IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Assorted CRs on REVmd draft 3.0 | | | | |
| Date: January 28, 2020 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Nehru Bhandaru | Broadcom | 250 Innovation Drive, San Jose CA | +1 408 391 2159 | [nehru.bhandaru@broadcom.com](mailto:nehru.bhandaru@broadcom.com) |
| Mike Montemurro | Blackberry |  |  | [montemurro.michael@gmail.com](mailto:montemurro.michael@gmail.com) |

Abstract

This document contains proposed resolutions for following CIDs against REVmd draft 3.0:

4031, 4032, 4033, 4086, 4087, 4088, 4089, 4090, 4091, 4092, 4093, 4188, 4204,

4230, 4308, ~~4326~~, 4388, 4417, 4465, 4522, 4602, 4612, 4672, 4728

The baseline for this document is Draft P802.11REVmd D3.0.

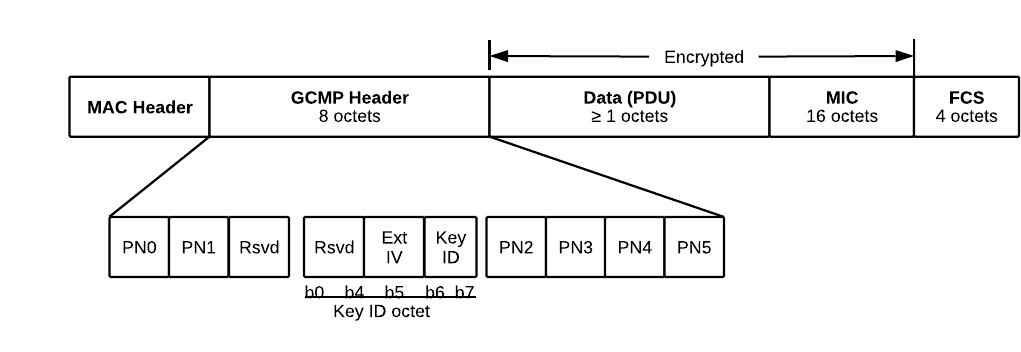
|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Clause Number** | **Page** | **Line** | **Comment** | **Proposed Change** | **Resolution** |
| 4031 | 12.5.3.3.2 | 2603 | 49 | dot11PNExhaustionThreshold has been changed to dot11PNExhaustionThresholdLow and dot11PNExhaustionThresholdHigh. | Fix dot11PNExhaustionThreshold to dot11PNExhaustionThresholdLow and dot11PNExhaustionThresholdHigh. | Accept.  TGm Editor: Change the sentence as follows  (#2500)If the PN is ~~larger than dot11PNExhaustionThreshold~~ not within thresholds defined in dot11PNExhaustionThresholdLow and dot11PNExhaustionThresholdHigh , ~~an~~ a MLME-PN-EXHAUSTION.indication  primitive shall be generated. |
| 4032 | 12.5.4.4 | 2612 | 27 | dot11PNExhaustionThreshold has been changed to dot11PNExhaustionThresholdLow and dot11PNExhaustionThresholdHigh. | Fix dot11PNExhaustionThreshold to dot11PNExhaustionThresholdLow and dot11PNExhaustionThresholdHigh. | Accept.  TGm Editor: Change the sentence as follows  (#2500)If the PN is ~~larger than dot11PNExhaustionThreshold~~ not within thresholds defined in dot11PNExhaustionThresholdLow and dot11PNExhaustionThresholdHigh , ~~an~~ a MLME-PN-EXHAUSTION.indication  primitive shall be generated. |
| 4033 | 12.5.5.3.2 | 2616 | 31 | dot11PNExhaustionThreshold has been changed to dot11PNExhaustionThresholdLow and dot11PNExhaustionThresholdHigh. | Fix dot11PNExhaustionThreshold to dot11PNExhaustionThresholdLow and dot11PNExhaustionThresholdHigh. | Accept.  TGm Editor: Change the sentence as follows  (#2500)If the PN is ~~larger than dot11PNExhaustionThreshold~~ not within thresholds defined in dot11PNExhaustionThresholdLow and dot11PNExhaustionThresholdHigh , ~~an~~ a MLME-PN-EXHAUSTION.indication  primitive shall be generated. |
| 4086 | 12.5.3.3.2 | 2603 | 46 | "For PV1 MPDUs, the PN shall never repeat for a series of encrypted MPDUs using the same temporal key and TID/ACI." The above implies that the PN are allowed to be repeated for the same Key if the TID/ACI is different. This appears to violates the rule that the same PN shall never be reused for the same key. Refer to 12.5.3.1 General (P2601L14) which states that reuse of a PN with the same temporal key voids all security guarantees. | Review whether encrpytion of PV1 MPDUs violates the rule that the same PN shall never be reused for the same key. If it does, ensure that the same PN is never resued for the same key for PV1 MPDUs as well regardless of the TID/ACI. | Reject.  Suggested action not specific enough.  However, in the construction of CCM Nonce, TID/ACI (Priority) is used in Nonce Flags (12.5.3.3.4 Construct CCM Nonce). That ensures that the CCM counter used for encryption is unique across TIDs and preserves security guarantees. |
| 4087 | 12.5.3.4.1 | 2608 | 25 | As per 12.5.3.3 (P2607L59), the MIC is also encrypted along with the plaintext MPDU, so it is not possible to obtain the original MIC at this stage. The original MIC can only be obtained after CCM decryption stage. The figure 12-23 is misleading, either it should be clarified that the MIC that is fed into the CCM decryption block is encrypted MIC, or the entire encrypted MPDU (instead of MIC and data) should be passed to the CCM decryption block. | Rectify the Figure 12-23 as per comment. Specifically, the MIC that is fed into the CCM decryption module should be "encrypted MIC" | Accept. It coukd be made clearer that MIC is the cncrypted MIC.  TGm Editor: replace the workd ‘MIC’ in Figure 12-23 with ‘Encrypted MIC’ |
| 4088 | 12.5.3.4.1 | 2608 | 50 | As per 12.5.3.3 (P2607L59), the MIC is also encrypted along with the plaintext MPDU, so it is not possible to obtain the original MIC at this stage. The original MIC can only be obtained after CCM decryption stage. The text "The MIC is extracted..." is misleading, at this stage this is encrypted MIC, the original MIC can only be obtained after passing through the CCM decryption block. | Reword to convey that the MIC that is used in the CCM integrity checking is only obtained after decryption of the encrypted MIC. | Accept.  TGm Editor: Replace  “The MIC is extracted for use in the CCM integrity checking”  with  “The Encrypted MIC is extracted for use in ~~the~~ CCM decryption that includes integrity checking” |
| 4089 | 12.5.3.4.1 | 2609 | 8 | As per 12.5.3.3 (P2607L59), the MIC is also encrypted along with the plaintext MPDU, so it is not possible to obtain the original MIC at this stage. The original MIC can only be obtained after CCM decryption stage. The text "The MIC is extracted..." is misleading, at this stage this is encrypted MIC, the original MIC can only be obtained after passing through the CCM decryption block. | Reword to convey that the MIC that is used in the CCM integrity checking is only obtained after decryption of the encrypted MIC. | Accept.  TGm Editor: Replace  “The MIC is extracted for use in the CCM integrity checking”  with  “The Encrypted MIC is extracted for use in the CCM decryption that includes integrity checking” |
| 4090 | 12.5.3.4.2 | 2609 | 50 | "CCM recipient processing checks the authentication and integrity of the frame body and the AAD as well as decrypting the frame body. The plaintext is returned only if the MIC check is successful." The above sentence is not clear at best, or is not accurate. The authentication and integrity check can only be performed once the original MIC has been decrypted. It should be explained that the decryption should happen first to obtain the plaintext MPDU and the original MIC. The MIC needs to be re-calculated over the plaintext MPDU following the procedure in 12.5.3.3 and compared with the decrypted MIC to verify that the MIC is correct. | Clarify that decryption should happen first to obtain the plaintext MPDU and the original MIC. The MIC needs to be re-calculated over the plaintext MPDU following the procedure in 12.5.3.3 and compared with the decrypted MIC to verify that the MIC is correct. | Revise.  The processing is described clearly in base CCM specifications (IETF RFC 3610). It probably suffices to say here that plaintext is returned if the checks are successful.  TGm Editor: Change as follows  CCM recipient processing checks the authentication and integrity of the frame body and the AAD as well as decrypting the frame body. The plaintext is returned only if the ~~MIC check is~~ checks are successful. |
| 4091 | 12.5.3.4.3 | 2609 | 61 | "The decapsulation process succeeds when the calculated MIC matches the MIC value obtained from decrypting the received encrypted MPDU." It should be elaborated clearly how the MIC is calculated for the MIC check. | Clarify how the MIC is calculated for the MIC check. | Revise.  A reference to CCM spec might help.  TGm Editor: Change as follows  “The decapsulation process succeeds when the calculated MIC matches the MIC value obtained from decrypting the received encrypted MPDU (See IETF RFC 3610)” |
| 4092 | 12.5.4.4 | 2612 | 1 | What field is this (MME Sequence Number)? this seems to be the only occurrence. Is it supposed to be the IPN/BIPN field? | Use the correct field name. | Revise.  This sentence seems redundant since later in the section it is specified to insert the IPN/BIPN etc. into the sequence number field of the MME (Management MIC Element). Remove this sentence,  TGm Edtior: Change as follows  ~~The MME Sequence Number field represents a sequence number whose length is 6 octets.~~ |
| 4093 | 12.5.5.2 | 2615 | 7 | Figure 12-26: In GCMP isn't MIC also encrypted? P2617L25 mentions that it is. The figure should be amended showing MIC as encrypted. | Amend Figure 12-26 to show MIC as encrypted. | Revise.  TGm Editor change figure as per 11-20-xxxxr0. |
| 4188 | 12.4.5.4 | 2574 | 14 | "a salt is passed to the KDF consisting of " is not using the normative form used in surrounding sentences | Change the cited text to "the salt passed to the KDF shall consist of " | Accept.  TGm Editor: Change as suggested. |
| 4204 | 12.6.10.3 | 2635 | 22 | " When the PMKSA was not created using pre-authentication, the AKM indicated in the RSNE by the STA in the (Ed)(re)association request shall be identical to the AKM used to establish the cached PMKSA in the first place. " is too far away from Table 9-151--AKM suite selectors. Furthermore, it makes the table messy with lots of insertions of "or PMKSA caching" | Add a column to the table with heading something like "Can be used with PMKSA caching" and then state that this means that the AKM can also be used for the use of a cached PMKSA for a previous AKM of that type, and cross-reference from there to 12.6.10.3 Cached PMKSAs and RSNA key management | Reject.  Needs a submission. Seems like an invasive change. Might need more time aned thought… |
| 4230 | 12.7 |  |  | Where "KDF-Hash-Length" is used, sometimes the "Length" is not specified (cf. "Length is Q plus 256", "Length = Q + 128", "Length is the total number of bits to derive, i.e., number of bits of the PTK. The length is dependent on the negotiated cipher suites and AKM suites as defined by Table 12-7 (Cipher suite key lengths) in 12.7.2 (EAPOL-Key frames) and Table 12-10 (Integrity and key-wrap algorithms(#102)(#1188)) in ", "Length is cipher-suite dependent and is defined by the TK\_bits value in Table 12-7 (Cipher suite key lengths).") | Specify the Length in 12.7.1.6.4. In 12.7.8.2 explicitly say "Length = TK\_bits + 128" | Revise.  TGm Editor change as follows  In 12.7.1.6.4  KDF-Hash-Length is the (#246)key derivation function as defined in 12.7.1.6.2 (Key derivation  function (KDF)) using the hash algorithm identified by the AKM suite selector (see Table 9-151  (AKM suite selectors)) to generate ~~a key whose length~~ the key where Length is equal to the length of the hash algorithm’s  digest.  In 12.7.8.2:  KDF-Hash-Length is the key derivation function defined in 12.7.1.6.2 (Key derivation function (KDF)) that uses Hash to generate ~~a key whose length~~ the key where Length is TK\_bits + 128 |
| 4308 | 12.6.1.1.9 | 2624 | 18 | "Direction vector (whether the IGTK is used for transmit or receive)" -- how can it not be rx for a non-AP STA and tx for an AP? | Delete the cited sentence | Accept.  TGm Editor: Change as suggested. |
| 4326 | 12.6.18 | 2640 | 41 | "NOTE 2---Because the IEEE 802.11 Null frame does not derive from an MA-UNITDATA.request primitive, it is not protected." -- the real reason is that there is nothing to protect. Some TDLS frames, for example, are not derived from MA-UNITDATA.requests, but are protected nonetheless. It's not clear what the point of this NOTE is anyway | Delete the cited text at the referenced location, and delete the " 1" immediately above | [Needs to be assigned to someone else] |
| 4388 | 12 |  |  | I presume GCMP is not allowed for S1G, since there's no description of GCMP for PV1 MPDUs. Where is this restriction specified? | As it says in the comment | Reject.  The comment does not propose a change to the draft. Cipher suite negotiation is not PHY specific so there's no reason to impose a requirement that GCM is not allowed for S1G STAs. |
| 4417 | 12.5.3.3.3 | 2604 | 51 | "The Fragment Number subfield is not modified." -- delete (2x), since we don't say so for any of the other not-modified fields | As it says in the comment | Reject.  Fragment number is part of the Sequence Control field. One subfield (Sequence number) of which is masked and the other (Fragment Number) is not. Current text is and would be clearer. No change is proposed. |
| 4465 | 12.6.18 | 2640 | 18 | "shall delete the PTKSA, GTKSA, IGTKSA, BIGTKSA(#2116) (#1504)and any TPKSA(#59)" -- there might not be an IGTKSA or BIGTKSA either | Change to "shall delete the PTKSA, GTKSA, any IGTKSA, any BIGTKSA(#2116) (#1504)and any TPKSA(#59)". In next sentence change " and IGTKSA" to " and any IGTKSA" | Accept.  IGTKSA is option and continguent on PMF being enabled. Ditto for BIGTKSA which is present only when optional Beacon Protection applies.  TGm Editor change as suggested. |
| 4522 | 12.5.4.4 | 2612 | 30 | 11md: "NOTE--When the IPN or BIPN space is exhausted, the choices available to an implementation are to replace the corresponding key or to end communications.(#2116)" should also be stated in the other places where PN-EXHAUSTION is discussed (12.5.3.3.3 for CCMP and 12.5.5.3.2 for GCMP) | As it says in the comment | Reject.  Agree in general more clarifications may be needed. But IGTK and BIGTK do not use CCMP or GCMP, but they use BIP. |
| 4602 | 12 |  |  | There is confusion (cf. CID 2137 I think) about the general concept of a temporal key, and the temporal key (TK) in PTKs (Jouni is adamant they are not the same) | As it says in the comment | Reject.  There is no specific change suggested by the commentor. |
| 4612 | 12 | 2609 | 5 | "4) The nonce(#1406) value is constructed from the STA MAC Address Identified By A2, PN, and Nonce Flags fields." is just duplication of Figure 12-21--Nonce field. Ditto duplication of Figure 12-28--Nonce field for GCMP | Replace the cited text, and "3) (11ah)The nonce(#1406) value is constructed from the A2, PN, and Nonce Flags fields." in 12.5.3.4.1 and "c) The nonce(#1406) value is constructed from the A2 and PN fields." in 12.5.5.4.1, with references to the figures. Also remove the "The Nonce field has an internal structure of Nonce Flags || (11ah)STA MAC Address Identified By A2 || PN" and "The Nonce field has an internal structure of A2 || PN" duplication (of figures immediately above!) | Reject.  Many a figure is followed by an explanation in the spec. The description seems correct. |
| 4672 | 12.4.4 |  |  | It should be "set to" on tx, not "equal to" | Change at end of first para of 12.4.4.2.3, second para of 12.4.7.4 | Accept.  TGm Editor: change as suggested by replacing ‘equal’ with ‘set’ |
| 4728 |  |  |  | "To prevent key reinstallation attacks, a non-AP STA in which dot11WNMSleepModeActivated is true shall maintain a copy of the most recent GTK and most recent IGTK " -- should not quadruplicate this statement, even less so with variant wordings. We did not duplicate the statement for the original KRACK fix (this point was ignored in the resolution of CID 2551) | In 11.2.3.16.1, 12.7.7.4, 12.12.2.1, 13.5.1 delete the para starting (#1321) and replace it with "NOTE---See 6.3.19 regarding prevention of key reinstallation attacks." | Reject.  There is a reference to 6.3.19 at the end of the paragraph and it seems clear enough. Also, to include any note some text is needed to provide the context for the note. |

**CID 4093**

Discussion:

The encrypted field extends to MIC. Figure to be adjusted accordingly

TGm Editor, please replace Figure 12-26 as shown below.



**CID 4388**

The comment is as follows:

“I presume GCMP is not allowed for S1G, since there's no description of GCMP for PV1 MPDUs. Where is this restriction specified?”

Discussion

PV1 frames are compressed frames that are optionally used with S1G

The comment seems to ask for a restriction that S1G STAs only use CCMP - which puts a requirement on using specific ciphers with specific PHYs. We didn't even do that with TKIP. There is nothing to stop (from a specification point of view) an S1G STAs advertising and negotiating a GSM cipher suite – in that case they would use PV0 frames, since GCMP is not specified for PV1 frames.

There is no technical problem that would be solved by adding any additional text since at this time since negotiating PV1 frame exchanges with GCMP isn't a requirement. If and when required, a separate submission could address how PV1 frames may be used with GCMP.

The proposed resolution doesn't actually propose a change.