MIPv6 with IKEv2 and revised IPsec Status Update

Vijay Devarapalli

MIP6 WG, IETF 63

Status

- A few reviews
- Version 02 published with a lot of changes
- Two issues remaining

Changes in version 02

- The draft is now self-contained with respect to the requirements section
- Added some text on what the SPD entries on the HA should contain when the MN's home address is not known yet
- Added some text to say that the MN could use a range of selectors to use the same SA for multiple messages, for e.g., BU and BAck, instead of creating pairs of IPsec SA per mobility message type
- Clarified the use of PKI and verification of identities presented by the mobility node
- Added some text related to the use of 'K' bit and IKEv2
- Clarified the use of EAP_ONLY_AUTHENTICATION payload. Added some text on this in the security considerations section
- Added some text in the security considerations section regarding home address configuration
- You can see the diff at http://people.nokia.net/vijayd/mip6/1to2_diff.html

Major issues – IPsec Selector Granularity

- RFC 3775 and 3776 describes SPD and SAD configurations assuming Mobility Header protocol and ICMP as IPsec selectors
  - Hard to differentiate between BU and HoTi message; so support for per-interface configuration of SPD and SAD entries is required
  - All ICMP messages between MN and HA are protected by IPsec SA created for MPD messages
- In 2401-bis, Mobility Header message type and ICMP message type are selectors
  - Easier SPD and SAD configuration
  - Per-interface configuration of SPD and SAD entries not required
  - MPD messages can be selectively protected

Major issues – IPsec Selector Granularity

- Should we require the MN and the HA to support the new IPsec selectors?
  - Use a 'MUST'?
  - Or just leave it to the implementations?

- Possible solutions
  1. Require the HA to support the new IPsec selectors and make it optional for the MN
  2. Remove 'MUST' for the support of new IPsec selectors
     - If new selectors not supported,
       - Use RFC 3776 like configuration, including per-interface support
       - draft-ietf-mip6-ikev2-ipsec will not describe any example configurations related to this
     - If the selectors are supported,
       - The MN and the HA use the example configurations described in draft-ietf-mip6-ikev2-ipsec

Major Issues – Packet formats

- As specified in RFC 3775 and 3776
  - Mandatory to support
  - Transport mode IPsec protection for BU/BAck and Mobile Prefix Discovery messages
  - Tunnel Mode IPsec protection for HoTi/HoT and payload messages
  - Most implementations support this

- Tunnel mode
  - BU/Back, MPD, RR and payload messages all sent through the tunnel between the MN and the HA
  - Advantages
    - Fewer SPD and SAD entries
    - Useful for location privacy solutions
  - Disadvantages
    - More packet overhead
  - Some implementations support this

Major Issues – Packet formats

- draft-ietf-mip6-ikev2-ipsec currently describes detailed SPD and SAD configurations for the ‘mandatory to support’ mode. Does not describe the SPD and SAD entries for the tunnel mode
  - They are examples anyway
  - Not meant to support all possible IPsec configurations
  - Will bloat the draft

- Francis argues for describing the tunnel mode also

- One could argue this belongs in location privacy solutions to hide the HoA from the visited network