IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Clarification PFTM Replay Counter Update | | | | |
| Date: Aug 05 2020 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Nehru Bhandaru | Broadcom Inc. | 250 Innovation Drive, San Jose CA | +1 408 391 2159 | [nehru.bhandaru@broadcom.com](mailto:nehru.bhandaru@broadcom.com) |

Abstract

This submission proposes a clarification about updating the replay counter used for Protected Fine Timing frames when decryption happens after replay checking.

**Revision Notes**

00 – Initial version

**References**

[1] IEEE P802.11-REVmd™/D3.4, July 2020

[2] P802.11az™/D2.2 – Amendment for Positioning

[3] Document 11-20/0797r0 - LMR/FTM Replay Counter

[4] Document 11-20/0889 – Protected LMR Counter

**Discussion**

The group adopted the changes in 11-20/889r4 related to Protected Fine Timing (PFTM) frames and a separate replay counter to be used with PFTM frames. That document specifies for CCMP replay detection §12.5.3.4.4

*“If the receiver performs replay detection prior to decryption, then the receiver shall check that the replay counter used to detect replays is correct and discard the frame if incorrect. In particular, the separate replay counter for individually addressed Protected Fine Timing frames shall be used if and only if the FTM subfield of CCMP Header (Figure 12-16—Expanded CCMP MPDU) signals that the management PDU is a Protected Fine Timing Frame.”*

A similar behavior is specified for GCMP in §12.5.5.4.4

Some concern was expressed that if replay detection was performed prior to decryption and the received updated the replay counter for a frame that would have failed decryption, an attacker may be able to perpetrate denial of service.

However, a receiver may detect replay and discard, but it only updates the replay counter when the decryption also succeeds - we are not changing that behavior.  
  
For both CCM and GCM replay detection, we have this in [1]  
  
*" The replay counter is set to the PN value of accepted \*CMP MPDUs.”*  
  
The frame is not accepted unless the decryption (also) succeeds. This isn't very clear in the spec and the early discard avoids decryption overhead for frames that are clearly replays. There is no security issue, for example BIP procedure explicitly allows this, and w/ TKIP replay checking happens before (MSDU) MIC check - only after which the replay counter is updated.  
  
See [1]-  §12.5.2.6 TKIP replay protection procedures,  §12.5.4.6 BIP reception  
  
In any case, there is no security issue - since this scheme is used (and is more efficient for some devices that might decrypt some frames in s/w) with IPSEC - see IETF rfc 4302 and 4303 where the receive window is updated only after integrity verification, that comes after replay checking succeeds.

This submission proposes a change to 11az spec so the behavior is clear.

**Proposed Changes**

***TGaz Editor – Replace bullet i) in 12.5.3.4.4 PN and replay detection as follows***

***Change* 12.5.3.4.4 PN and replay detection (2603.25) *as follows***

**…**

The following processing rules are used to detect replay:

a) The receiver shall maintain a separate set of replay counters for each PTKSA, GTKSA, (#59)(11ah)and protocol version value. The receiver initializes these replay…

***Replace***

i) If the receiver performs replay detection prior to decryption, then the receiver shall check that the replay counter used to detect replays is correct and discard the frame if incorrect. In particular, the separate replay counter for individually addressed Protected Fine Timing frames shall be used if and only if the FTM subfield of CCMP Header (Figure 12-16—Expanded CCMP MPDU) signals that the management PDU is a Protected Fine Timing Frame.

***With***

i) If the receiver performs replay detection prior to decryption, then the receiver shall check that the replay counter used to detect replays is correct and discard the frame if incorrect. In particular, the separate replay counter for individually addressed Protected Fine Timing frames shall be used if and only if the FTM subfield of CCMP Header (Figure 12-16—Expanded CCMP MPDU) signals that the management PDU is a Protected Fine Timing Frame. The replay counter shall not be updated unless the decryption is successful and the frame is accepted.

***TGaz Editor – Replace bullet i) in 12.5.5.4.4 PN and replay detection as follows***

***Change* 12.5.5.4.4 PN and replay detection *(p2612.32) as follows***

a) The receiver shall maintain a separate set of replay counters for each PTKSA and GTKSA(#59). The receiver initializes these replay counters to 0 when it resets the temporal key for a peer. The replay counter is set to the PN value of accepted GCMP MPDUs…

***Replace***

i) If the receiver performs replay detection prior to decryption, then the receiver shall check that the replay counter used to detect replays is correct and discard the frame if incorrect. In particular, the separate replay counter for individually addressed Protected Fine Timing frames shall be used if and only if the FTM subfield of GCMP Header (Figure 12-26—Expanded GCMP MPDU) signals that the management PDU is a Protected Fine Timing Frame.

***With***

i) If the receiver performs replay detection prior to decryption, then the receiver shall check that the replay counter used to detect replays is correct and discard the frame if incorrect. In particular, the separate replay counter for individually addressed Protected Fine Timing frames shall be used if and only if the FTM subfield of GCMP Header (Figure 12-26—Expanded GCMP MPDU) signals that the management PDU is a Protected Fine Timing Frame. The replay counter shall not be updated unless the decryption is successful and the frame is accepted.