IEEE P802.11  
Wireless LANs

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  | | --- | --- | --- | --- | --- | | SB CR for CID 7028 | | | | | | Date: 2024-04-10 | | | | | | Author(s): | | | | | | Name | Affiliation | Address | Phone | email | | Po-Kai Huang | Intel |  |  | po-kai.huang@intel.com | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |  |  |  |  |  | |

Abstract

This submission proposes resolutions for the following comments from comment collection on P802.11-REVme D5.0:

7028

**Revision History:**

R0: Initial version.

R1: Revision after offline discussion

R2: Further revision after offline discussion

# CID 7028

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page.Line** | **Comment** | **Proposed Change** |
| 7028 | 12.5.4.3.4 | 3040.17 | The security of QMF depends on the ACI of the MMPDU being protected. This is similar to how the security of QoS for Data frames depends on the TID being protected. ACI is protected when using CCMP, but not when using GCMP.  ACI is encoded in the ACI subfield in the Sequence Number field. That field is masked out from AAD construction for both CCMP and GCMP and as such, AAD does not protect it (unlikely it does for QoS Data frames with QC being included).  CCMP protects the ACI subfield value by defining the priority value of the MPDU to be equal to its value (P3021 L28). This priority value is then included in the CCM nonce (see Figure 12-21) and that provides protection to the ACI value. GCMP on the other hand does not include the priority value in the GCM nonce (see Figure 12-30). Consequently, there is no protection for the ACI value and attacker can modify it without the frame recipient being able to detect the modification based on GCMP processing. This enabled attacks that could be used to reorder Robust Management frames between different access categories.  Protection of ACI with GCMP is inconvenient since there is no room in the GCM nonce for the priority value. The standard could be extended to construct the AAD for GCMP to include a new field for the QMF cases (e.g., a "virtual" octet with the ACI encoded in it at the end of the AAD) or by not masking the ACI subfield of the Sequence Number field in QMFs. This would make the AAD construction different for GCMP compared to CCMP (since we should not change CCMP definition for this and break compatibility with the original design). It might be acceptable to modify GCMP for QMF due to limited, if any, interest in deploying QMF so far. It would also be possible to negotiate use of the extended AAD for GCMP when QMF is used. That said, if there is no interest in deploying QMF, there may not be much benefit from coming up with more complex solutions for this than simply disallow use of QMF with GCMP.  This comment proposes an unconditional change to the AAD construction for GCMP for QMFs to unmask the ACI field. This is not compatible with previous definition. However, this is believed to be acceptable due to no known deployment of QMF with GCMP. This comment could be satisfied with a similar change done based on negotiated capability (e.g., and RSNXE bit) or by disallowing use of QMF with GCMP. | At P3023 L45-46, replace "SC – MPDU Sequence Control field, with the Sequence Number subfield (bits 4–15 of the Sequence Control field) masked out"  with  "SC – MPDU Sequence Control field, with the QMF Sequence Number field (bits 4-13 of the Sequence Control field) masked out in QMFs and with the Sequence Number subfield (bits 4–15 of the Sequence Control field) masked out in frames that are not QMFs" . |

## Discussion:

Agree that unprotected ACI field under QMF for GCMP is an issue for replay check. The proposed solution to have capability in RSNXE and unmask ACI bits if QMF is used seems to be the way to address the issues. Note that today CCMP and GCMP has the same AAD constructions, so the proposal does not try to differenaite AAD construction for GCMP and CCMP.

## Proposed Resolution: CID 7028

**REVISED**

**Instruction to TGme Editor:**

Implement the proposed text updates for corresponding CID in 11-24/0682r2

**TGme Editor: *Instruction: Insert new rows in Table 9-363 in 9.4.2.241 RSNXE as shown below***

9.4.2.240 RSNXE

|  |  |  |
| --- | --- | --- |
| * **Extended RSN Capabilities field** | | |
| **Bit** | **Information** | **Notes** |
| <ANA> | QMF ACI Subfield Unmask Support | A STA sets the QMF ACI Subfield Unmask Support to 1 if the STA supports to unmask ACI subfiled during AAD construction. Otherwise, this subfield is set to 0. |

**TGme Editor: *Instruction: Modify 12.5.2.3.3 as shown below***

* Construct AAD
* For PV0 MPDUs, the format of the AAD is shown in Figure 12-18 (AAD construction for PV0 MPDUs). The length of the AAD for PV0 varies depending on the presence or absence of the QC and A4 fields and is shown in Table 12-3 (AAD length for PV0 MPDUs).

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | FC | A1 | A2 | A3 | SC | A4 | QC |
| Octets: | 2 | 6 | 6 | 6 | 2 | 6 | 2 |
| * AAD construction for PV0 MPDUs | | | | | | | |



|  |  |  |
| --- | --- | --- |
| * AAD length for PV0 MPDUs | | |
| QC field | A4 field | AAD length (octets) |
| Absent | Absent | 22 |
| Present | Absent | 24 |
| Absent | Present | 28 |
| Present | Present | 30 |

The AAD is constructed from the MPDU header. The AAD includes neither the Duration/ID field nor the HT Control field because the contents of these fields might change during normal operation (e.g., due to a rate change preceding retransmission). The HT Control field might also be inserted or removed during normal operation (e.g., retransmission of an A-MPDU where the original A-MPDU included an MRQ that has already generated a response). For similar reasons, several subfields in the Frame Control field are (#1951)masked out. For PV0 MPDUs, AAD construction is performed as follows:

* FC – MPDU Frame Control field, with(#4183):
* (#486)The 3 LSBs of the Subtype subfield (bits 4 5 6) in a Data frame (#1951)masked out. Bit 7 is not modified
* Retry subfield (bit 11) (#1951)masked out
* Power Management subfield (bit 12) (#1951)masked out
* More Data subfield (bit 13) (#1951)masked out
* Protected Frame subfield (bit 14) (#1951)not modified (left as 1)
* +HTC subfield (bit 15) as follows:
* (#1951)Masked out in all Data frames containing a QoS Control field
* (#1951)Not modified otherwise
* (#4183)No modification to other subfields
* A1 – MPDU Address 1 field.
* A2 – MPDU Address 2 field.
* A3 – MPDU Address 3 field.

5) SC – MPDU Sequence Control field, with bits 0-9 of the Sequence Number subfield masked out if the frame is an IQMF and both the STA and its peer set the QMF ACI Subfield Unmask Support subfield to 1 (see 9.4.2.240 (RSNXE)), and with the entire Sequence Number subfield masked out otherwise.

NOTE—The Fragment Number subfield is not modified. Bits 10-11 of the Sequence Number subfield are not modified if the frame is an IQMF and both the STA and its peer set the QMF ACI Subfield Unmask Support subfield to 1.

SC – MPDU Sequence Control field, with bits 0-9 of the Sequence Number subfield (bits 4–15 of the Sequence Control field) masked out if the frame is an IQMF and both the STA and its peer set the QMF ACI Subfield Unmask Support subfield to 1 (see 9.4.2.240 (RSNXE)), and with the entire Sequence Number subfield masked out otherwise.

NOTE—The Fragment Number subfield is not modified. Bits 10-11 of the Sequence Number subfield are not modified if the frame is an IQMF and both the STA and its peer set the QMF ACI Subfield Unmask Support subfield to 1.

* A4 – MPDU Address field, if present.
* (#2145)(#217)QC – MDPU QoS Control field contains the MSDU priority, if present. The QC TID is used in the construction of the AAD. When in a non-DMG BSS, if both the STA and its peer have their SPP A-MSDU Capable (M57)subfields (see 9.4.2.240 (RSNXE(#1776))) equal to 1, the A-MSDU Present field is also used in the construction of the AAD. When in a DMG BSS, the A-MSDU Present field and A-MSDU Type field are also used in the construction of the AAD. The remaining QC fields are not used and are (#1951)masked out for the AAD calculation (for a non-DMG BSS, bits 4 to 6, bits 8 to 15, and bit 7 when either the STA or its peer has the SPP A-MSDU Capable field equal to 0; for a DMG BSS, bits 4 to 6 and bits 9 to 15). When in a DMG BSS, the A-MSDU Present bit 7 and A-MSDU Type bit 8 are used in the construction of the AAD, and the remaining QC fields are (#1951)masked out for the AAD calculation (bits 4 to 6, bits 9 to 15).
* For PV1 MPDUs, the format of the AAD is shown in Figure 12-19 (AAD construction for PV1 MPDUs).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | FC | A1 | A2 | SC | A3 | A4 |
| Octets: | 2 | 6 | 6 | 2 | 0 or 6 | 0 or 6 |
| * AAD construction for PV1 MPDUs | | | | | | |

For PV1 MPDUs, the length of the AAD varies depending on the presence or absence of the A3 and A4 fields and is shown in Table 12-4 (AAD length for PV1 MPDUs).

|  |  |  |  |
| --- | --- | --- | --- |
| * AAD length for PV1 MPDUs | | | |
| Type subfield in the Frame Control | A3 field in uncompressed header | A4 field in uncompressed header | AAD length  (octets) |
| 0, 1 or 3 | Absent | Absent | 16 |
| 0, 1 or 3 | Present | Absent | 22 |
| 0 or 3 | Absent | Present | 22 |
| 0 or 3 | Present | Present | 28 |

For PV1 MPDUs, AAD construction is performed as follows:

* FC – MPDU Frame Control field, with(#4183):
* Power Management subfield (bit 10) (#1951)masked out
* More Data subfield (bit 11) (#1951)masked out
* Protected Frame subfield (bit 12) (#1951)not modified (left as 1)
* EOSP subfield (bit 13) (#1951)masked out
* Relayed Frame subfield (bit 14) (#1951)masked out
* Ack Policy Indicator subfield (bit 15) (#1951)masked out
* (#4183)No modification to other subfields
* A1 – MPDU A1 field if it contains a MAC address; otherwise, the MAC address that corresponds to the AID value contained in the SID field of the A1 field.
* A2 – MPDU A2 field if it contains a MAC address; otherwise, the MAC address corresponding to the AID value contained in the SID field of the A2 field.
* SC – MPDU Sequence Control field, with the Sequence Number subfield (bits 4–15 of the Sequence Control field) (#1951)masked out. The Fragment Number subfield is not modified.
* A3 – MPDU A3 field if present in the MPDU, the value of A3 stored at the receiver if A3 is stored at the receiver and is not present in the MPDU (see 10.57 (Generation of PV1 MPDUs and header compression procedure)); otherwise, not present.
* A4 – MPDU A4 field if present in the MPDU, the value of A4 stored at the receiver if A4 is stored at the receiver and is not present in the MPDU (see 10.57 (Generation of PV1 MPDUs and header compression procedure)); otherwise, not present.