6TiSCH   S. Chasko
Internet-Draft   L+G
Intended status: Informational   S. Das
Expires: September 23, 2014   ACS
                                                       R. Marin-Lopez
                                                 University of Murcia
                                                        Y. Ohba, Ed.
                                                            Toshiba
                                                        P. Thubert
                                                            cisco
                                                          A. Yegin
                                                          Samsung
                                                    March 22, 2014

Security Framework and Key Management Protocol Requirements for 6TiSCH
draft-ohba-6tisch-security-01

Abstract

   6TiSCH is enabling IPv6 over the TSCH mode of the IEEE802.15.4e
   standard that allows the IEEE 802.15.4e TSCH wireless networks and
   nodes to connect to the backbone network via layer 3 meshes over
   IPv6. In this operation of network architecture, understanding the
   security framework and requirements for key management protocols are
   critical. This document discusses such security framework and key
   management protocol requirements by highlighting different phases of
   key management in which a new node can securely join the network
   under the purview of overall 6TiSCH architecture.

Status of This Memo

Table of Contents

1. Introduction

   The emergence of radio technology enabled a large variety of new
   types of devices to be interconnected, at a very low marginal cost
   compared to wire, at any range from Near Field to interplanetary
   distances, and in circumstances where wiring could be less than
   practical, for instance rotating devices.

   At the same time, a new breed of Time Sensitive Networks is being
   developed to enable traffic that is highly sensitive to jitter and
   quite sensitive to latency. Such traffic is not limited to voice and
   video, but also includes command and control operations such as found
   in industrial automation or in-vehicular sensors and actuators.

   6TiSCH aims at providing an interoperable standard with new
   capabilities, both in terms of scalability (number of IPv6 devices in
   a single subnet) and in terms of guarantees (delivery and

timeliness). Both the ISA100.11a [ISA100] and Wireless HART
[WirelessHART] protocols are gaining acceptance in the automation
industry and demonstrate that a level of determinism can be achieved
on a wireless medium with adequate guarantees for low speed control
loops, used in mission critical Process Control applications. For
industrial applications, security is not an option and a power
efficient authentication mechanism is strictly required.

For other usages such as rust control, intrusion detection or seismic
activity monitoring, the capability to correlate inputs from multiple
sources can be critical, and the value of the network directly
augments with the number of connected devices. In order to scale to
appropriate levels, the need for spatial reuse of the spectrum often
implies routing capabilities over short range radios. Proprietary
variations demonstrate that RPL can scale to multiple thousands of
devices, but at the same time expose a new challenge for security
that must enable deployments of any scale with security requirements
that may vary widely. If the cost of the security in terms of
network operations and system resources depends on that degree of
security, then 6TiSCH should enable different profiles that can match
different requirements and capabilities.

Since 6TiSCH enables layer 3 meshes over IPv6, key management
protocols defined at layer 3 or above can be directly applied to the
networks and nodes that join the mesh network. However,
understanding the security framework and requirements for key
management protocols are critical before adopting an existing
protocol or designing a new one that fits the operational needs for
these types of networks. This document details such operations and
discusses the security framework with requirements within the context
of 6TiSCH architecture [I-D.ietf-6tisch-architecture].

2. Acronyms

In addition to the acronyms defined in [I-D.ietf-6tisch-terminology],
the following acronyms are used in this document.

KMP: Key Management Protocol

SA: Security Association

MAC: Media Access Control

3. Security Framework

This section describes a security framework consisting of four phases
of key management operation as shown in Figure 1. It is expected
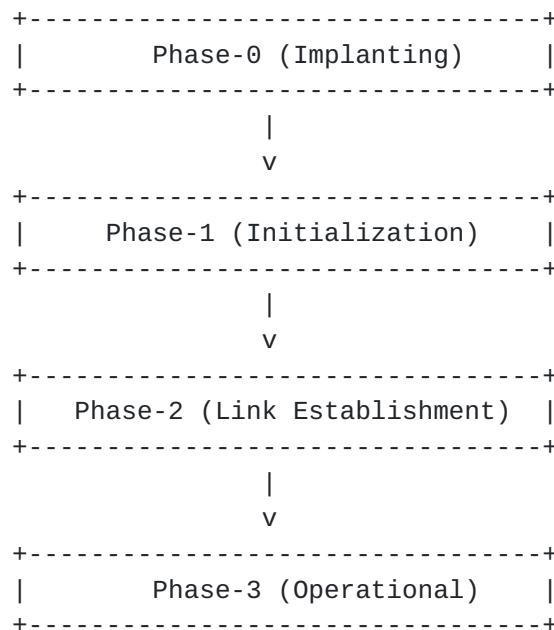that each node in a mesh network runs through the four phases.

```
              +--------------------------------+
              |        Phase-0 (Implanting)    |
              +--------------------------------+
                              |
                              v
              +--------------------------------+
              |      Phase-1 (Initialization)  |
              +--------------------------------+
                              |
                              v
              +--------------------------------+
              |    Phase-2 (Link Establishment)|
              +--------------------------------+
                              |
                              v
              +--------------------------------+
              |        Phase-3 (Operational)   |
              +--------------------------------+
```

                 Figure 1: 4-Phase Key Management Model

   Each phase is explained as follows.

   o Phase-0 (Implanting Phase): In this phase, a node installs
      credentials used for subsequent phases in a physically secure and
      managed location before the node is placed to where it is expected
      to operate. Details on how Phase-0 can be achieved are outside
      the scope of this document.

   o Phase-1 (Initialization Phase): Phase-1 (Initializing Phase): In
      this phase, an authentication and key Establishment protocol
      called a Phase-1 KMP is conducted either between nodes or between
      a node and the authentication/authorization server using Phase-1
      credentials. Both symmetric and asymmetric key credentials can be
      used as Phase-1 credentials. When phase-1 KMP is run between a
      node and an authentication/authorization server, a node
      (re)install credentials used for subsequent phases (e.g., Phase 2
      and 3). The credentials installed during Phase-1 include Phase-2
      credentials and Phase-3 credentials, and may also include long-
      term Phase-1 credentials if the initial Phase-1 credentials are
      intended for one-time use such as a temporary PIN. The Phase-1
      credentials usually have longer lifetime than Phase-2 and Phase-3
      credentials so that Phase-2 and Phase-3 credentials can be renewed
      using the Phase-1 credentials. When the authentication server is
      multiple hops away from the node, mutual authentication between
      the node and the authentication server may be conducted via a
      neighboring node acting as an authentication relay. There may be
      no link-layer security available between the node and its

neighboring node in this phase. An authentication/authorization
server is typically (but is not necessarily) co-located with the
coordinator of the mesh network. Contacting the authentication/
authorization server is optional if Phase-2 credentials are
installed during Phase-0 and do not need to be updated.

o Phase-2 (Link Establishment Phase): In this phase, the node
   performs mutual authentication with its neighboring node using the
   Phase-2 credentials to establish SAs between adjacent nodes for
   protecting 802.15.4 MAC frames. The authentication and key
   establishment protocol used in this phase is referred as a Phase-2
   KMP or a link establishment KMP. For highly scalable mesh
   networks consisting of thousands of mesh nodes, certificates are
   used as the Phase-2 credentials. The SA of a link between node i
   and node j maintains link-layer keys, i.e., 128-bit keys used in
   AES-CCM* [IEEE802154] mode, a variant of the Counter with Cipher
   Block Chaining - Message Authentication Code (CBC-MAC) Mode, for
   encryption, authentication or authenticated encryption of 802.15.4
   frames. In the following example, K_i denotes a link-layer key
   for protecting broadcast MAC frames originated at node i. K_ij
   denotes a link-layer key for protecting unicast MAC frames
   originated at node i and destined for node j. There are several
   ways link-layer keys can be formed, for example, the models are:

   1. Per-Network key model

       K_ij=K_ji=K_i=K_j=K for all i, j (i!=j)

   2. Per-Neighbor key model

       K_ij!=K_ji, K_ij=K_i, K_i!=K_j for all i,j (i!=j)

   3. Pair-Wise key model

       K_ij=K_ji, Kij!=Kik, K_i!=K_j, for all i,j (i!=j, j!=k)

   In model 1, a network key that is shared by all nodes in the
   network is used for enciphering and deciphering outgoing and
   incoming unicast and broadcast MAC frames at any node. In model
   2, each node has a unique key for enciphering outgoing unicast and
   broadcast MAC frames originated at the node and its neighbors use
   the key for deciphering incoming unicast and broadcast MAC frames
   received from that node. In model 3, each pair of nodes has a
   unique key for enciphering and deciphering unicast frames
   exchanged between them. In addition, each node in model 3 has a
   unique key for enciphering outgoing broadcast MAC frames
   originated at the node and its neighbors use the key for
   deciphering incoming broadcast MAC frames received from that node.

One model may be sufficient among these three models depending on
the required security level and the number of keys maintained by
each node.

o Phase-3 (Operational Phase): In this phase, the node is able to
   run various higher-layer protocols over IP over an established
   secure link. Additional authentication, authorization and key
   establishment may take place for the higher-layer protocols using
   Phase-3 credentials. A node in Phase-3 is able to process Phase-1
   and Phase-2 KMPs. Example use cases are:

   * A Phase-3 node can initiate a Phase-1 KMP to update its Phase-2
      or Phase-3 credentials.

   * A Phase-3 node can forward Phase-1 KMP messages originated from
      or destined for a Phase-1 node that is joining the mesh network
      through the Phase-3 node.

   * A Phase-3 node can initiate a Phase 2 KMP to establish a new
      link with a newly discovered neighbor node.

Figure 2 shows an example sequence for authentication and
authorization message exchanges for Phase-1 and Phase-2. The example
sequence is explained as follows:

1. Initially all nodes are in Phase-1.

2. Nodes B and C run Phase-1 KMP with Node A which is acting as the
    authentication/authorization server) to obtain Phase-2 and
    Phase-3 credentials.

3. Nodes B and C run Phase-2 KMP with Node A.

4. Nodes D and E run Phase-1 KMP using Node B as an authentication
    relay. (Alternatively, Node E may use Node C as an
    authentication relay.)

5. Node D runs Phase-2 KMP with Node B. Node E runs Phase-2 KMP
    with Nodes B and C.

6. All nodes are operational.

```
            N)s - Node N is running Phase-1 KMP as a server
            N)c - Node N is running Phase-1 KMP as a client
            N)r - Node N is running Phase-1 KMP as a relay
            N)) - Node N is running Phase-2 KMP
            .  .. ...
            N, N,  N  - Node N is in Phase-1, -2 and -3, respectively


     .           .           ..          ...         ...          ...
      A           A)s         A))         A)s          A            A
              / \         / \         / \         / \          / \
     .   .       .   .       ..  ..      ... ...     ... ...      ... ...
    B   C       B)c C)c     B)) C))      B)r C       B)) C))      B   C
                                                / \ /       / \ /        / \ /
    .   .       .   .         .   .         .   .       ..  ..      ... ...
   D   E       D   E       D   E       D)c E)c     D)) E))      D   E

     (1)  ->    (2)    ->   (3)    ->   (4)  ->    (5)    ->    (6)
```
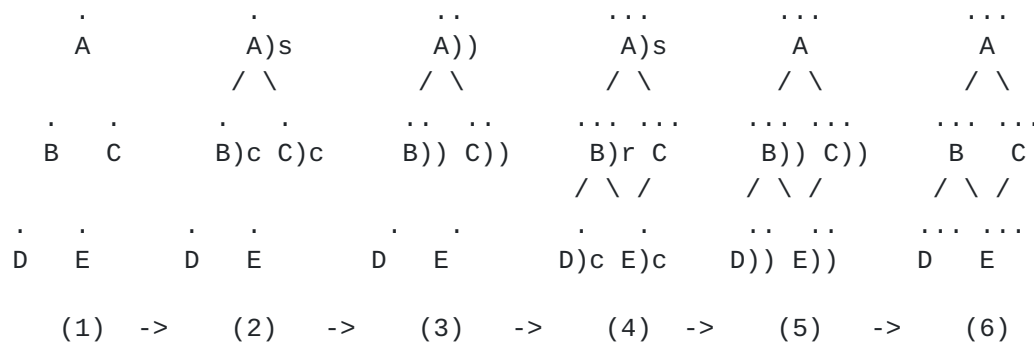
Figure 2: Example Sequence

4. KMP requirements

Since Phase-3 KMP requirements would depend on application protocols,
we focus on Phase-1 and Phase-2 KMP requirements.

4.1. Phase-1 KMP requirements

Requirements on Phase-1 KMP are listed below.

R1-1: Phase-1 KMP MUST support mutual authentication.

R1-2: Phase-1 KMP MUST support stateless authentication relay
operation.

R1-3:s Phase-1 KMP MUST support secure credential distribution.

4.2. Phase-2 KMP requirements

Requirements on Phase-2 KMP are listed below.

R2-1: Phase-2 KMP Nodes MUST mutually authenticate each other before
establishing a link and forming a mesh network. An authentication/
authorization server is not a requirement for this operation.

R2-2: Phase-2 KMP authentication credentials MAY be pre-provisioned
or MAY be obtained via Phase-1 KMP.

R2-3: Phase-2 KMP authentication credentials MUST have a lifetime.

R2-4: Phase-2 KMP MUST support certificates for scalable operation.

R2-5: Phase-2 KMP message exchanges MUST be integrity and replay
protected after successful authentication.

R2-6: Phase-2 KMP MUST have the capability to establish security
association and unicast session keys after successful authentication
to protect unicast MAC frames between nodes.

R2-7: Phase-2 KMP MUST have the capability to establish security
association and broadcast session keys after successful
authentication to protect broadcast MAC frames between nodes.

R2-8: Phase-2 KMP MUST support confidentiality to distribute the
broadcast session keys securely.

[5](). Security Considerations

In this section, security issues that can potentially impact the
operation of IEEE 802.15.4e TSCH MAC are described.

In TSCH MAC, time synchronization and channel hopping information are
advertised in Enhanced Beacon (EB) frames
[I-D.ietf-6tisch-terminology]. The advertised information is used by
mesh nodes to determine the timeslots available for transmission and
reception of MAC frames. A rogue node can inject forged EB frames
and can cause replay and DoS attacks to TSCH MAC operation. To
mitigate such attacks, all EB frames MUST be integrity protected.
While it is possible to use a pre-installed static key for protecting
EB frames to every node, the static key becomes vulnerable when the
associated MAC frame counter continues to be used after the frame
counter wraps. Therefore, the 6TiSCH solution MUST provide a
mechanism by which mesh nodes can use the available time slots to run
Phase-1 and Phase-2 KMPs and provide integrity protection to EB
frames.

For use cases where certificates are used for a Phase-1 KMP, pre-
provisioning of absolute time to devices from a trustable time source
using an out-of-band (OOB) mechanism is a general requirement.
Accuracy of time depends on the OOB mechanism, including use of the
time hard-coded into the installed firmware. The less time accuracy
is, the more attack opportunities during Phase-1. In addition, use
of CRL is another requirement for Phase-1 KMP employing certificates
to avoid an attack that can happen by a compromised server or CA
certificate.

6. IANA Considerations

   There is no IANA action required for this document.

7. Acknowledgments

   We would like to thank Thomas Watteyne, Jonathan Simon, Maria Rita
   Palattella and Rene Struik for their valuable comments.

8. References

8.1. Normative References

   [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate
              Requirement Levels", BCP 14, RFC 2119, March 1997.

   [I-D.ietf-6tisch-terminology]
              Palattella, M., Thubert, P., Watteyne, T., and Q. Wang,
              "Terminology in IPv6 over the TSCH mode of IEEE
              802.15.4e", draft-ietf-6tisch-terminology-01 (work in
              progress), February 2014.

   [I-D.ietf-6tisch-architecture]
              Thubert, P., Watteyne, T., and R. Assimiti, "An
              Architecture for IPv6 over the TSCH mode of IEEE
              802.15.4e", draft-ietf-6tisch-architecture-01 (work in
              progress), February 2014.

8.2. 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.

   [ISA100]   ANSI/ISA-100.11a-2011, "Wireless systems for industrial
              automation: Process control and related applications",
              2011.

   [WirelessHART]
              IEC 62591 Ed. 1.0 b:2010, "Industrial communication
              networks - Wireless communication network and
              communication profiles - WirelessHART", 2010.

Authors' Addresses

    Stephen Chasko
    Landis+Gyr
    3000 Mill Creek Ave.
    Alpharetta, GA 30022
    USA

    Email: Stephen.Chasko@landisgyr.com

    Subir Das
    Applied Communication Sciences
    1 Telcordia Drive
    Piscataway, NJ 08854
    USA

    Email: sdas@appcomsci.com

    Rafa Marin-Lopez
    University of Murcia
    Campus de Espinardo S/N, Faculty of Computer Science
    Murcia 30100
    Spain

    Phone: +34 868 88 85 01
    Email: rafa@um.es

    Yoshihiro Ohba (editor)
    Toshiba Corporate Research and Development Center
    1 Komukai-Toshiba-cho
    Saiwai-ku, Kawasaki, Kanagawa 212-8582
    Japan

    Phone: +81 44 549 2127
    Email: yoshihiro.ohba@toshiba.co.jp

Pascal Thubert
Cisco Systems, Inc
Village d'Entreprises Green Side
400, Avenue de Roumanille
Batiment T3
Biot - Sophia Antipolis 06410
FRANCE

Phone: +33 497 23 26 34
Email: pthubert@cisco.com

Alper Yegin
Samsung
Istanbul
Turkey

Email: alper.yegin@yegin.org