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

draft-ohba-6lo-mle-hip-dex-01

Yoshihiro Ohba

Background

- HIP DEX (Host Identity Protocol Diet EXchange) [I-D.moskowitz-hip-dex] is a light-weight key exchange protocol 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 configuring 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 and IETF93 6lo WG meetings:
  - https://www.ietf.org/proceedings/92/slides/slides-92-6lo-9.pdf
  - https://www.ietf.org/proceedings/93/slides/slides-93-6lo-7.pdf
    - Use of the draft by ZigBee NAN (Neighborhood Area Network) WG was mentioned
    - Mentioned that intended status is "**Experimenta**l"

Changes from version -00

- In Section 7, added support for use of MPL multicast for Certificate Revocation List (CRL) distribution

    “When a CRL TLV is carried in a multicast Update message and forwarded multiple hops, MPL [I-D.ietf-roll-trickle-mcast] MAY be used. In this case, the multicast Update message MUST be secured at the link layer and MUST NOT be secured by MLE as specified in [I-D.kelsey-6lo-mesh-link-establishment]. Detailed MPL parameters for the multicast-based CRL distribution are out of the scope of this document.”

    - Discussion related to this change came from ZigBee NAN letter ballot comment resolution

Needed change in MLE base specification

- MLE base specification: draft-kelsey-6lo-mesh-link-establishment

- Needed change in MLE base specification (cf. https://mailarchive.ietf.org/arch/msg/6lo/vgbvU7I61pyVo2taHgrU-SYIosQhange)

  "The length of the TLV Length field is currently one octet, allowing up to 255 bytes for Value field. However, an MLE extension defined in draft-ohba-6lo-mle-hip-dex needs more than 255 bytes for Value field. One case is to carry HIP DEX certificates in MLE message. Another case is to carry a certificate revocation list in MLE. Therefore, the length of TLV Length should be at least 2-octet for longer Value fields."

Next Steps

- Wait for the needed change (i.e., longer Length field length) of MLE base specification