IEEE Std. 802.1X as an P802.15.9 KMP

Brian Weis

Introduction

The Draft Recommended Practice for transport of key management protocol (KMP) datagrams (P802.15.9) “defines a message exchange framework ... as a transport method for key management protocol (KMP) datagrams and guidelines for the use of some existing KMPs with the IEEE Std 802.15.4 and IEEE Std 802.15.7”. A number of KMPs have been specified, and the existing Appendix A has already been reserved for a description specifying how IEEE Std 802.1X-2010 can be used as a KMP with the framework.

This document proposes descriptive text for that Appendix A. It should be noted that certain protocol elements may need additional definitions before this vision can be fully achieved.

A. KMP Specifics - 802.1X

A.1. Description

IEEE 802.1X [B5] is a port-based network access control for IEEE 802 networks. It allows network administrators to restrict the use of IEEE 802 LAN service access points (ports) to secure communication with authenticated and authorized systems. Among its several services, it provides two security services that can be passed within the Key Management Transport defined in IEEE 802.15.9:

1. Device Authentication. EAP (Extensible Authentication Protocol) [B2] is transported between a Supplicant PAE (Port Access Entity, see Clause 6.3 of [B5]) and an Authenticator PAE. Successful authentication can be accompanied by the secure delivery, to both PAEs, of a secret key that can be used to prove mutual authentication and to distribute or agree further secret keys, such as the Connectivity Association Key (CAK).

2. Cryptographic Key Agreement. The MACsec Key Agreement (MKA) protocol is used to discover other PAEs attached to the same LAN, to confirm mutual possession of a CAK and hence to prove a past mutual authentication, and to agree the secret keys used by a datagram security services. The CAK can either be derived from an EAP exchange, or pre-shared between a set of stations that are authorized to communicate between themselves.

Several policy profiles can be built using one or more of these two security services, as described in the following clauses.

A.1.1. Device Authentication

When a Wireless Personal Area Network (WPAN) network includes a network Access Point (AP) controlling access to devices on a secured network behind the AP, the AP can act as an Authenticator. The Authenticator facilitates authentication and authorization of each Supplicant (i.e., WPAN device) desiring to communicate to the secured network behind it, and discards data frames prior to the completion of the authentication process. An Authenticator PAE relies upon an Authentication Server (AS) to perform Supplicant PAE authentication and authorization. The AS may be either co-located with the Authenticator or the Authenticator may access the AS remotely via a network to which the Authenticator has access.

The Supplicant PAE and AS use EAP (Extensible Authentication Protocol) [B2] transported in EAPOL (EAP over LAN) messages. The Supplicant PAE and AS share credentials appropriate for the EAP method used for authentication. Credentials can be passwords or device identifiers (e.g., digital certificates).

A.1.2. Device Authentication and Cryptographic Key Agreement

Device Authentication does not itself provide for any protection of frames between WPAN devices themselves. However, when AS policy includes the use of an EAP method that produces a shared secret (e.g., EAP-TLS) [B6], and the Authenticator and Supplicant policy indicates that the MACsec Key Agreement (MKA) are to be initiated, then it is possible for the devices to agree upon keys and policy to provide security services (e.g., confidentiality, integrity, and replay protection) for WPAN frames.

As defined in IEEE Std. 802.1X-2010, MKA provides agreement of MACsec policy and keying material. However, it would be possible to develop definitions suitable for IEEE 802.15 standard ciphers (e.g., CCM*).

The scope of MKA can be pairwise (i.e., between the Authenticator and a single Supplicant), effectively extending the pair-wise security obtained during device authentication to WPAN frames. Alternatively, an MKA session can be shared between a set of devices, effectively providing for shared secure communications including broadcast and multicast frames.

A.1.3. Cryptographic Key Agreement with Pre-shared CAK

Some use cases will require key agreement without WPAN devices having previously executed Supplicant PAE or Authenticator PAE state machines. This is possible by pre-installing a CAK on each of the WPAN devices, and setting a policy on each device requiring that no WPAN data frames be transmitted and received WPAN data frames are discarded until MKA has obtained and installed WPAN cipher keys.

The use of a pre-shared CAK is most expedient for resource-constrained WPAN devices, however a secure method of installing and refreshing CAKs to the WPAN devices would be critical to maintaining strong security.

A.2. Use Cases

The flexibility of Device Authentication and Cryptographic Key Agreement make IEEE Std. 802.1X-2010 suitable for a variety of use cases.

A.2.1. Isolated Enclave

MKA was designed to provide Cryptographic Key Agreement services to a group (i.e., two or more) of devices that need to communicate together. An isolated enclave of WPAN devices that need to communicate amongst themselves with a mix of unicast, broadcast, and/or multicast frames could benefit from MKA's shared security model. If needed, strong authentication of group members can be first obtained using Device Authentication, when one device acts as both an Authenticator and AS. Alternatively, if strong device authentication is not required the WPAN devices can use a pre-shared CAK to establish group authorization.

A.2.2. Star Topology

A network topology where a set of WPAN devices communicate privately with a PAN Coordinator would benefit from pair-wise Cryptographic Key Agreement services. The Controller may use Device Authentication to strongly authenticate the WPAN devices, or may depend on a pre-shared pair-wise CAK in order to guarantee keying material is shared only with the expected WPAN device.

A.2.3. Mesh

If a mesh of WPAN devices comprises more than one broadcast domain, then each WPAN needs be considered an individual Isolated Enclave or Star.

A.3. 802.15 Specifics

A.3.1. EAPOL Message Framing

IEEE 802.1X-2010 messages are specified as being carried in EAPOL PDUs. When carried in a KMP Information Element, the EAPOL PDU (beginning with the Protocol Version field) follows the KMP ID value (1) in the first KMP Fragment.

A.3.2. EAPOL-MKA

Several modifications are necessary to the semantics and parameter sets within EAPOL-MKA messages.

ICV Calculation

An Integrity Check Value (ICV) is calculated using AES-CMAC, with the bytes being MACed defined as follows:

M = DA + SA + (MSDU – ICV)

where DA and SA refer to the Destination and Source Addresses respectively, MSDU is the message (beginning with the Ethertype). When an EAPOL-MKA message is passed in an KMP Information Element, M is defined as follows:

M = DA + SA + (EAPOL - ICV)

where

- DA is the Destination Address used to deliver the EAPOL-MKA message (of either type *macCoordExtendedAddress* or *macShortAddress*).
- SA is the Source Address used to deliver the EAPOL-MKA message (of either type *macCoordExtendedAddress* or *macShortAddress*).
- EAPOL is the full message
- ICV is the bytes of the EAPOL message comprising the ICV

Note that the KMP Information Element bytes cannot be protected because the EAPOL-MKA is reassembled before being validated.

MKA Basic Parameter Set

The fields MACsec Desired and MACsec Capability are used to mean “WPAN Security Desired” and “WPAN Security Capability”.

The SCI field is taken to be the *macCoordExtendedAddress* of the sender.

MACsec SAK Use Parameter Set

The following fields have unique semantics when delivered in an KMP Information Element.

- Latest Key AN is the KeyIndex. Note that the size of KeyIndex is effectively reduced to 0x00-0x11.
- Old Key AN, Old Key tx, Old Key rx are unused.

- Delay protect is unused.
- Latest Key Lowest Acceptable PN and Old Key Lowest Acceptable PN are unused.

Distributed SAK Parameter Set

The following fields have unique semantics when delivered in an KMP Information Element.

- Distributed AN is the KeyIndex in the range of 0x00-0x11.
- Offset Confidentiality is unused.
- MACsec Cipher Suite is taken to mean "WPAN Cipher Suite". A new cipher suite (OUI + assigned reference number) needs to be allocated for CCM* as defined in the WPAN standards.

MKA State Machine - Suspension

MKA requires each station to emit an MKA frame at least every two seconds, which may not be possible in all Use Cases. In particular, when devices are battery powered this will provide an unwelcome drain on the battery. Also when the WPAN includes a Coordinator, messages may only be sent during the active portion of a superframe (IEEE Std 802.15.4-2011, Clause 4.5.1).

The MKA suspension semantics defined in P802.1Xbx intended for Managing in-service upgrades may be useful here as well. To ensure the MKA Live Peer List is not cleared when devices are asleep, the MKA Suspension Limit should be reset from 120 seconds to a value that is more appropriate for the WPAN networks use case (likely a much larger value).

MKA State Machine - Key Server Selection

When a WLAN includes a PAN Coordinator (e.g., in a Star Topology), the PAN Coordinator should be the key server for the group. A PAN Coordinator is required to be a full functioned device (FFD) (Clause 3 .1 of IEEE Std. 802.15.4), and it must also have the capability to generate high quality keying material.

Normative References

The following existing P802.15.9/D01 normative references are used in this document:

[B2] Extensible Authentication Protocol (EAP), RFC 3748.

The following normative references are added to P802.15.9/D01.

[B5] IEEE Std 802.1X-2010, IEEE Standard for Local and Metropolitan Area Networks: Port-based Network Access Control.

[B6] The EAP-TLS Authentication Protocol, RFC 5216.