Mobile IPv6 with IKEv2 and 2401bis – Update

Vijay Devarapalli, Francis Dupont

MIP6 WG, IETF 64

IPsec Selector Granularity

- A lot of confusion from RFC 3776 about what kind of IPsec protection to use
  - Implementations MUST support transport mode for BU/BAck and tunnel mode for HoTi/HoT
  - But other formats are not prohibited
    - Some implementations infact use just one IPsec tunnel SA for all signaling messages
  - The SPD/SAD entries in RFC 3776 are just examples

- Some IPsec implementations may not support fine grained selectors such as mobility header message type and ICMPv6 type

- IPsec protection can be provided in different ways while satisfying the security requirements of RFC 3775

IPsec Selector Granularity

- Fine grained selectors are supported
  - Transport mode SA for the BU/BAck and MPD
  - Tunnel mode SA for HoTi
    - No requirement for using interface selector while applying the SA
    - All other tunneled mobility header messages can be sent in clear
  - Examples in draft-ietf-mip6-ikev2-ipsec are explained assuming this

- Only protocol level selectors are supported
  - Only mobility header and ICMPv6 available as selectors
  - Results in protecting all ICMPv6 messages between the MN and the HA
  - Results in protecting all tunneled mobility header messages
  - Requires interface selector for SA lookup to distinguish between BU and HoTi
    - or some implementation hacks
  - RFC 3776 examples assume this

IPsec Selector Granularity

- Protocol selector not available
  - One IPsec tunnel SA setup with protocol selector set to ‘any’
  - All MIPv6 signaling messages will be tunneled
  - BU Format

```
IPv6 hdr (src=CoA, dst=HA)
ESP in tunnel mode
IPv6 hdr (src=HoA, dst=HA)
Mobility Hdr
      Binding Update
           AltCoA option
```

  - Also useful for privacy solutions when you don’t want the access network to see the HoA

Combining SPD Entries

- Earlier we had separate SPD entries for protecting BU and BAck

```
mobile node SPD-S:
     IF destination = home_agent_1 & proto = MH & mh_type = BU
     Then use SA ESP transport mode
          IDi = user_1, IDr = home_agent_1,
          TSi = home_address_1, MH, BU

     IF source = home_agent_1 & proto = MH & mh_type = BAck
     Then use SA ESP transport mode
          IDi = user_1, IDr = home_agent_1,
          TSi = home_address_1, MH, BAck
```

- IKEv2 allows you to negotiate IPsec SAs for a range of selectors
  - This was optional in the previous versions of the draft
  - But now described as the default

Combining SPD Entries

- Include BU and BAck in the range of selectors in IKEv2 negotiation
- This reduces the number of IPsec SA pairs

```
mobile node SPD-S: -
     IF source = home_address_1 & destination = home_agent_1 & proto = MH &
        local_mh_type = BU & remote_mh_type = BAck
     Then use SA ESP transport mode
          IDi = user_1, IDr = home_agent_1,
          TSi = home_address_1, MH, BU
          TSr = home_agent_1, MH, BAck
```

Minor Changes

- Support for Mobility Header message type
  - The requirement changed from ‘MUST’ to ‘SHOULD’
- Home Address as the identity
  - IPsec implementations check if the source address in the IKE exchange is the same as the address in the IDi field if an address is used as an identity
  - In MIPv6, the source address is CoA, while IDi contains the home address
    - The check fails
  - This should be configurable in an implementation and disabled for Mobile IPv6
  - Not an issue when, for e.g. FQDN is used as an identifier
- Other cosmetic changes
  - diffs at http://tools.ietf.org/wg/mip6/draft-ietf-mip6-ikev2-ipsec/