IEEE P802.11
Wireless LANs

|  |
| --- |
| Some editorial CIDs |
| Date: 2019-11-12 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Jerome Henry | Cisco |  |  | jerhenry@cisco.com |

Abstract

This document presents resolutions to several editorial CIDs: 1942, 1993, and 1999.

Change request refer to D1.5 paging and structure.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1942 | 137.12 | 12 | 12.2.11 | "The Info field is a fixed string unique to this protocol: For example: "IEEE 802.11az ranging"" -- it shouldn't be an example, and it should have sexy quotes on both sides | Change to "The Info field is "IEEE 802.11az ranging" without a trailing null" with both the double quotes being sexy | **Revised** . |

Discussion:

RFC 5869 section 2 describes how the HMAC-based key is derived. In the ‘expand’ phase, the optional info field can be used. As per RC 5869 3.2:

 “While the 'info' value is optional in the definition of HKDF, it is

 often of great importance in applications. Its main objective is to

 bind the derived key material to application- and context-specific

 information. For example, 'info' may contain a protocol number,

 algorithm identifiers, user identities, etc. In particular, it may

 prevent the derivation of the same keying material for different

 contexts (when the same input key material (IKM) is used in such

 different contexts). It may also accommodate additional inputs to

 the key expansion part, if so desired (e.g., an application may want

 to bind the key material to its length L, thus making L part of the

 'info' field). There is one technical requirement from 'info': it

 should be independent of the input key material value IKM.

As such, if the info field is used, it has to contain information that is clearly identified as representing 802.11az. Thus the value we design here should not be an example, but a fixed value that implementers will use to recognize 802.11az (on both sides).

CID 1455 made a comment in that direction, however D1.2 implements the following change:

*The Info field is a fixed string unique to this protocolin order to guard against accidental key re-use in a different subsystem. Key reuse across different subsystems must be avoided through careful system architecture, Secret Key must not be visible outside of the subsystem. See RFC5869, Section 2.3 for Info field.*

Such change is only partly satisfactory, as it resolves the problem by hiding it, thus leaving to implementers (or other organisations like WFA) the task of choosing the info value. As we define the other elements of the protocol, it might be valuable to also define the value of this field. There is no repository of RFC 5869 info fields, however it is reasonable to assess that no one has used any value yet within the PEDMG Secure ranging exchange.

***TGaz Editor: Change paragraph of 12.2.11 P166L18-21 as follows:***

The Info field is “IEEE 802.11az ranging” in order to guard against accidental key re-use in a different subsystem. Key reuse across different subsystems must be avoided through careful system architecture, Secret Key must not be visible outside of the subsystem. See RFC5869, Section 2.3 for Info field.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1993 | 59 |  |  | Duplication is bad, m'kay? | Delete "is one octet wide and " at 59.4/8 (and change "indicate" to "indicates") and "is four Bits wide and " at 59.15 | Revised |

Discussion:

The field size is described in the figure above. We do not usually tell the size of a field when it is already known.

***TGaz Editor: Modify the text in 9.4.2.279 P73L6to16:***

The MinTimeBetweenMeasurements field is requested by the ISTA in the IFTMR frame and assigned by RSTA in the IFTM frame which indicate the minimum time between two consecutive range measurements initiated by an ISTA, in units of 100 microseconds.

The MaxTimeBetweenMeasurements field is requested by the ISTA in the IFTMR frame and assigned by RSTA in the IFTM frame, which indicates the latest time that the ISTA completes the next round of measurement, in units of 10 millisecond. The TB Specific subelement is included in the initial Fine Timing Measurement Request to describe the requested set of parameters that the initiator proposes to use and in the initial Fine Timing Measurement, if the initiator and the responder successfully negotiate and Fine Timing Measurement session where the negotiated ranging protocol is TB.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1999 | 11.22.6.1.2 | "may not" is ambiguous | Change to "is not required to" | **Revised** |

***TGaz Editor: Change the paragraph in 11.22.6.1.2 P107L14-18 and P108L1-4 as follows***

In Non-TB ranging measurement exchange the ISTA determines the measurement timing, based on its scheduling conflicts with other activities and the parameters of the availability window which is a time window referenced to the previous measurement instance. During this measurement time window the ISTA may come to the channel at any time and use contention based access to initiate a new measurement exchange. Because of conflict arising due to other activities, it happens that the ISTA does not start measurement at start of availability window while the RSTA waits for the start of measurement phase. Dotted region in Figure 11-35a indicates that the non-TB measurement exchange phase does not always start at the beginning of the time window since the ISTA may have been active on another channel.

**References:**

[1] Draft P802.11azD1.5