IEEE P802.11
Wireless LANs

|  |
| --- |
| TGmd SB1 CID 4728 |
| Date: June 22, 2020 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Nehru Bhandaru | Broadcom Inc. | 250 Innovation Drive, San Jose CA 95134 | +1 408 391 2159 | nehru.bhandaru@broadcom.com |

Abstract

This document provides some discussion and a proposed resolution for CID 4728. It is duplicate of CID 2551 that has a resolution of ‘Reject’ currently. The group may consider rejecting CID 4728 also with the same reason; alternatively both the CIDs could be resolved using the proposed changes, relative to TGmd Draft 3.3 [1], in this submission.

**References**

[1] IEEE P802.11-REVmd™/D3.3, May 2020

**Revision Notes**

r0 – Initial Revision

r1 – Adjust based on CID 2551 which is a duplicate

**Comment**:

**CID 4728**

To prevent key reinstallation attacks, a non-AP STA in which dot11WNMSleepModeActivated is
true shall maintain a copy of the most recent GTK and most recent IGTK " -- should not quadruplicate this statement, even less so with variant wordings.  We did not duplicate the statement for the original KRACK fix (this point was ignored in the resolution of CID 2551)

*Commenter Proposed Resolution:*

In 11.2.3.16.1, 12.7.7.4, 12.12.2.1, 13.5.1 delete the para starting (#1321) and replace it with "NOTE---See 6.3.19 regarding prevention of key reinstallation attacks in 6.3.19 (SetKeys)

***Proposed Resolution: Revise as indicated in 11-20/0928r1 or Reject with a reason used for CID 2551*** *(See below)*

**Discussion**

6.3.19.1.4 Effect of receipt already discusses the rules for updating keys and checking for reinstallation

“(#1321)(#2550)When the Key Type is Group, IGTK, or BIGTK(#2116), and the key matches the GTK,

IGTK, or BIGTK(#2116), if any, installed as a result of EAPOL-Key frames (see 12.7.7.4 (Group key

handshake implementation considerations)) or exiting WNM sleep mode (see 11.2.3.16.1 (WNM sleep

mode capability)) receipt of this primitive shall have no effect. Otherwise, receipt of this primitive causes

the MAC to apply the keys as follows, subject to the MLME-SETPROTECTION.request primitive:”

Exit from WMN sleep mode is already covered here. So, 11.2.3.16.1 WNM sleep mode exit can simply reference this as suggested.

Ditto for group key installation (12.7.7.4), FILS key installation (12.11.2.1) and 13.5.1

[r1]

This comment is a duplicate of CID 2551 which was resolved as follows

REJECTED (PHY: 2019-03-13 22:24:13Z) - KRACK was the result of people not reading the standard fully and implementing a component protocol or API. IT is not reasonable to assume future implementers will do anything different. There does not seem to be a problem with being explicit and repetitive like this. In fact, it is kind of emphatic. So the combination of no existing problem and a problem created by accepting the proposed change means reject.

We could keep the same reason and **reject** this CID too **or** abbreviate the paragraph and **revise** it as suggested in this document while reminding the implementors to look at the details related to key reinstallation prevention in 6.3.19 (SetKeys). If additional keys are added to 6.3.19, the details repeated in each of these other locations do not have to be changed.

Accept suggested changes except for some minor rewording.

**Proposed Changes for a ‘Revise’ resolution**

***TGm Editor: Change 11.2.3.16.1 WNM Sleep mode capability p2195.5 as follows***

WNM sleep mode is a service that may be provided by an AP to its associated STAs. The WNM sleep mode is

not supported in an IBSS.

~~(#1321)To prevent key reinstallation attacks, a non-AP STA in which dot11WNMSleepModeActivated is true~~

~~shall maintain a copy of the most recent GTK, most recent IGTK and most recent BIGTK (#2116)installed~~

~~when exiting WNM sleep mode and shall not install a GTK, IGTK or BIGTK(#2116) when the key to be set~~

~~upon exiting WNM sleep mode matches either of the two maintained keys (see 6.3.19 (SetKeys)).~~

NOTE—See 6.3.19 (SetKeys) on key reinstallation attack prevention when exiting from WNM sleep mode.

WNM sleep mode enables an extended power…

***TGm Editor: Change 12.7.7.4 p2676.43 as follows***

**12.7.7.4 Group key handshake implementation considerations**

…

~~(#1321)To prevent key reinstallation attacks, the Supplicant shall maintain a copy of the most recent~~

~~GTK(#4470), most recent IGTK(#4470), and most recent BIGTK(#2116), installed as a result of receipt of~~

~~EAPOL-Key frames. The Supplicant shall not install a GTK, an IGTK or a BIGTK(#2116) when the key to be~~

~~set matches either of these two keys (see 6.3.19 (SetKeys)).~~

NOTE—See 6.3.19 (SetKeys) on key reinstallation attack prevention when installing group keys.

***TGm Editor: Change 12.11.2.1 p2700.5 as follows***

**12.11.2 FILS authentication protocol**

**12.11.2.1 General**

**…**

When a shared key is used for FILS authentication, and if the STA shares a valid rRK with the TTP, then EAPRP

as defined in IETF RFC 5295 and IETF RFC 6696 shall be used.

~~(#1321)To prevent key reinstallation attacks, the non-AP STA shall maintain a copy of the most recent GTK,~~

~~most recent IGTK and most recent BIGTK(#2116) installed as part of the FILS authentication protocol as if~~

~~they were installed as a result of receipt of EAPOL-Key frames (see 12.7.7.4 (Group key handshake~~

~~implementation considerations)) and shall refuse to update a GTK, IGTK or BIGTK(#2116) when the key to~~

~~be set matches either one of these two keys (see 6.3.19 (SetKeys)).~~

NOTE—See 6.3.19 (SetKeys) on key reinstallation attack prevention when keys are installed as part of FILS authentication protocol.

**…**

***TGm Editor: Change 12.11.2.1 p2722.63 as follows***

**13.5 FT protocol**

**13.5.1 Overview**

STAs with dot11FastBSSTransitionActivated equal to true shall support the FT protocol.

The FT protocol supports resource requests as part of the reassociation. The optional FT resource request

protocol (see 13.6 (FT resource request protocol)) supports resource requests prior to reassociation.

A STA shall not use any authentication algorithm except the FT authentication algorithm when using the FT

protocol.

~~(#1321)To prevent key reinstallation attacks, the non-AP STA shall maintain a copy of the most recent GTK,~~

~~IGTK, and BIGTK when present(#2116) installed as part of the FT protocol as if they were installed as a~~

~~result of receipt of EAPOL-Key frames (see 12.7.7.4 (Group key handshake implementation~~

~~considerations)) and shall refuse to update a GTK, IGTK, or a BIGTK(#2116) when the key to be set~~

~~matches either one of these two keys (see 6.3.19 (SetKeys)).~~

NOTE—See 6.3.19 (SetKeys) on key reinstallation attack prevention when keys are installed as part of FT protocol.

…