IEEE P802.11
Wireless LANs

|  |
| --- |
| Resolution of CID 3940 |
| Date: 2020-05-21 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Solomon Trainin | Qualcomm |  |  | strainin@qti.qualcomm.com |
| Alecsander Eitan | Qualcomm |  |  | eitana@qti.qualcomm.com |
| Assaf Kasher | Qualcomm |  |  | akasher@qti.qualcomm.com |

Abstract

Resolution of CID 3940

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Line** | **Sub-clause** | **Comment** | **Proposed change** | **Resolution** |
| 3940 | 68.00 | 6 | 9.4.2.250.2 | The Secure Time of Flight is part of the management frame protection that any part of the related frame exchanges shall be protected. However, the capability "Secure ToF Supported" is defined as part of the EDMG Capabilities element that can be delivered in unprotected frame exchanges exposed to the "man in the middle" attack. The capability shall be moved to the RSN extension element to be protected. | Move the Secure ToF capability to the RSN extension - 9.4.2.241 RSN Extension element (RSNXE) | **Revised** See below in the document |

Discussion:

The PHY security features of the secure ToF and the secure LTF are provided under the protection of the Management frames. At the establishment of the FTM session, the actual use of the secure ToF and the secure LTF is protected by the exchange of the encrypted Fine Timing Measurement frames of the Protected Dual of Public Action category.

At the same time the capabilities responsible to negotiate these features: Secure LTF Support, and Secure ToF Supported, are delivered in the Extended Capabilities element and in the EDMG Capabilities element respectively. The elements are not protected; thus, the negotiation is defenceless against the man-in-the-middle downgrade attack.

Indication of the capability of “Protection of Range Negotiation and Measurement Management Frames Required” while associated is a duplication of the MFPR hence it is not needed. The capability is relevant for pre-association. The “Protection of Range Negotiation and Measurement Management Frames Required” is delivered in the Extended Capabilities element that is not applicable to DMG stations, propose to move the capability to RSNXE to unify signalling and protection

Following changes are proposed to be implemented in the text of the draft:

Keep the capability of “Protection of Range Negotiation and Measurement Management Frames Required” for pre-association. and require the STA to set this bit to 1 when dot11RSNAProtectedManagementFramesActivated is true to advertise that protection of robust Management frames is required while pre-associated.

Enable protection of the Protection of Range Negotiation and Measurement Management Frames Required, Secure LTF Support, and Secure ToF Supported capabilities by moving them to the RSN extension element (RSNXE).

**TGaz editor, make the following changes**

**9.4.2.241 RSN Extension element (RSNXE)**

**Append rows to Table 9-321—Extended RSN Capabilities field**

|  |  |  |
| --- | --- | --- |
| **Bit** | **Information** | **Notes** |
| <ANA> | Secure LTF Support  | A STA sets the Secure LTF Support field to 1 when dot11SecureLTFImplemented is true. Otherwise, the STA sets the Secure LTF Support field to 0. See 11.22.6.4.6 (Secure LTF Measurement Exchange Protocol)  |
| <ANA> | Secure ToF Supported | A STA sets the Secure ToF Supported field to 1 if it supports Secure Time of Flight (ToF) Measurement exchange as defined in 11.22.6.4.8 (Secure EDMG Measurement Exchange Protocol). |
| <ANA> | Protection of Range Negotiation and Measurement Management Frames Required | A STA sets the Protection of Range Measurement Management Frames Required field to 1 if dot11RSTARequiresPMFActivated is true. Otherwise the STA sets the Protection of Range Measurement Management Frames Required field to 0. See 11.22.6.3.1 (General)  |

**9.4.2.26 Extended Capabilities element**

***On P58, Table 9-153—Extended Capabilities element (#1295) remove the row***



***On P58, Table 9-153—Extended Capabilities element (#1295) remove the row***



**9.4.2.250.2 Beamforming Capability subelement**

***P68, Figure 9-787ap—Data field of the Beamforming Capability subelement format***

***Under B20, replace*** *“*Secure ToF Supported” by “Reserved”

***P68L8***

***Remove paragraph that starts with*** “A STA sets the Secure ToF Supported field…”

**11.22.6.2 FTM capabilities**

***P114L22***

***Change as follows***

A STA in which dot11SecureLTFImplemented is true shall set the Secure LTF Support field of the RSNXE to 1. Otherwise, it shall set the Secure LTF Support field to 0.

***P L11425***

***Change as follows***

…the Protection of Range Negotiation and Measurement Management Frames Required field of the RSNXEto 1

***P114L43***

***Replace*** *“*EDMG capabilities element” by RSNXE

**11.22.6.3.1 General**

***P116L6***

If the ISTA and the RSTA are associated, the security context is established as defined in (12.6.19 Protection of Robust Management Frames, and 12.6.20 Robust management frame selection procedure).

NOTE-The MFPC and MFPR capabilities defines if the security context between RSTA and ISTA is established or not.

If the ISTA and the RSTA are not associated the is established as defined in and conditions to establish the context are defined below.

Prior to initiating a Fine Timing Measurement Procedure Negotiation for a Trigger-Based session, non-Trigger-Based session or a Fine Timing Measurement session using Format and Bandwidth in the range 31 through 41, with an RSTA if the RSTA has the Protection of Range Negotiation and Measurement Management Frames Required field in the RSNXE to 1, ISTA shall establish a security context with the RSTA.

An RSTA shall reject a request, unless the request is for Passive TB Ranging, if it has set the Protection of Range Negotiation and Measurement Management Frames Required field of the RSNXE to 1, and the ISTA has not successfully set up a security context to protect IFTMR, IFTM and LMR frames exchanged between the RSTA and the ISTA.

An ISTA initiating a Fine Timing Measurement Procedure Negotiation for a Trigger-Based session, non-Trigger-Based session or a Fine Timing Measurement session using Format and Bandwidth in the range 31 through 41, with an RSTA if the RSTA has the Protection of Range Negotiation and Measurement Management Frames Required field in the RSNXE to 0 may establish a security context with the RSTA based on its operating policy setting.

A Secure Fine Timing Measurement Session is established when an ISTA and a RSTA establish a security context and use it to exchange the initial Fine Timing Measurement Request frame and the corresponding initial Fine Timing Measurement frame in the Protected Dual of Public Action frame format (see Cl. 9.6.10 Protect Dual of Public Action frames) and the negotiation completes successfully.

**11.22.6.3.3 Negotiation for TB and non-TB ranging measurement exchange**

***P120L13***

***Move the paragraph that starts with “An RSTA shall reject a request, unless …” to the subclause 11.22.6.3.1 General***

***P123L29***

When an RSTA has set the Secure LTF Support field to 1 in the RSNXE,

**11.22.6.3.4 Negotiation for Secure LTF in the TB and Non-TB Ranging measurement exchange (#1817, #1818, #1824, #2321)**

***P123L25***

***Change as follows***

An RSTA in which dot11SecureLTFImplemented is true shall set the Secure LTF Support field in the RSNXE to 1.

**11.22.6.3.5 Negotiation for Secure EDMG TRN in EDCA based Ranging measurement exchange**

***P124L33***

***Replace*** *“*EDMG capabilities element” by RSNXE

**11.22.6.3.5 Negotiation for Secure EDMG TRN in EDCA based Ranging measurement exchange**

***P125L3***

***Replace*** *“*EDMG capabilities element” by RSNXE

**11.22.6.3.6 Direction measurement negotiation for DMG STAs**

***P125L42***

***Replace*** *“*EDMG capabilities element” by RSNXE

**12.6.1.1.6 PTKSA**

***P178L29***

HLTK shall be derived if dot11SecureLTFImplemented is true and the peer STA has indicated Secure LTF Support capability in its advertised RSNXE.

**12.7.1.6.5 PTK**

**P180L17**

HLTK shall be derived if dot11SecureLTFImplemented is true and the peer STA has indicated Secure LTF Support capability in its advertised RSNXE.

**12.12.2.5.3 PTKSA Key derivation with FILS authentication**

***P181L24***

HLTK shall be derived if dot11SecureLTFImplemented is true and the peer STA has indicated Secure LTF Support capability in its advertised RSNXE.

**12.13.7 PTKSA derivation with PASN authentication**

***P193L22***

HLTK shall be derived if dot11SecureLTFImplemented is true and the peer STA has indicated Secure LTF Support capability in its advertised RSNXE.

**C. 3 MIB detail**

***P229L31***

***Change as follows***

For the pre-association ranging this attribute, when true, indicates that the station requires …

***P229L38***

For the pre-association ranging False indicates that the station does not require …

**References:**

1. Draft P802.11az\_D2.0
2. Draft P802.11REVmd\_D3.2