IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolutions for some CCMP GCMP CIDs | | | | |
| Date: 2020-03-10 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Rojan Chitrakar | Panasonic | 202 Bedok South Avenue 1, #02-11 Singapore 469332 |  | Rojan.chitrakar@sg.panasonic.com |
|  |  |  |  |  |

Abstract

This submission proposes resolution to some comments related to CCMP and GCMP received in SB1.

Rev0: Initial Version

**CID 4088**

Comment (P2608L50): 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.

Proposed Change: Reword to convey that the MIC that is used in the CCM integrity checking is only obtained after decryption of the encrypted MIC.

Discussion: From the description of the Originator processing, it is clear that the MIC is also encrypted. However, in the description of the CCMP decapsulation, it is not clear that the MIC needs to be decrypted before it can be used for integrity checking.

Resolution: **Revised**. Change P2608L50 as follows:

4) (11ah)The encrypted MIC is extracted and decrypted for use in the CCM integrity checking.

**CID 4089**

Comment (P2609L8): 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.

Proposed Change: Reword to convey that the MIC that is used in the CCM integrity checking is only obtained after decryption of the encrypted MIC.

Discussion: Same as CID 4088.

Resolution: **Revised**. Change P2608L50 as follows:

5) The encrypted MIC is extracted and decrypted for use in the CCM integrity checking.

**CID 4090**

Comment (P2609L50): "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.

Proposed Change: 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.

Discussion: From the description of the Originator processing, it is clear that the MIC is also encrypted. However, in the description of the recipient processing, it is not clear that the MIC needs to be decrypted before it can be used for integrity checking.

Resolution: **Revised**. Change P2609L50 as follows:

CCM recipient processing checks the authentication and integrity of the frame body and the AAD as

well as decrypting the frame body. A MIC check is performed by comparing the decrypted MIC with a MIC formed as described in 12.5.3.3 CCMP cryptographic encapsulation. The plaintext is returned only if the MIC check is successful.

**CID 4090**

Comment (P2609L61): "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.

Proposed Change: Clarify how the MIC is calculated for the MIC check.

Discussion: Although it is probably not difficult to deduce how the MIC is calculated, it would be clearer if a reference is provided to 12.5.3.3 CCMP cryptographic encapsulation which explains how the MIC is calculated.

Resolution: **Revised**. Change P2609L61 as follows:

The decapsulation process succeeds when the calculated MIC (as described in 12.5.3.3 CCMP cryptographic encapsulation) matches the MIC value obtained from decrypting the received encrypted MPDU. The original MPDU header is concatenated with the plaintext data resulting from the successful CCM recipient processing to create the plaintext MPDU.

**CID 4093**

Comment (P2615L7): Figure 12-26: In GCMP isn't MIC also encrypted? P2617L25 mentions that it is. The figure should be amended showing MIC as encrypted.

Proposed Change: Amend Figure 12-26 to show MIC as encrypted.

Discussion: Figure 12-16—Expanded CCMP MPDU clearly shows the MIC as being encrypted. Figure 12-26 should also show MIC as encrypted.

Resolution: **Revised**. Replace Figure 12-26 with below:

