IEEE P802.11
Wireless LANs

|  |
| --- |
| Release Davy Jones |
| Date: 2018-11-11 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE | 3333 Scott boulevard Santa Clara, California,United States of America |  |  |
|  |  |  |  |  |

Abstract

“Release the Kracken: New Kracks in the 802.11 standard” describes a key reinstallation attack that bypasses the existing key reinstallation countermeasures. It also describes improved countermeasures to deal with it (see 6.3.2):

“A more efficient defense is to track the latest (integrity) group key installed in response to an EAPOL-Key frame, and the latest (integrity) group key installed in response a WNM-Sleep frame. This means that two normal group keys are saved, and two integrity group keys are also saved. When now receiving a new key in either an EAPOL-Key or WNM-Sleep frame, the new (integrity) group key must only be installed if it differs from both of the two saved (integrity) group keys. Additionally, we require that the client disconnects from the network if it did not receive a WNM-Sleep response frame when exiting sleep mode. We also recommend that a client deletes the current (integrity) group key before entering WNM-Sleep mode.”

***Discussion:***

Section 11.2.3.18.2 of Draft P802.11REVmd D1.0 already requires the non-AP STA to delete the current group and integrity group keys when entering WNM Sleep mode. But it does not instruct the STA to deauthenticate if it did not receive a WNM Sleep Mode Response after sending a WNM Sleep Mode Request. So it’s necessary to add text requiring that behavior.

It is also necessary to add text instructing the STA to maintain the values of both the GTK and IGTK installed by either exiting WNM Sleep mode or using EAPOL-Key frames and refuse to install a new (I)GTK key if the key to be installed is the same as any of the maintained GTKs or IGTKs. The simplest way to implement this is to add new text to 6.3.19.1.4 regarding this new requirement and to instruct the STA, in sections 11.2.3.18.1, 12.12.2, 12.7.7.4, and 13.5 to maintain both sets keys. Since the non-WNM Sleep mode case includes the Group Key Handshake, FILS, and FT, similar text is needed in all three to maintain a single pair of “non-WNM Sleep” keys.

***Instruct the editor to modify section 6.3.19.1.4 as indicated:***

**6.3.19.1.4 Effect of receipt**

When the Key Type is Group or IGTK, and the Key matches the existing GTK or IGTK installed from exiting WNM sleep mode (see 11.2.3.18.1 WNM Sleep Mode Capability) or matches the existing GTK or IGTK installed using EAPOL-Key frames (see 12.7.7.4 Group key handshake implementation considerations) 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 MLMESETPROTECTION. request primitive:

* The MAC uses the key information (as defined by the Key Type, Key ID, and Address parameters) for the transmission of subsequent frames to which the key applies (as defined by the Key Type, Key ID and Address parameters.
* The MAC installs the key with the associated Key ID such that received frames for that cipher, of the appropriate type, and containing the matching Key ID are processed using that key and its associated state information, subject to validation based on the Receive Sequence Count, if applicable.
* When the Key, Address, Key Type, and Key ID parameters identify a new key to be set, the MAC initializes the transmitter TSC/PN/IPN counter to 0. When the Key, Address, Key Type, and Key ID parameters identify an existing key, the MAC shall not change the current transmitter TSC/PN/IPN counter or the receiver replay counter values associated with that key.

***Instruct the editor to modify section 11.2.3.18.1 and 11.2.3.18.2 as indicated:***

**11.2.3.18.1 WNM Sleep Mode Capability**

 A STA in which dot11WNMSleepModeActivated is true may send a WNM Sleep Mode Request or WNM Sleep Mode Response frame to a STA within the same infrastructure BSS whose last received Extended Capabilities element contained a value of 1 for the WNM Sleep Mode field in the Extended Capabilities field. 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.

A non-AP STA in which dot11WNMSleepModeActivated is true shall maintain the most recent GTK and most recent IGTK installed when exiting WNM sleep mode and shall not install a GTK or IGTK with MLME-SETKEYS when the key to be set upon exiting WNM sleep mode matches either of the two maintained keys (see 6.3.19 Set Keys).

WNM sleep mode enables an extended power save mode for non-AP STAs in which a non-AP STA need not listen for every DTIM Beacon frame, and need not perform GTK/IGTK updates. A non-AP STA can sleep for extended periods as indicated by the WNM Sleep Interval field of the WNM Sleep Mode element, which is present in WNM Sleep Mode Request frames transmitted by the non-AP STA.

**11.2.3.18.2 WNM sleep mode non-AP STA operation**

To exit WNM sleep mode, the non-AP STA’s SME shall issue an MLME-SLEEPMODE.request primitive to send a WNM Sleep Mode Request frame with an Action Type field in the WNM Sleep Mode element set to “Exit WNM sleep mode” If a STA receives an unsolicited WNM Sleep Mode Response frame with the WNM Sleep Mode Response status value (see Table 9-219 (WNM Sleep Mode Response Status definition)) equal to 1, the STA exits WNM sleep mode. If the STA does not receive a WNM Sleep Mode Response frame after sending a WNM Sleep Mode Request frame, it shall issue an MLME-DEAUTHENTICATE.request primitive to deauthenticate from the current AP.

***Instruct the editor to modify section 12.7.7.4 as indicated:***

**12.7.7.4 Group key handshake implementation considerations**

If the Authenticator does not receive a reply to its messages, its shall attempt dot11RSNAConfigGroupUpdateCount transmits of the message, plus a final timeout. The retransmit timeout value shall be 100 ms for the first timeout, half the listen interval for the second timeout, and the listen interval for subsequent timeouts. If there is no listen interval or the listen interval is zero, then 100 ms shall be used for all timeout values. If it still has not received a response after this, then the Authenticator’s STA should use the MLME-DEAUTHENTICATE.request primitive to deauthenticate the STA.

To prevent key reinstallation attacks, the Supplicant shall maintain two keys: the most recent GTK key and most recent IGTK key installed using EAPOL-Key frames. The Supplicant shall not install a GTK or an IGTK with MLME-SETKEYS when the key to be set matches either of theese two keys (see 6.3.19 Set Keys).

***Instruct the editor to modify section 13.5.1 as indicated:***

**12.12.2 FILS authentication protocol**

**12.12.2.1 General**

The STA and AP perform key establishment using Authentication frames and perform key confirmation using (Re)Association Request and (Re)Association Response frames.

After exchanging Authentication frames, the STA and AP derive a shared and secret key that will be used to derive a set of secret keys (as defined in 12.12.2.5.2 (PMKSA key derivation with FILS authentication)) that are authenticated after exchanging (Re)Association Request and (Re)Association Response frames.

When a shared key is used for FILS authentication, and if the STA shares a valid rRK with the TTP, then EAP-RP as defined in IETF RFC 5295 and IETF RFC 6696 shall be used.

The non-AP STA shall maintain the most recent GTK and most recent IGTK installed as part of the FILS authentication protocol as if they were installed with EAPOL-Key frames (see 12.7.7.4 Group key handshake implementation considerations) and shall refuse to update a GTK or IGTK with MLME-SETKEYS when the key to be set matches either one of these two keys (see 6.3.19 Set Keys).

***Instruct the editor to modify section 13.5.1 as indicated:***

**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.

The non-AP STA shall maintain the most recent GTK and IGTK installed as part of the FT protocol as if they were installed with EAPOL-Key frames (see 12.7.7.4 Group key handshake implementation considerations) and shall refuse to update a GTK or IGTK with MLME-SETKEYS when the key to be set matches either one of these two keys (see 6.3.19 Set Keys).

**References:**

Vanheof, M. and Piessens, F., “Release the Kracken: New Kracks in the 802.11 standard”, Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pages 299-314.

[https://en.wikipedia.org/wiki/Kraken\_(Pirates\_of\_the\_Caribbean)#At\_World's\_End](https://en.wikipedia.org/wiki/Kraken_%28Pirates_of_the_Caribbean%29#At_World's_End)