IEEE P802.11
Wireless LANs

|  |
| --- |
| REVme Security Comment resolutions |
| Date: 2021-05-07 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Michael Montemurro | Huawei |  |  | montemurro.michael@gmail.com  |

Background

Resolutions to security comments received in CC35. The list includes 188, 189, 202, 271, 308, 354, 364, 408, 212, 193

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 188 |  | 12 |  |  | It's not sufficient to construct the message, you have to transmit it too! | Change "onstructs" to "onstructs and sends" at 2640.47, 2642.27. Change "creating" to "constructing" at 2650.52 |

### Discussion:

For the 3 locations specified in the comment

2650.47

“Processing for PTK generation is as follows:

The Authenticator sends message 1 to the Supplicant at the end of a successful IEEE 802.1X authentication, after (re)association completes for a STA that has authenticated with SAE or PSK authentication is negotiated, when a cached PMKSA is used, or after a STA requests a new key. On reception of message 1, the Supplicant determines whether the Key Replay Counter field value has been used before with the current PMKSA. If the Key Replay Counter field value is less than or equal to the current local value, the Supplicant discards the message. Otherwise, the Supplicant:

a) Generates a new nonce SNonce.

b) Derives PTK.

c) Constructs message 2.”

* From the context, this text describes what the Supplicant does to verify message 1. The next clause describes how to construct message 2.

2642.27

 Similar comments to 2650.47

2650.52

 In this case, the text states:

“e) Responds by creating and sending message 2 of the group key handshake to the Authenticator and incrementing the replay counter.”

However the replay counter is incremented after successfully sending message 2.

Clause 12.7.6.1 summarizes the 4-way handshake message flow and clause 12.7.7.1 summarizes the group key exchange, so its clear which message is constructed and transmitted next for the protocols. The important content around the cited text is the description of how the message is validated by the receiver.

### Proposed Resolution:

Revised. The text that specifies “sending” the EAPoL message is in the subsequent clause which describes the content of the frame that was sent. However it would be useful to add a pointer to indicate where to find the content of the frame to be sent.

For the 4-way handshake:

At 2640.47, change “c) Constructs message 2.” To “c) Constructs and sends message 2 to the Authenticator as described in 12.7.6.3.“

At 2642.24, change “If these are not exactly the same,” to “If they do not match bitwise,”

At 2642.27, change “If they do match bitwise, the Authenticator constructs message 3.” to “If they do match bitwise, the Authenticator constructs and sends message 3 to the Supplicant as described in 12.7.6.4.”

At 2644.51, delete “e) Constructs message 4.”

At 2644.53, change “f) Sends message 4 to the Authenticator.” with “e) Constructs and Sends message 4 to the Authenticator as described in 12.7.6.5.” and renumber “g)” to “f)”

For the group key exchange:

At 2650.52, change “Responds by creating and sending message 2 of the group key handshake to the Authenticator and incrementing the replay counter.” To “Responds by constructing and sending message 2 of the group key handshake to the Authenticator as described in 12.7.7.3 and incrementing the replay counter.”

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 189 | 2650.00 | 12.7.7.2 |  |  | For group key handshake M1, Key Data is specified to be "encrypted, encapsulated" but this is not done for 4WH M3 or indeed anywhere else | Delete "encrypted, encapsulated" at the referenced location |

### Discussion:

From the 4-way handshake:

* Message 1: Key Data = PMKID for the PMK being used during PTK generation
* Message 2 and 3: Key Data = is followed by a bulleted list
* Message 4: Key Data = is followed by “none required”

There is no mention of encryption or encapsulation and there is already a Encrypted Key Data field in the EAPoL-Key frame which indicates whether the Key Data field is encrypted.

The group key handshake should follow the same convention as the 4-way handshake.

### Proposed Resolution:

Accepted.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 202 | 2608.00 | 12.6.15 |  |  | "If enabled, management frame protection shall only be used as a required feature (MFPR) in an IBSS." -- what does this mean? It might be trying to say that in an IBSS if you're going to do MFP you have to set MFPR, but that's contradicted by Table 12-6--Robust management frame selection in an IBSS. Even with the "only" (a word that always massively increases the risk of ambiguity) it's not clear what it might be trying to say | Delete the cited sentence |

### Discussion:

The cited sentence in context looks like

“A STA joining an IBSS is required to adopt the security configuration of the IBSS, which includes the group cipher suite, pairwise cipher suite, AKMP, and if management frame protection is enabled, group management cipher suite (see 12.6.5 (RSNA policy selection in an IBSS)). The STA shall not set up a security association with any STA having a different security configuration. The Beacon and Probe Response frames of the various STAs within an IBSS need to reflect a consistent security policy, as the beacon initiation rotates among the STAs.

A STA joining an IBSS shall support and advertise in the Beacon frame the security configuration of the IBSS, which includes the group cipher suite, advertised pairwise cipher suite, AKMP, and if management frame protection is enabled, group management cipher suite (see 12.6.5 (RSNA policy selection in an IBSS)). The STA may use the Probe Request frame to discover the security policy of a STA, including additional individual cipher suites the STA supports. **If enabled, management frame protection shall only be used as a required feature (MFPR) in an IBSS.**

NOTE—Because of the requirement for a STA joining an IBSS to support the security configuration of the IBSS, all Beacon frames transmitted in an IBSS have the same security policy.”

From 2600.40: (in RSNA policy selection in an IBSS)
“To establish a connection with a peer STA, an RSNA enabled STA that implements management frame protection shall use Table 12-6 (Robust management frame selection in an IBSS) and the MFPC and MFPR values advertised in the RSNEs exchanged in the 4-way handshake initiated by the Authenticator of the STA with the larger MAC address to determine if the communication is allowed. Management frame protection is enabled when dot11RSNAProtectedManagementFramesActivated is set to 1. The STAs negotiate protection of Management frames when the both STAs set the Management Frame Protection Capable subfield to 1 during the 4-way handshake.”

Feedback from Jouni (21/07/19): *There was a long(ish) discussion on what to do with PMF and IBSS during the P802.11w work and the conclusion of thar was that if MFP is used, it needs to be set to required (MFPR=1). This might have been towards the end of the project and as such, I'm not surprised if it did not got defined clearly in the standard. Regardless, this sentence should not be removed since that would likely remove most of the conclusions from that debate. In other words, that comment should either be rejected ("MFPR=1 is required for IBSS and as such, this sentence should not be removed") or revised (get rid of "only" or otherwise make this easier to understand and fix the table to match).*

Table 12-6 indicates the possible cases where the peer STAs can connect and where there is a policy violation, not where MFP is negotiated. The cited sentence provides the requirement that MFP shall only be negotiated when both peers set MFPR to 1 and therefore cannot be deleted.

### Proposed Resolution:

Rejected. The cited sentence indicates that MFPR=1 is required for IBSS and cannot be removed. Table 12-6 does not conflict with the cited text and provides requirements on RSNA policy selection in an IBSS to determine whether communications between IBSS STAs are allowed.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 271 | 2592.00 | 12.6.1.1.6 |  |  | "Authenticator MAC address or BSSID" -- when does the PTKSA include the BSSID rather than the Authenticator MAC address? | Delete "or BSSID", and also "or STA's MAC address" above |

### Discussion:

The text at the cited location is as follows:

“The PTKSA consists of the following:

— PTK

— Pairwise cipher suite selector

— Supplicant MAC address or STA’s MAC address

— Authenticator MAC address or BSSID

— Key ID

— If FT key hierarchy is used,

— R1KH-ID

— S1KH-ID

— PTKName”

The text was originally added by IEEE 802.11r to clarify that in an infrastructure network with FT enabled, the BSSID and the STAs MAC address are bound into the PTKSA (see 12.7.1.6.5). Note that FT introduces R0/R1 key holder represent the Authenticator address and S0/S1 key holders identify the Supplicant address.

Feedback from Jouni (21/07/19): *I would reject this unless there is strong justification for getting rid of the current concept of Authenticator potentially being an entity that differs from the AP (BSSID). In particular, this better remain consistent with how FT uses the R0/R1-KH concept and R0KH being a different entity from the current AP (the former being the Authenticator when the FT key hierarchy was established and the latter being the Authenticator when the PTKSA was established).*

Feedback from Dan (21/07/20): *I'd be fine with a reject.*

### Proposed Resolution:

Rejected. The cited text is correct. For FT, the PTKSA is bound to the BSSID and the STA’s MAC Address (see 12.7.1.6.5).

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 308 | 2523.00 | 12.3.1 |  |  | "Open System Authentication and Open System Deauthentication shall not be used between mesh STAs." -- no such thing as OS deauth, and for auth the "A" should be lowercase | Change to "Open System authentication shall not be used between mesh STAs." |

### Discussion:

Confirmed with Guido Hertz that the resolution can be accepted.

### Proposed Resolution:

Accepted.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 354 | 2555.00 | 12.5.1 |  |  | "BIP is used only to protect Management frames within the BSS." -- does this mean "is not used to protect other frames" or "is not used to protect Management frames outside the BSS"? | Change to "BIP is not used to protect Management frames intended for members of the BSS." |

### Discussion:

The cited text in context is as follows:

“BIP is a mechanism that is used only when management frame protection is negotiated. BIP provides integrity protection for group addressed robust Management frames. BIP is used only to protect Management frames within the BSS.”

Since only members of the BSS have BIP keys to verify the integrity protection, the protection is intended for members of the BSS.

Feedback from Jouni (21/07/19): *The meaning of this sentence is that BIP cannot be used for protecting Data frames and as such, neither the proposed change in the comment or the proposed resolution in this document look correct to me, i.e., the current standard language is significantly better than either of those. I'd reject this comment or if there is real need for clarifying this, reword it in a manner that maintains the original intent of the design.*

### Proposed Resolution:

Rejected. Since only members of the BSS have BIP keys to verify integrity protection, the protection is only available to members within the BSS.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 364 | 2583.00 | 12.5.5.1 |  |  | "A DMG RSNA STA shall support GCMP-128." -- a DMG STA is an RSNA STA, so "RSNA" is superfluous and misleading (suggests a DMG STA might not be an RSNA STA) | Delete "RSNA " |

### Discussion:

None

### Proposed Resolution:

Accepted. Note to Editor that the cited text is a 2583.41

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 193 | 2577.00 | 12.5.3.4.1 |  |  | "The decryption processing prevents replay of MPDUs by validating that the PN in theMPDU is greater than the replay counter maintained for the session." should be ... "and TID" or "and AC" to allow for reordering across TIDs/ACs, where the receiver has indicated support for multiple replay counters (so maybe better as "(or the replay counter corresponding to the TID, if more than one replay counter is supported)" Or actually, since in 802.11 (unlike WMM) you allocate TIDs up to the max num replay counters supported, maybe just say "replay counter maintained for the session for that TID"?) | Change to "The decryption processing prevents replay of MPDUs by validating that the PN in theMPDU is greater than the replay counter maintained for the session for that TID." Ditto at 2587.36. At 2577.49 change "the PN in the CCMPheader is greater than the replay counter maintained for the session and TID/ACI." to "the PN in the MPDU is greater than the replay counter maintained for the session for that TID." |

### Discussion:

Cited text for CCMP:

2577.30:

“5) The decryption processing prevents replay of MPDUs by validating that the PN in the MPDU is greater than the replay counter maintained for the session.”

2577.49

“The decryption processing prevents replay of MPDUs by validating that the PN in the CCMP

header is greater than the replay counter maintained for the session and TID/ACI.”

Note that for CCMP, the last sentence of the clause states:

“See 12.5.3.4.2 (CCM recipient processing) to 12.5.3.4.4 (PN and replay detection) for details of this processing.”

Cited Text for GCMP

2587.36

“e) The decryption processing prevents replay of MPDUs by validating that the PN in the MPDU is greater than the replay counter maintained for the session.”

For GCMP, the last sentence of the clause states:

“See 12.5.5.4.2 (GCM recipient processing) to 12.5.5.4.4 (PN and replay detection) for details of this processing.

PV1 frames can be QMF.

### Proposed Resolution:

Revised. Make the following changes in the direction proposed by the commenter:

At 2577.30, replace:

“for the session.”

With

“for the session and TID/ACI.”

At 2587.36, replace:

“for the session.”

With

“for the session and TID.”

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 212 | 2575.00 | 12.5.3.3.4 |  |  | "The Priority subfield shall be set to the priority value of the MPDU" is not clear (if the MPDU is a non-QoS Data frame or a Management frame) | Append "(see 12.5.3.3.1)" since this defines what is meant by "the priority value of the MPDU" |

### Discussion:

The requirements for assigning a priority value are given in 12.5.3.3.1 on page 2571 in item a) 3 for PV0 frames and b) 3 for PV1 frames. It doesn’t hurt to provide a clause reference at the cited location.

### Proposed Resolution:

Accepted.

### Comment

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **CID** | **Page** | **Clause** | **Duplicate of CID** | **Resn Status** | **Comment** | **Proposed Change** |
| 408 |  | 12.7.2 |  |  | "into its IEEE 802.11 MAC" doesn't make sense, since an 802.1X component doesn't have an 802.11 MAC per se | Change to "into the IEEE 802.11 MAC" (3x) as in all the other locations |

### Discussion:

First location: (2620.26)

“4) Install (bit 6).

i) If the value of Key Type (bit 3) is 1, then for the Install bit,

— The value 1 means the IEEE 802.1X component shall configure the temporal key derived from this message into its IEEE 802.11 MAC.

— The value 0 means the IEEE 802.1X component shall not configure the temporal key into the IEEE 802.11 MAC.”

Second and third location: (2633.9 and 2633.12)

“4) Install (bit 6).

i) If the value of Key Type (bit 3) is 1, then for the Install bit,

— The value 1 means the IEEE 802.1X component shall configure the temporal key derived from this message into its IEEE 802.11 MAC.

— The value 0 means the IEEE 802.1X component shall not configure the temporal key into the IEEE 802.11 MAC.”

### Proposed Resolution:

Accepted. Note to Editor that the cited text is a 2620.26, 2633.9 and 2633.12