver MIP6 home prefix information to the MN so that the MN can auto-configure a home address
- Changes
  - Shortened the “Attribute Type” field to 15 bits from 31 bits
  - Shortened the “Prefix Length” field to 8 bits from 16 bits
  - Fixed the “Length” field to say it is not “multi-valued”
    - It can be set to 0 or 21 bits, but this is not “multi-valued” means in RFC 4301.

Home Address Authorization

- RFC 3775 requires that a HA verify that the MN is authorized for a particular home address
- More text has been added on this
- Two Modes
  - Each MN is already allocated a home address. The same address is given out to the NM every time
  - First-come-first-served basis. Home Agent allows a MN to request an address as long as it is not used by another MN.
- Addresses are marked as used for at least as long as the binding cache entry exists for the corresponding home address
- The allocated address is associated with the identity of the MN
- The above allows a home agent to verify the MN if authorized to use a particular home address for most use cases

Minor changes

- Local HA discovery using DNS
  - Removed the example showing how to construct a FQDN that could correspond to a local HA
- Added more text on explicitly authorizing the HA to perform a DNS update from the AAA server if required