Mobile IPv6 with IKEv2 and 2401bis – Update

MIP6 WG, IETF 65
Vijay Devarapalli, Francis Dupont
Updates

• Minor changes to address Jari Arkko’s comments

• Removed reference to EAP-ONLY-AUTHENTICATION notification payload
  – Should be pursued separately
The K bit

• An issue was raised on whether we still need the ‘K’ bit if MOBIKE is available
  – At least move it to a separate specification

• Discussion on the mailing list
  – If IKE SA is deleted, associated IPsec SAs are also deleted. Therefore updating the IKE SA is very important
  – Does not make sense to use MIPv6 and MOBIKE at the same time
  – If one end is capable of updating the IKE SA and the other is not, ‘K’ bit needed so that both ends either update or don’t
  – K bit much easier to implement with IKEv2 than IKEv1
The K bit

- Consensus to keep the ‘K’ bit as is.
IPsec Selector Granularity

- More text added to clarify this

- Three different ways of using ESP protection
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
IPsec Selector Granularity

• 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)
    MobilityHdr
      Binding Update
      AltCoA option
  – Also useful for privacy solutions when you don’t want the access network to see the HoA