IEEE P802.11
Wireless LANs

|  |
| --- |
| LB240-Secure-EDMG-FTM-CIDs |
| Date: 2019-10-03 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Assaf Kasher | Qualcomm | 6 Nahum Het St., Haifa Israel |  | akasher@qti.qualcomm.com |
| Nehru Bhandaru | Broadcom Inc. | 250 Innovation Drive, San Jose CA 95134 USA | 408-391-2159 | nehru.bhandaru@broadcom.com |

Abstract

This document proposes resolution to CIDs 1454, 1455, 1456 on TGaz D1.0.

The correction are based on D1.5

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 1454 | 104.04 | 4 | 12.2.9 | first 32 octets of the "Secret Key" are an encryption key for CCMP. What's the IV/Counter and how is uniqueness guaranteed? | define how CCMP is used properly | Revise as in 11-19-1785 |
| 1455 | 104.24 | 24 | 12.2.9 | the info field must be fixed to ensure interoperability | you can't leave it up to for example, fix it to something. | Revise as in 11-19-1785 |
| 1456 | 104.00 |  | 12.2.9 | what's the length of this Secure TRN Sequence | see comment | Revise as in 11-19-1785 |
| 1450 | 33.45 |  | 9.4.2.166 | how is the secret key generated? | explain where this secret comes from | Revise as in 11-19-1785 |
| 1089 | 51.01 |  | 9.4.2.167 | It is not clear how the Secret Key is derivated on both sides of the link | Add text to explain | Revise as in 11-19-1785 – the explanation is in 12.2.11 |

***TGaz Editor: Change the text in 12.2.11 (P165L30-37), (P166L1-31)***

PEDMG Secure Ranging uses Secure TRN subfields (see 29.9.3) as part of the TRN fields of EDMG PPDUs. Those TRN subfields are based on bit sequences henceforth denoted as Secure TRN Sequences. These Secure TRN bit Sequences are generated as follows:

.

The Secret Key is 32 octets randomly generated by the ISTA and sent in the Secure Ranging Operation Parameters field (see Figure 9-619e Ranging Operation Parameters field format) of the PEDMG Specific Parameters subelement of the Fine Timing Parameters element sent by the ISTA to the RSTA in the initial Protected Fine Timing Measurement request. (see 11.22.6.3.5 EDMG Secure ToF Measurement Setup). The Secret Key is used as Input Key Material (IKM) to generate pseudo-random Secure TRN Sequences that are used to construct secure ranging waveforms at the I-STA and R-STA respectively.

The Secret Key shall be discarded after the FTM session is terminated. Each FTM session shall have a different Secret Key.

Pseudo-random Secure TRN Sequences are generated using HKDF (Hashed Message Authentication Code (HMAC)-based Key Derivation Function) specified in IETF RFC5869 (https://tools.ietf.org/html/rfc5869)

The hash function to be employed in HKDF is SHA-256.

The Secret Key is used as the IKM in HKDF. See RFC5869 section 2.2 for IKM.

The Salt is the PMKID corresponding to the security association between the ISTA and RSTA. See RFC5869, section 2.2 for Salt.

A pseudo-random key (PRK) is generated using the hash function accepting IKM and salt as inputs. See RFC5869 section 2.2.

The Info field is the fixed string ”PEDMG Secure ToF”. Key reuse across different subsystems must be avoided through carefull system architecture, Secret Key must not be visible outside of the subsystem. See RFC5869, subclause 2.3 for Info field.

Pseudo-random Secure TRN Sequences are the output of the HKDF-Expand function with PRK, Info field and the length of Secure TRN Sequences required as inputs . See RFC5869, section 2.3.

One-time calculation of all pseudo-random Secure TRN Sequences for multiple timing measurements should be used for minimizing HKDF set-up costs in case of multiple ranging attempts. The length of the Secure TRN seqeuences generated shall be long enough for generating Secure TRN subfields for the number of bursts expected in the session.

Furthermore, if memory is not constrained in an implementation, caching multiple Secret Keys and pre-generating all Secure TRN Sequences for multiple timing measurements and multiple FTM sessions is allowed provided that this information is not revealed to third parties.

***TGaz Editor: Change the text in 11.22.6.3.5 (P120L32-39)***

An ISTA may request a Secure ToF measurement by setting the Secure ToF Measurement subfield in the Measurement Parameters field in the initial **(#1449)** Protected Dual of the Fine Timing Measurement Request frame. An ISTA shall not set the Secure ToF Measurement subfield in a request to an RSTA if the RSTA has not set the Secure ToF Supported field in the EDMG Capabilities field to 1. The ISTA shall generate a 32 bit random Secret Key and a 32 bit salt key and include them in the Secure Ranging Operation Parameters field (see Figure 9-619e Ranging Operation Parameters field format) in the initial Protected Dual of the Fine Timing Measurement Request frame An RSTA that supports Secure ToF measurement shall acknowledge a request for Secure ToF measurement by setting the Secure ToF Measurement subfield in the Measurement Parameters field in the initial (#1449) Protected Dual of the Fine Timing Measurement frame.

***TGaz Editor: Change the text in* 11.22.6.4.2.1.6  *P127L25-30 and P128L1-8:***

* The Protected dual of the Fine Timing Measurement Request frame shall be used by the ISTA to initiate the exchange
* The ISTA shall use the Protected dual of the Fine Timing Measurement frame during the exchange.
* The PPDUs carrying the Protected Dual of Fine Timing Measurement frames transmitted by the RSTA and the Acks transmitted by the ISTA shall be based on the format as described in subclause 29.9.3. In these PPDUs, the SECURED\_TRN parameter of the TXVECTOR shall be set to SECURED\_TRN.

— The PPDU carrying the protectd dual of FTM frames transmitted by the responder to initiator shall use the first path AWVs obtained during first path beamforming training as described in 10.43.10.6 First Path Beamforming Training

— The PPDU carrying the Ack frame transmitted by the initiator to the responder shall use the first path AWVs obtained during first path beamforming training as described in 10.43.10.6 First Path Beamforming Training

— If the Ack frame for FTM frame is not received, the RSTA may retransmit the FTM frame. In this case, the RSTA shall send an FTM frame with the same Action frame body as the Fine Timing Measurement frame for which the Ack was not received, except for updating the Dialog Token if it was nonzero, and a new Secure TRN Sequence shall be used. The Sequence Number in the MAC header is also updated.

***TGaz Editor: in Figure 9-619c (PEDMG Specific Parameter subelement format), change the numb er below*** Secure Ranging Parameter ***to*** 64

***TGaz Editor: in Figure 9-619e (Secure Ranging Operation Parameters field format) change the number below*** Secret Key ***to*** 32

**References:**

**Draft P802.11az\_D1.5**