MIPv6 with IKEv2 and RFC 4301

MIP6 WG, IETF 67

Vijay Devarapalli (vijay.devarapalli@azairenet.com)

Current Status

- AD review complete
  - Comments addressed in version 07
- IETF last call going on
  - Some comments received

IPsec Selector Granularity

- Current spec allows varying granularity of IPsec selectors
  - MH protocol not implemented in an IPsec implementation
  - MH protocol is implemented
  - MH Type as a selector is implemented
- Suggest to mandate the third option
- Rejected
  - This was discussed extensively on the mailing list earlier; there were objections to mandating MH Type as selector

Dynamic HoA and SPD entries

- When HoA is configured dynamically during IKEv2 message exchange, what does the SPD contain?
- Generic SPD entries exist
  - Prevent BU/BAck without IPsec protection
- SPD entries need to be dynamically created for the new home address

IKEv2 Authentication

- There was a lot of text on the use of shared keys, certificates, etc…
- Suggestion was to remove the text and just point to RFC 4306
  - Description is at a high level now
- Accepted

IDi and use of EAP

- When EAP is used, the IDi field might not represent the actual identity of the mobile node
- Added some text to clarify the use of IDi field with EAP
  - The identity in IDi may be used for AAA routing and for selecting the right EAP method
  - The actual identity is carried in EAP payloads
  - The home agent MUST acquire the “real” identity from the corresponding AAA server
- Accepted

Peer Authorization Database

- What is it used for?
  - To store per-MN state like shared-key, public key or trust anchor to verify MN's certificate
- How is it populated?
  - If HA is assigned dynamically, the PAD needs to be also dynamically populated
  - Proprietary interface?

SPD/SAD Representation

- SPD/SAD representation may not match RFC 4301
- Some help expected from 4301 experts

IETF Last Call comments

- MOBIKE brought up again
  - Discussed many times in the past
  - Consensus was not to use both at the same time
- Proposal is to add text which says the following
  - Both MIPv6 and MOBIKE can manage an IPsec protected tunnel between the mobile node and a gateway
  - Running both at the same time has issues
    - Redundant
    - Conflict in managing the tunnel

HoA in IDi and PKI4IPsec

- A permanent HoA can be used in the IDi field
- PKI4IPsec requires the source address on the IKE message to match the IDi in this case
  - But this may be relaxed
- In MIPv6, the source address on the IKE message is CoA even when the IDi is set to the HoA
- RFC 4306 says ignore the source address on the IKE messages
- Suggestion is to simplify the text to say we just follow RFC 4306

INTERNAL_ADDRESS_EXPIRY Attribute

- The current document talks about using the INTERNAL_ADDRESS_EXPIRY attribute to indicate for how long the MN is allowed use of the allocated HoA
- RFC 4718 (IKEv2 clarifications document) recommends not using this attribute
  - The address lifetime would be the same as the IKE SA lifetime
- Accept?