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

Rev1: Made some changes based on email comments from Mark Rison.

Rev2: Reversed the changes made to GCMP based on feedback from Dan Harkins and extensive email discussions: encrypted MIC -> MIC.

**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 used for integrity checking is encrypted. Clarification is added that the MIC included in a protected frame is encrypted in relevant places in the specs.

Resolution: **Revised**.

Change P2603L3 as follows:

5) Use the temporal key, AAD, nonce, and MPDU data to form the cipher text and the encrypted MIC. This step is known as CCM originator processing.

Change P2603L5 as follows:

6) Form the encrypted MPDU by combining the original MPDU header, the CCMP header, the

encrypted data and the encrypted MIC, as described in 12.5.3.2 (CCMP MPDU format).

Change P2603L30 as follows:

5) Use the temporal key, AAD, nonce, (#2720)and MPDU data to form the cipher text and the encrypted MIC. This step is known as (#2720)CCM originator processing.

Change P2603L33 as follows:

6) Form the encrypted MPDU by combining the original MPDU header, the encrypted data, and

the encrypted MIC, as described in 12.5.3.2 (CCMP MPDU format).

Change P2608L50 as follows:

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

Change P2609L44 as follows:

— Encrypted frame body: the encrypted frame body from the received MPDU. The encrypted frame

body includes the encrypted MIC.

Change P2616L13 as follows:

e) Use the temporal key, AAD, nonce, and MPDU data to form the cipher text and the MIC. This step is known as GCM originator processing.

Change P2616L16 as follows:

f) Form the encrypted MPDU by combining the original MPDU header, the GCMP header, the

encrypted data and the MIC, as described in 12.5.5.2 (GCMP MPDU format).

Change P2618L28 - P2618L35 as follows:

d) The MIC is extracted for use in the GCM integrity checking.

e) GCM recipient processing uses the temporal key, AAD, nonce, MIC, and MPDU cipher text

data to recover the MPDU plaintext data as well as to check the integrity of the AAD and MPDU

plaintext data.

f) The received MPDU header and the MPDU plaintext data from GCM recipient processing are

concatenated to form a plaintext MPDU.

Change P2618L50 as follows:

GCM recipient processing uses the same parameters as GCM originator processing. A GCMP protected individually addressed robust Management frame shall use the same TK as a Data frame.

Change P2618L59 as follows:

— Encrypted frame body: the encrypted frame body from the received MPDU. The encrypted frame

body includes a MIC.

**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 P2609L8 as follows:

5) The encrypted MIC is extracted 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. Similar change is also applied for GCMP at P2619L1.

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 received MIC with a MIC calculated as described in 12.5.3.3 (CCMP cryptographic encapsulation). The plaintext is returned only if the MIC check is successful.

Change P2619L1 as follows:

GCM 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 received MIC with a MIC calculated as described in 12.5.5.3 (GCMP cryptographic encapsulation). The plaintext is returned only if the MIC check is successful.

**CID 4091**

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. Similar change is also applied to GCMP at P2619L11.

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.

Change P2619L11 as follows:

The decapsulation process succeeds when the calculated MIC (as described in 12.5.5.3 GCMP 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 GCM 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: Through considerable offline discussions, it was agreed that for GCMP the MIC should not be considered as being encrypted. The conclusion of the discussion was to leave Figure 12-26 as it is, change “encrypted MIC” to “MIC” at P2617L25, and add a NOTE to clarify that the MIC is not encrypted in GCMP.

Resolution: **Revised**.

Change P2617L23as follows:

The GCM originator processing provides authentication and integrity of the frame body and the AAD as well as data confidentiality of the frame body. The output from the GCM originator processing consists of the encrypted data and 16 additional octets of MIC (see Figure 12-26 (Expanded GCMP MPDU)).

NOTE—In GCM originator processing, the MIC obtained is not encrypted, unlike in CCM originator processing. Refer to NIST Special Publication 800-38D for details.