# IPsec and IKEv2 with Multiple Care-of Addresses

Vijay Devarapalli

MONAMI6 WG, IETF 64

# Assumptions in RFC 3775, 3776 and 3963

- There is one primary care-of address per mobile node
- The CoA is stored in the IPsec database for tunnel encapsulation and decapsulation
- CoA is verified when a tunneled packet is received from the mobile node
  - tunneled packet could be HoTi or regular CN traffic protected by IPsec
- IKE is run between the CoA and the home agent's address

# Issues

- Problems arise when the mobile node wants to send/receive IPsec protected tunneled packets from/to multiple CoAs

- The home agent should be able to decapsulate tunneled packets from all care-of addresses used by the mobile node
  - If CoA stored in the IPsec database as tunnel state, do we store all CoAs?
    - Otherwise the tunneled packet might be dropped by IPsec
  - Mandate that check on the outer source address is done only by the home agent
    - IPsec does not check the outer tunnel source address

# Issues

- Do we use multiple tunnel mode IPsec SAs?
  - Tunnel mode IPsec SA
    - HoTi/HoT, Payload
  - One tunnel IPsec SA per CoA?
    - Might be needed if you want to receive IPsec protected traffic at two CoAs simultaneously
- Do we run multiple IKEv2 sessions?
  - One from each CoA?
  - Required if you want a tunnel IPsec SA per CoA

# Solution – Only one CoA is used at any time

- Designate one CoA as primary CoA
- The primary CoA is always used to tunnel IPsec protected packets
  - No other CoA
  - All HoTi messages tunneled using the primary CoA
- When you want to change primary CoA
  - Indicate it in the BU
  - Update the IKE SA endpoint
    - The ‘K’ bit
  - Update the IPsec SA tunnel end point state immediately

# Solution – Multiple CoAs Used Simultaneously

- We should avoid multiple IKEv2 exchanges and multiple sets of IPsec SAs
- This may require tighter coupling between MIPv6 and IPsec
- During tunnel decapsulation the home agent must check the outer source address
  - IPsec skips checking the outer source address
  - Only decapsulates and decrypts the packet
  - This is not be a big deal since 2401bis says IPsec does not check the outer source address
- During forwarding, the home agent lets MIPv6 specify the tunnel end point
  - IPsec tunnel encapsulation should not be used
  - Internal to the home agent
  - However, this may be a significant change for some implementations

# Other Possible Solutions

- Avoid IPsec protection of flows when using multiple CoAs

- Use MOBIKE to add additional CoAs
  - IKEv2 is aware of additional CoAs
  - But MOBIKE has multiple IKEv2 exchanges
  - Allows the use of only one CoA at a time

- Use authentication option protocol instead of IKEv2 ;)
  - Tunnel encapsulation/decapsulation done by MIPv6 all the time
  - Needs extensions to encrypt HoTi and payload traffic