IEEE P802.11  
Wireless LANs

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Resolution to Revmd CC25 CID 96 | | | | | |
| Date: 2017-07-20 | | | | | |
| Author(s): | | | | | |
| Name | Company | Address | Phone | email |
| Michael Montemurro | BlackBerry Ltd | 4701 Tahoe Blvd, Mississauga, ON. CANADA. L4W 0B4 | +1-289-261-4183 | mmontemurro@blackberry.com |

**Abstract**

This document contains the resolution to CID 96

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 96 | 2207 | 20 | 12.7.11.1 | Configuring a GTK for Tx/Rx instead of Tx -only on an AP is a security vulnerability as noted in the "Predicting, Decrypting, and Abusing WPA2/802.11 Group Keys" paper by Mathy Vanhoef and Frank Piessens (https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/vanhoef). This was certainly not the design that P802.11i tried to introduce, i.e., GTK is Tx-only on AP (and TX GTK in IBSS is similarly Tx-only on one each STA while other STAs use that as RX GTK). However, Figure 12-53 (Authenticator state machines, part 4) is indeed configuring GTK (and also IGTK for that matter) for both TX and RX in the SETKEYSDONE state. This is a serious flaw in the standard and if vendors follow that guidance without understanding how GTK/IGTK are supposed to be used, there is high risk of exposing vulnerabilities (allow unicast frames to be injected by any associated STA in an RSN to any other STA). | Remove cited sentenc In Figure 12-53, SETKEYSDONE state, replace "MLME-SETKEYS.request (GN, Tx/Rx, GTK[GN])" with "MLME-SETKEYS.request (GN, Tx, GTK[GN])" and "MLME-SETPROTECTION.request (Rx\_Tx, IGTK)" with "MLME-SETPROTECTION.request (Tx, IGTK)". For more complete cleanup, it should also be noted that MLME-SETKEYS.request does not actually take the direction parameter (Tx/Rx vs. Tx), i.e., the original GTK case from P802.11i is not correct; it should use MLME-SETPROTECTION.request like IGTK.e. |

Discussion:

* The commentor is correct in noting that the Authenticator only uses the GTK for TX.
* The figure does not align with the MLME primitives. This change corrects the alignment.

Proposed Resolution: Make changes in Figure 12-53 as indicated below.

\\

GInit

or

|  |  |
| --- | --- |
| GTK\_INIT | |
| GTK[0...N] = 0  GN = 1  GM = 2  GTK[GN] = CalcGTK() IGTK[ 0... M] = 0  GN\_igtk = 4  GM\_igtk = 5  IGTK[ GN\_igtk] = random key | |
|  | GTKAuthenticat |

# SETKEYSDONE

MLME-SETKEYS .request (GN, Group, GTK[ GN])

MLME-SETPROTECTION.request(Tx, Group)

MLME-SETKEYS .request (GN\_igtk, IGTK, IGTK[ GN\_igtk]) MLME-SETPROTECTION .request (Tx, IGTK )

GKeyDoneStations == 0 GTKRekey

GTKReKey = false Swap( GM. GN)

# SETKEYS

GKeyDoneStations = GNoStations GTK[ GN] = CalcGTK()

For each STA

if STA is in WNM sleep mode GKeyDoneStations --

else

GUpdateStationsKeys = true

GTKRekey

Swap(GM\_igtk, GN\_igtk ) IGTK[GN\_igtk ] = random key