Use of IKEv2 and IPsec with Multiple CoA support

MONAMI6 WG, IETF 68

Vijay Devarapalli (vijay.devarapalli@azairenet.com)

Assumptions in RFC 3775, 3963

- There is only one primary care-of address per mobile node
- The primary care-of address is stored in the IPsec database for tunnel encapsulation and decapsulation
- The source address on packets from MN to HA is verified against the care-of address in the corresponding binding cache entry
  - If the packet is a reverse tunneled packet, the care-of address check is done against the source address on the outer IPv6 header
- The IKE SA is based on the care-of address of the mobile node

IKEv2 security associations

- The mobile node picks one CoA as the source address of the IKEv2 exchange
- The same CoA is used all the time for all IKEv2 exchanges
- If the MN wants to use a new CoA for any existing IKEv2 SA, it just sends a BU with the ‘K’ bit set to update the IKEv2 SA with the new CoA
    - If dynamic update of IKEv2 SAs not supported, the MN re-establishes IKEv2 SAs with the new CoA

Transport Mode IPsec SAs

- IPsec in transport mode is used for BU/BAck and Mobile Prefix discovery messages
- The source address on the messages is checked against the CoA in the BCE
  - If the source address matches any one of the CoAs in the BCE, the packet is accepted
  - Otherwise dropped
  - Check is done by the MIPv6/Monami6 implementation on the home agent
- The IPsec implementation on the home agent does not care about the source address used on the BU

Tunneled HoTi/HoT Messages

- The MN uses just one CoA for all HoTi messages reverse tunneled through the HA
  - It does not matter which CoA is used to send the HoTi to the CN, since the CN does not see the CoA used on the HoTi messages
- The same tunnel mode IPsec SA is used to tunnel all HoTi messages
- The HA checks the source address on the outer header with the BCE
  - Decapsulates and forwards the tunnel HoTi message as long as the source address matches one of the CoAs
- For HoT messages, it does not matter which CoA is used to tunnel the packet to the MN
  - The HoT message just needs to reach the MN

Tunneled Payload Traffic

- Multiple IPsec protected tunneled flows is a bit harder
- Receiving tunneled IPsec payload messages
  - IPsec ignores the source address used in the outer IPv6 header
  - CoA used for the reverse tunneled payload traffic can be different from the CoA used for setting up the IPsec SA
  - HA must still verify that the CoA is one of the CoAs in the BCE
- Sending tunneled IPsec payload messages
  - The IPsec implementation on the HA may not be aware of which CoA to use when performing tunnel encapsulation
  - The Monami6 stack must specify which tunnel end point to use
  - Requires tighter integration between the IPsec and Monami6 implementations on the HA

Comments/Questions?