Network Working Group                                    Y. Ohba, Ed.
Internet-Draft                                                Toshiba
Intended status: Experimental                       October 18, 2015
Expires: April 20, 2016


        An Extension to Mesh Link Establishment (MLE) for Host Identity Protocol
                         Diet Exchange (HIP DEX)
                       draft-ohba-6lo-mle-hip-dex-01

Abstract

   This document defines an extension of MLE (Mesh Link Establishment)
   protocol to encapsulate HIP DEX key exchange protocol messages.

Status of This Memo

   This Internet-Draft is submitted in full conformance with the
   provisions of BCP 78 and BCP 79.

   Internet-Drafts are working documents of the Internet Engineering
   Task Force (IETF).  Note that other groups may also distribute
   working documents as Internet-Drafts.  The list of current Internet-
   Drafts is at http://datatracker.ietf.org/drafts/current/.

   Internet-Drafts are draft documents valid for a maximum of six months
   and may be updated, replaced, or obsoleted by other documents at any
   time.  It is inappropriate to use Internet-Drafts as reference
   material or to cite them other than as "work in progress."

   This Internet-Draft will expire on April 20, 2016.

---

Table of Contents

1.  Introduction

   HIP DEX (Host Identity Protocol Diet EXchange)
   [I-D.moskowitz-hip-dex] is a light-weight key exchange protocol
   designed for constrained devices.  HIP DEX builds on the HIP Base
   EXchange (HIP BEX) [I-D.ietf-hip-rfc5201-bis] and inherits the
   transport-agnostic property of HIP BEX.

   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.  MLE
   assumes that shared keys to secure link-layer frames and MLE messages
   exchanged between a pair of nodes are pre-configured between the
   nodes.  Therefore, a key exchange protocol is required in order to
   dynamically configure the required shared keys.  While such a key
   exchange protocol can be run outside MLE, sequentially running a key
   exchange protocol and MLE as separate protocols requires more message
   roundtrips.  For example, running a HIP DEX 4-way handshake followed
   by an MLE 3-way handshake requires 3.5 message roundtrips.

In this document, an extension to the MLE protocol for encapsulating
HIP DEX messages is defined in order to realize optimized key
exchange and link establishment for IEEE 802.15.4 mesh networks.

## 1.1.  Requirement Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",
"SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and
"OPTIONAL" in this document are to be interpreted as described in
[RFC2119].

## 1.2.  Acronyms

DEX-I1, DEX-R1, DEX-I2, DEX-R2: HIP DEX I1, R1, I2, R2 messages

ECDH: Elliptic Curve Diffie-Hellman

EI: HIP DEX Key Establishment Initiator

ER: HIP DEX Key Establishment Responder

LLFC: Link-Layer Frame Counter

MIC: MLE Message Integrity Code

MLFC: MLE Frame Counter

UI: HIP DEX Key Update Initiator

UR: HIP DEX Key Update Responder

## 1.3.  Convention

In the figures of this document, MLE messages marked with '*' are
those secured by the MLE protocol.

In the key material formats in this document, '|' denotes
concatenation operator.

## 2.  Overview

HIP DEX over MLE consists of two phases, i.e., Key Establishment
Phase and Key Update Phase.  In Key Establishment Phase, a HIP DEX
4-way handshake using I1, R1, I2 and R2 messages is conducted to
establish a secure channel between an EI and an ER based on an ECDH
shared secret and exchange session key materials over the secure
channel.

In Key Update Phase, HIP DEX Update messages encrypting session key
materials are exchanged between a UI and each UR using an MLE Update
Request and Update exchange, followed by a multicast MLE Update
message for triggering each UR to simultaneously activate new key

materials and reset the associated link-layer frame counters.  The UI
and UR roles for a pair of nodes may be determined independently of
the EI and ER roles that have been taken by the nodes.

All MLE messages used for the extension defined in this document
SHOULD NOT be protected by link-layer so that a key exchange can be
done regardless of the security state of the link-layer.  A node that
implements this specification MUST allow sending and receiving MLE
messages not secured by the link-layer.

Secured 802.15.4 MAC frames and MLE messages that use keys
established via HIP DEX MUST use a 5-octet Frame Counter so that the
Frame Counter does not reach its maximum value throughout the
lifetime of a node.  An MLE Frame Counter is always carried in the
Frame Counter field in the Aux Header of any secured MLE frame.

Other than the rules described in this document, the rules defined in
[I-D.kelsey-6lo-mesh-link-establishment] are preserved.

3.  Key Establishment Phase

A message exchange diagram for Key Establishment Phase is shown in
Figure 1.

```
 (EI)  (ER)
   -->     Advertisement [HIP{DEX-I1}, Link Quality]

   <--     Advertisement [HIP{DEX-R1}, Link Quality]
```

```
    -->     Link Request  [HIP{DEX-I2}, Source Address, Mode,
                        Timeout, Challenge]*

    <--     Link Accept and Request
                        [HIP{DEX-R2}, LLFC, MLFC, Source Address, Mode,
                        Timeout, Response, Challenge]*

    -->     Link Accept   [LLFC, MLFC, Response]*
```

                   Figure 1: Key Establishment Phase

   An EI sends an MLE Advertisement message containing a HIP TLV and a
   Link Quality TLV to an ER.  The HIP TLV carries a DEX-I1 packet.  How
   an EI discovers an ER is outside the scope of this document.

   The ER receives the MLE Advertisement message containing a DEX-I1
   packet from the EI and sends an MLE Advertisement message containing
   a HIP TLV and a Link Quality TLV to the EI.  The HIP TLV carries a
   DEX-R1 packet.  The DEX-R1 packet MUST contain mandatory R1

   parameters specified in [I-D.moskowitz-hip-dex].  The DEX-R1 packet
   MAY contain optional R1 parameters specified in
   [I-D.moskowitz-hip-dex] and a CERT parameter defined in [RFC6253].

   The EI receives the MLE Advertisement message from the ER and sends a
   secured MLE Link Request message containing HIP, Source Address,
   Mode, Timeout and Challenge TLVs to the ER.  The HIP TLV carries a
   DEX-I2 packet.  The DEX-I2 packet MUST contain mandatory I2
   parameters specified in [I-D.moskowitz-hip-dex] including an
   ENCRYPTED_KEY parameter wrapping a session key material of the EI.
   The DEX-I2 packet MUST also contain an ENCRYPTED parameter wrapping
   group key materials of the EI.  The DEX-I2 packet MAY contain
   optional I2 parameters specified in [I-D.moskowitz-hip-dex] and a
   CERT parameter defined in [RFC6253].  The MLE Link Request message is
   protected by the EI's group MLE key (see section Section 5.2) derived
   from the EI's group key materials.

   The ER receives the MLE Link Request message from the EI and extracts
   the EI's session key material wrapped in the ENCRYPTED_KEY parameter
   and the EI's group key materials wrapped in the ENCRYPTED parameter.
   Then the ER sends a secured MLE Link Accept and Request message
   containing HIP, LLFC, MLFC, Source Address, Mode Timeout, Response

and Challenge TLVs to the EI.  The HIP TLV carries a DEX-R2 packet.
The DEX-R2 packet MUST contain R2 parameters specified in
[I-D.moskowitz-hip-dex] including an ENCRYPTED_KEY parameter wrapping
a session key material of the ER.  The DEX-R2 packet MUST also
contain an ENCRYPTED parameter wrapping group key materials of the
ER.  The DEX-R2 packet MAY contain optional R2 parameters specified
in [I-D.moskowitz-hip-dex].  Note that the MIC field of the MLE Link
Request message is verified after the ER successfully extracts the
EI's group key materials.

The EI receives the MLE Link Accept and Request message from the ER
and extracts the ER's session key material wrapped in the
ENCRYPTED_KEY parameter and the ER's group key materials wrapped in
the ENCRYPTED parameter.  Then the EI sends a secured MLE Link Accept
message containing LLFC TLV, MLFC and Response TLVs to the ER.  If a
pair-wise key is used by the link-layer, the EI also creates a Pair-
wise Key SA with the session key generated by the pair of session key
materials of the EI and ER as specified in [I-D.moskowitz-hip-dex].
Note that the MIC field of the MLE Link Accept and Request message is
verified after the EI successfully extracts the ER's group key
materials.

The ER receives the MLE Link Accept message from the EI.  If a pair-
wise key is used by the link-layer, the EI creates a Pair-wise Key SA
with the session key generated by the pair of session key materials
of the EI and ER as specified in [I-D.moskowitz-hip-dex].

4.  Key Update Phase

    In Key Update Phase, group key materials are updated.

    Since the 5-octet Frame Counter space is large enough considering the
    maximum bandwidth of 250Kbps in 802.15.4 [IEEE802154] to make an
    assumption that a Frame Counter does not reach its maximum value
    throughout the lifetime of a node, a mechanism for updating a pair-
    wise key is not defined in this document.  Both link-layer Frame
    Counters and MLE Frame Counters are not reset in the Key Update
    Phase.

    Updating a group key may happen when a node that shares the group key
    is revoked.  A message exchange diagram for group key update is shown
    in Figure 2.

```
(UI) (UR1)..(URn)
                    // Update 1st peer
  ---->             Update Request [HIP{DEX-UPDATE}, MLFC, Source Address]*
  <----             Update [HIP{DEX-UPDATE}, MLFC, Source Address]*
      ..                            ..

                    // Update n-th peer
  ----------->      Update Request [HIP{DEX-UPDATE}, MLFC, Source Address]*
  <-----------      Update [HIP{DEX-UPDATE}, MLFC, Source Address]*

                    // Key switch notification (multicast)
  ----> .. -->      Update [LLFC, MLFC]*

                    Figure 2: Group Key Update
```

First, a UI performs the following exchange for each UR:

o  The UI sends an MLE Update Request message containing HIP, MLFC,
   Source Address and MIC TLVs to a UR.  The HIP TLV carries a DEX-
   UPDATE packet containing SEC, MAC and ENCRYPTED parameters.  The
   ENCRYPTED parameter wraps new group key materials of the UI.

o  The UR receives the MLE Update Request message from the UI,
   extracts UI's new group key materials from the ENCRYPTED
   parameter, activates the UI's new group key materials for incoming
   frames, and sends an MLE Update message containing HIP, MLFC and
   Source Address TLVs, where the HIP TLV carries a DEX-UPDATE packet
   containing ACK and MAC parameters.  Note that the MIC field of the
   MLE Update message is verified after the UR successfully extracts
   the UI's new group key materials.

   Once MLE Update Request and Update exchange is completed for all URs,
   the UI activates the UI's new group key materials for outgoing frames
   by multicasting an MLE Update message containing LLFC and MLFC TLVs.
   The MLE Update message is protected by the UI's group MLE key (see
   section Section 5.2) derived from the UI's new group key materials.

   When a UR receives the multicast MLE Update message, If the received
   message is valid, the UR deactivates the UI's old group key materials

for incoming frames.

    A UR that did not receive the multicast MLE Update message may
    deactivate the UI's old group key materials for incoming frames when
    it receives a valid MAC frame protected by the link-layer key derived
    from the UI's new group key materials.

## 5. Key Materials

## 5.1. Pair-wise Key

    The first 16 octets of the session key corresponding to the HIP DEX
    Pair-wise SA [I-D.moskowitz-hip-dex] is used as the pairwise link-
    layer key used for securing unicast link-layer frames with Key
    Identifier Mode 0x00.

    An encrypted session key material is contained in an ENCRYPTED_KEY
    parameter of HIP when the session key is distributed during Key
    Establishment Phase.

## 5.2. Group Keys

    Group key materials are created by a node and distributed to peer
    nodes.

    The group key materials consist of a 1-octet key identifier (KeyId)
    and a 16-octet group master key (GroupMasterKey), and encoded as
    follows:

    Group Key Materials = KeyId | GroupMasterKey

    A 16-octet group link-layer key (GroupL2Key), and a 16-octet group
    MLE key (GroupMLEKey) are derived from GroupMasterKey as follows:

    GroupL2Key = The first 16-octet of HMAC_SHA256(GroupMasterKey,
    KeyId).

    GroupMLEKey = The last 16-octet of HMAC_SHA256(GroupMasterKey,
    KeyId).

    A GroupL2Key is used for securing link-layer frames with Key

Identifier Mode 0x03 sent by the node that created the group key material.  GroupL2Key MUST be used for securing broadcast link-layer frames and MAY also be used for securing unicast link-layer frames.

A GroupMLEKey MUST be used for securing MLE messages with Key Identifier Mode 0x03 sent by the node that created the group key material.

The group key materials are contained in an GROUP_KEY_MATERIALS parameter of HIP, where the GROUP_KEY_MATERIALS parameter MUST be encrypted in an ENCRYPTED parameter of HIP.

6.  MLE Security

As described in [I-D.kelsey-6lo-mesh-link-establishment], MLE security reuses that of IEEE 802.15.4, i.e., AES-CCM* [IEEE802154]. Since some of the MLE messages (i.e., MLE Link Accept and Request and MLE Accept messages carrying DEX-I2 and DEX-R2 packets, respectively, and unicast MLE Update Request and Update messages carrying a DEX-UPDATE packet) require to be sent unencrypted and only authentication is needed, MIC-64 (Security Level 2) or MIC-128 (Security Level 3) is used to secure MLE messages.  MIC-64 is the default security level for securing MLE messages used in this document.  GroupMLEKey (see section Section 5.2) with Key Identifier Mode 0x03 and a 5-octet Frame Counter MUST be used for any secured MLE message.

7.  Certificate Revocation

Any MLE message used in this document MAY also contain a CRL (Certificate Revocation List) TLV in which CertificateList defined in [RFC5280] is encoded in the Value field.  A node that receives a valid MLE message containing a CRL TLV revokes certificates specified in the TLV and deletes all pair-wise and group keys associated with the revoked certificates.  A node MUST reject a CERT parameter for a revoked certificate in Key Establishment Phase.

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.

8.  Security Considerations

   The MLE extension defined in this document uses HIP DEX for key
   management of computation or memory constrained sensor/actuator
   devices, and thus it inherits all security considerations made for
   HIP DEX [I-D.moskowitz-hip-dex].

   In order to mitigate security weakness caused by lack of Perfect
   Forward Secrecy (PFS) in HIP DEX, it is RECOMMENDED to use this MLE
   extension in conjunction with an additional mechanism to update
   public/private key pairs and renew HIP DEX SAs using new public/
   private key pairs whenever necessary.

   In both Key Establishment Phase and Key Update Phase, MLE messages
   are secured using a group key instead of a pairwise key in order to
   optimize message roundtrips since a group key establishment requires
   only a half roundtrip.  As a result, a Denial of Service (DoS) attack
   from an insider sharing the group key is possible over MLE TLVs.

   Due to integration of HIP DEX into MLE, secured MLE messages are
   authenticated but not encrypted because decryption can be done only
   after establishing a key.  As a result, Source Address, Mode,
   Timeout, Challenge, Response LLFC and MLFC TLVs are sent in clear,
   and the cleartext information may be used by attackers for the DoS
   attack described above.  Note that authentication of the MLE message
   carrying a DEX-I2, DEX-R2 or DEX-UPDATE packet is possible by
   validating MIC of the MLE message after extracting the authentication
   key (i.e., GroupMLEKey) from the HIP DEX packet.

9.  IANA Considerations

9.1.  MLE TLV Types

   The following MLE TLV types are to be assigned by IANA based on the
   policy described in [I-D.kelsey-6lo-mesh-link-establishment]:

   o  HIP-DEX (Value: 9, Length: Variable, Meaning: HIP DEX packet,
      Reference: this document).

   o  CRL (Value: 10, Length: Variable, Meaning: Certificate Revocation
      List, Reference: this document).

9.2.  HIP Parameter

   The following HIP Parameter is assigned based on the policy described
   in [I-D.ietf-hip-rfc5201-bis]:

   o  GROUP_KEY_MATERIALS, (Value: 65530, Length: 33, Meaning: Group key
      materials for MLE and link-layer, Reference: this document).

## 10.  Acknowledgments

   The author would like to acknowledge the helpful comments of Randy
   Turner, Robert Cragie and Subir Das.

## 11.  References

## 11.1.  Normative References

   [RFC2119]  Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119,
              DOI 10.17487/RFC2119, March 1997,
              <http://www.rfc-editor.org/info/rfc2119>.

   [RFC5280]  Cooper, D., Santesson, S., Farrell, S., Boeyen, S.,
              Housley, R., and W. Polk, "Internet X.509 Public Key
              Infrastructure Certificate and Certificate Revocation List
              (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008,
              <http://www.rfc-editor.org/info/rfc5280>.

   [RFC6253]  Heer, T. and S. Varjonen, "Host Identity Protocol
              Certificates", RFC 6253, DOI 10.17487/RFC6253, May 2011,
              <http://www.rfc-editor.org/info/rfc6253>.

   [I-D.moskowitz-hip-dex]
              Moskowitz, R. and R. Hummen, "HIP Diet EXchange (DEX)",
              draft-moskowitz-hip-dex-04 (work in progress), July 2015.

   [I-D.ietf-hip-rfc5201-bis]
              Moskowitz, R., Heer, T., Jokela, P., and T. Henderson,
              "Host Identity Protocol Version 2 (HIPv2)", draft-ietf-
              hip-rfc5201-bis-20 (work in progress), October 2014.

   [I-D.kelsey-6lo-mesh-link-establishment]
              Kelsey, R., "Mesh Link Establishment", draft-kelsey-6lo-
              mesh-link-establishment-00 (work in progress), July 2015.

[I-D.ietf-roll-trickle-mcast]
            Hui, J. and R. Kelsey, "Multicast Protocol for Low power
            and Lossy Networks (MPL)", draft-ietf-roll-trickle-
            mcast-12 (work in progress), June 2015.

11.2.  External Informative References

   [IEEE802154]
            IEEE standard for Information Technology, "IEEE std.
            802.15.4, Part. 15.4: Wireless Medium Access Control (MAC)
            and Physical Layer (PHY) Specifications for Low-Rate
            Wireless Personal Area Networks", June 2011.

Author's Address

   Yoshihiro Ohba (editor)
   Toshiba Electronics Asia
   20 Pasir Panjang Road, #12-25/28, Mapletree Business City
   117439
   Singapore

   Phone: +65 6278 5252
   Email: yoshihiro.ohba@toshiba.co.jp