An Extension to Mesh Link Establishment (MLE) for Host Identity Protocol Diet Exchange (HIP DEX)

draft-ohba-6lo-mle-hip-dex-00

Yoshihiro Ohba

Presented by Subir Das

Background

- HIP DEX (Host Identity Protocol Diet EXchange) [I-D.moskowitz-hip-dex] is a light-weight key exchange protoc ol designed for constrained devices
  - 4-way handshake for authenticated static ECDH to establish session key materials
- MLE (Mesh Link Establishment) [I-D.kelsey-6lo-mesh-link-establishment] is defined for establishing and config uring secure links in IEEE 802.15.4 mesh networks
  - 3-way handshake for exchanging PSK-based authenticated link-layer parameters such as a frame counter
- Integration of HIP DEX and MLE can make
  - MLE support keying with public-key based mutual authentication
  - total handshake of HIP DEX and MLE 5-way (or 2.5 roundtrips), instead of 7-way (or 3.5 roundtrips)
- Presented in IETF92 6lo WG meeting:
  - https://www.ietf.org/proceedings/92/slides/slides-92-6lo-9.pdf

Changes from draft-ohba-6lo-mle-hip-dex

1. Changed key derivation algorithm to derive GroupL2Key and GroupMLEKey from GroupMasterKey
   - In the previous version, both GroupL2Key and GroupMLEKey are distributed

2. Added a rule that both link-layer Frame Counters and MLE Frame Counters are n ot reset in the Key Update Phase
   - 5-octet Frame Counter is enough for this

3. Added a rule that any valid MAC frame protected by new GroupL2Key can be use d as a trigger to deactivate old GroupL2Key
   - To deal with loss of multicast MLE Update used for key switch
   - The change #2 made this possible

Next Steps

- ZigBee NAN (Neighborhood Area Network) WG uses this draft i n their profile specification
  - ZigBee NAN specification is under 0.7 letter ballot recirculation
  - Once 0.7 letter ballot completes, the specification will be ready for inte rop tests

- Intended status: Experimental RFC
  - The author requests the draft to be 6lo WG item together with MLE ba se draft