Adapted Multimedia Internet KEYing (AMIKEY): An extension of Multimedia Internet KEYing (MIKEY) Methods for Generic LLN Environments

draft-alexander-roll-mikey-lln-key-mgmt-01.txt

R. Alexander
T. Tsao

IETF-81, ROLL WG Meeting, 7/29/2011

Outline

- Motivation
- Objectives
- MIKEY Strengths
- RPL Security
- AMIKEY Overview
    - 01 draft included specific RPL elements
    - 02 will include additional signaling mechanism
        - Discussed in this presentation
- Summary

Motivation

- “Security Framework for ROLL” (Tsao et al) set requirements for routing protocol security
  - Provided guidance for security features developed as part of Secure RPL
  - Framework was not a KM specification
- Current Secure RPL specifies packet level security but relies on external, out-of-band (OOB) Key Management
  - (Reference: RPL, Sections 3.2.3 and 10.3)
  - AMIKEY is developed to meet RPL KM requirement and for LLN use more generally

Objective for AMIKEY

- Support RPL security within an efficient LLN device security model
  - Addressing system as well as routing security
- Offer Generic LLN key management (KM) protocol
  - Short-term, per-session/association keys [RFC4107], or long-term credentials update
- Extend capability of an established, validated and current IETF KM protocol
  - MIKEY [RFC3830] base
  - Standard AKM features already defined and specified
  - Introduce AES-based default algorithms (as available in many LLN HW platforms)

Relevant MIKEY Strengths

- Lightweight, low bandwidth
  - Binary encoded 1-byte aligned
- Simple, low-latency, end-to-end security
  - Key assignment can be completed in as little as ½ roundtrip; 1 roundtrip at most
- Flexible and extensible with multiple methods defined for establishing security associations
  - Pre-shared key, public key, Diffie-Hellman
- Independent from underlying transport network security
  - Messages embedded in other protocols or sent over TCP or UDP/IP (port 2269)

RPL Security

- 3 modes: Unsecured, pre-installed, authenticated
  - Pre-installed provides pre-configured credentials
  - Authenticated allows subsequent key update
- ‘Code’ field in HDR designates secured messages
- Message confidentiality and integrity provided including timeliness
  - Security header specifies: Algorithm, Key ID and Source, and applied Security Level
  - No per-routing association/session key generation
- Key management needed to update long-term key credentials and security policy

Multi-Layer Key Mgmt Context

```
.............................          .............................
: +----------+              :          :              +----------+ :
: |+--------+|              :          :              |+--------+| :
: || AMIKEY ||              :  AMIKEY  :              || AMIKEY || :
: || Key    |<========================================>| Key    || :
: || Mgmt.  ||           Key Exchange (TGK)           || Mgmt.  || :
: || Entity ||              :          :              || Entity || :
: |+--------+|              :          :              |+--------+| :
: | Security |   Node i     :          :     Node j   | Security | :
: | Services |              :          :              | Services | :
: | Entity   |              :          :              | Entity   | :
: +----------+              :          :              +----------+ :
:  |                        :          :                        |  :
:  |           +-----------+:          :+-----------+           |  :
:  | (CSn)+--->| Protocol-n|:          :| Protocol-n|<---+(CSn) |  :
:  |      |    +-----------+:          :+-----------+    |      |  :
:  |      |  +-----------+  :          :  +-----------+  |      |  :
:  | (CS7)|->|Application|  :          :  |Application|<-|(CS7) |  :
:  |      |  +-----------+  :          :  +-----------+  |      |  :
:  |      |  +-----------+  :          :  +-----------+  |      |  :
:  | (CS4)|->| Transport |  :          :  | Transport |<-|(CS4) |  :
:  |      |  +-----------+  :          :  +-----------+  |      |  :
:  +------|                 :          :                 |------+  :
:         |  +-----------+  :          :  +-----------+  |         :
:    (CS3)|->|  Network  |  :          :  |  Network  |<-|(CS3)    :
:         |  +-----------+  :          :  +-----------+  |         :
:         |  +-----------+  :          :  +-----------+  |         :
:    (CS2)|->|     L2    |  :          :  |     L2    |<-|(CS2)    :
:         |  +-----------+  :          :  +-----------+  |         :
:         |  +-----------+  :          :  +-----------+  |         :
:    (CS1)+->|     L1    |  :          :  |     L1    |<-+(CS1)    :
:            +-----------+  :          :  +-----------+            :
:...........................:          :...........................:
```

- LLN model for multi-layer key management

Key Exchange Signaling Modes

```
   Key                                 Key Assignment
Responder                                 Initiator
 +-----+                                 +---------+
 |  R  |                                 | I(KMS)  |
 +-----+                                 +---------+
                     I_MESSAGE
     <------------------------------------------
                [Optional] R_MESSAGE
     ------------------------------------------->
```

Key server (push) initiated

```
   Key                                 Key Assignment
ReQuestor                                 Initiator
 +-----+                                 +---------+
 |  Q  |                                 | I(KMS)  |
 +-----+                                 +---------+
                    Q_MESSAGE
     ------------------------------------------>
                     I_MESSAGE
     <-----------------------------------------
```

Key client (pull) requested

Pre-shared Key Example

```
                                                  Requestor

                                                     Q_MESSAGE =
                                        [<---]       HDR, T, [IDq], V


Initiator                                         Responder

   I_MESSAGE =
   HDR, T, RAND, [IDi],[IDr],
        {SP}, KEMAC                      --->
                                                     R_MESSAGE =
                                        [<---]       HDR, T, [IDr], V
```

- Supported key request or initiated key assignment
  - [Optional] Requestor or Responder messages
    - Header (HDR), Timestamp (T), and Verification (V) message elements

Public-Key Encryption Example

```
                                               Requestor

                                                Q_MESSAGE =
                                       [<---]   HDR, T, [IDq|CERTq], SIGNq


Initiator                                      Responder

I_MESSAGE =
HDR, T, RAND, [IDi|CERTi], [IDr], {SP},
    KEMAC, [CHASH], PKE, SIGNi          --->
                                                R_MESSAGE =
                                       [<---]   HDR, T, [IDr], V
```

- Same low latency exchanges as PSK method
  - PK signature replaces PSK verification
  - Certificates used or just ID where certificate can be retrieved based on ID

Example Message Sizes

- Pre-shared Key (PSK) Exchange
  - Requestor/Responder Message = **32** bytes
  - Initiator Message = **80** bytes
- Public-Key Encryption (PKE) Exchange
  - Requestor Message = **44** bytes
    - Signature = 18 bytes (replaces PSK Verification)
  - Initiator Message = **118** bytes
    - Additional PKE and SIGN elements
  - 1K bytes size increase if X.509 certificate transported rather than accessed from ID

AMIKEY Extension

- New Requestor message defined
  - Allows device to trigger key assignment from centralized Key Server
- New transforms and parameters defined
  - All AES-based given ready availability and implementation within LLN HW platforms
- New policy payload defined
  - Generic-LLN
- Support for LLN protocols security
  - RPL as well as domain specific (AMI, for ex.)
- Multimedia crypto-sessions re-purposed to allow simultaneous KM for multiple protocols

RPL Elements

- Requestor message allows RPL joining nodes to request DODAG key
  - Both PSK and PKE options
- Key Index and Key Source ID elements specified
  - IPv6 and MAC address ID types included
- Security policy specification and update
- Existing key-data, timestamp, and algorithm specification used for key control
  - Including Counters or NTP timestamps

Summary

- Extension to simple, efficient KM protocol
  - Supports long-term and short-term (session) KM
  - Allows all-AES algorithm defaults
  - Supports LLN device implementation efficiency
- Generic KM protocol offers greater utility to LLNs versus stand-alone RPL key management
  - Able to meet current and future RPL requirements
  - Tradeoff of additional effort/overhead to create general LLN KM protocol versus RPL-only
- Look forward to WG discussion on adopting and completing the specification
  - RPL companion with wider domain applicability