IEEE P802.11
Wireless LANs

|  |
| --- |
| Putting TKIP in Its Place |
| Date: 2022-02-16 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE |  |  |  |
|  |  |  |  |  |

Abstract

This submission resolves several CIDs—1076, 1077, and 1079—that all advise that references to TKIP be removed from RSN sections and be dealt with as a non-RSN mode.

**CID 1077**

Comment: put TKIP with WEP in a non-RSNA section.

Proposed Change: Title 12.3 as “Non-RSNA security methods” and then move 12.5.2 into that section.

Discussion: TKIP is really not an RSNA. It’s used in a TSN where the pairwise cipher is TKIP and the group cipher is WEP, so this CID is a bit more expansive than it proposes. WEP is deprecated, so we should probably not talk about TSNs in the RSN security association management section.

In addition to doing what the CID proposes, it is also proposed to move discussion of TSN policy selection from 12.6 into the newly revised 12.3.

Resolution:

*Instruct the editor to modify section 12.3 as indicated:*

**12.3 Non-RSNA security methods**

**12.3.1 Overview**

Non-RSNA security methods consist of pre-RSNA security mechanisms and TSN security mechanisms.

Except for Open System authentication, all pre-RSNA security mechanisms are obsolete. Support for them might be removed in a later revision of the standard. TSN security mechanisms are deprecated.

Open System authentication shall not be used between mesh STAs.

*Further instruct the editor to move 12.5.2 to a new section 12.3.4, renumbering 12.5 as required.*

**CID 1076**

Comment: TKIP is not an RSNA protocol

Proposed Change: remove mention of TKIP as an RSNA, remove the paragraph on lines 15-18 too.

Discussion: TKIP is deprecated so the paragraph talking about it being optional for an RSNA is obviously dated.

Resolution: Accept

*Instruct the editor to further modify section 12.5 as indicated:*

**12.5 RSNA confidentiality and integrity protocols**

**12.5.1 Overview**

This standard defines the following RSNA data confidentiality and integrity protocols: CCMP, and GCMP. This standard defines the following integrity protocol for Management frames and for WUR Wake-up frames: BIP.

BIP is a mechanism that is used only when management frame protection is negotiated. BIP provides integrity protection for group addressed robust Management frames and WUR Wake-up frames (see 29.10 (WUR frame protection)).

**CID 1079**

Comment: let's stop talking about how to use WEP and TKIP

Proposed Change: remove the paragraphs on the pages and lines this comment refers to.

Discussion: WEP is obsoleted, TKIP is deprecated. We should stop talking about how to use them because we are telling people they should not be used. If we remove the discussion about “no pairwise” in the paragraphs and lines this comment refers to, we should also remove all other mentions of “no pairwise” since that is for a TSN.

Resolution: Revised….

*Instruct the editor to modify section 9.4.2.24.4 as indicated:*

**9.4.2.24.4 RSN capabilities**

The RSN Capabilities field indicates requested or advertised capabilities. If the RSN Capabilities field is not present, the default value of 0 is used for all of the capability subfields.

The length of the RSN Capabilities field is 2 octets. The format of the RSN Capabilities field is as shown in Figure 9-350 (RSN Capabilities field format) and described after the figure.

 B0 B1 B2 B3 B4 B5 B6 B7

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Preauthentication | Reserved  | PTKSA Replay Counter | GTKSA Replay Counter | MFPR | MFPC |

 Bits: 1 1 2 2 1 1

Bit 1: This bit is reserved, it is set to 0 on transmission and ignored on receipt.

*Instruct the editor to modify section 12.7.1.1 as indicated:*

**12.7.1 Key hierarchy**

**12.7.1.1 General**

An RSNA STA shall support at least one pairwise key for any <TA,RA> pair for use with enhanced data cryptographic encapsulation mechanisms. The <TA,RA> identifies the pairwise key, which does not correspond to any WEP key identifier.

*Instruct editor to modofy section 12.7.6.4.4 as indicated:*

**12.7.6.4.4 4-way handshake message 3**

Message 3 uses the following values for each of the EAPOL-Key frame fields:

 Descriptor Type = N – see 12.7.2 (EAPOL-Key frames)

 Key Information:

 Key Descriptor Version = 1 (ARC4 encryption with HMAC-MD5) or 2 (NIST AES key wrap with HMAC-SHA-1-128) or 3 (NIST AES key wrap with AES-128-CMAC), in all other cases 0 – same as message 1

 Key Type = 1 (Pairwise) – same as message 1

 Reserved = 0

 Install = 0/1 – For PTK generation, 0 only if the AP does not support key mapping keys.

 Key Ack = 1

 Key MIC = 0 when using an AEAD cipher or 1 otherwise

*Instruct editor to modify section 12.7.4 as indicated:*

**12.7.4 EAPOL-Key frame notation**

{Key Data} is a sequence of zero or more elements and KDEs, concatenated and contained in the Key Data field, where

 RSNE is described in 9.4.2.24 (RSNE)

 RSNE[KeyName] is the RSNE, with the PMKID List field set to KeyName

 GTK[N] is the GTK, with the key identifier field set to N (The key identifier specifies

 which index is used for this GTK. Index 0 shall not be used for GTKs.)

 FTE is the Fast BSS Transition

*Instruct editor to modify section 12.7.8.4.2 as indicated:*

**12.7.8.4.2 TPK handshake message 1**

If security is required on the TDLS direct link (see 12.7.8.1 (General)), the TDLS initiator STA shall add an RSNE, FTE, and Timeout Interval element to its TDLS Setup Request frame. The elements shall be formatted as follows:

 The RSNE, if present, shall be set as follows:

 Version shall be set to 1.

 The pairwise cipher suite list field indicating the pairwise cipher suites the TDLS initiator STA

 is willing to use with the TPKSA. WEP-40, WEP-104, and TKIP shall not be included in

 this list.

 The group cipher suite shall be set to 00-0F-AC:7.

 The AKM suite count field shall be set to 1.

 The AKM suite list field shall be set to indicate TPK handshake (00-0F-AC:7).

 In the RSN Capabilities field, the PeerKey

 Enabled subfield shall be set to 1.

 PMKID Count subfield, if present, shall be set to 0.

 PMKID list shall not be present.

 The Group Management Cipher

**References:**