IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Addressing the Issue of Nonce Reuse in 802.11 Implementations | | | | |
| Date: 2017-10-26 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE | 3333 Scott boulevard  Santa Clara, California,  United States of America |  |  |
| Jouni Malinen | Qualcomm |  |  | jouni@qca.qualcomm.com |

Abstract

This submission repeats normative language for implementers to prevent cryptographic replay counters from being reset during key installation events, an action that voids the security of the underlying cipher.

**Discussion**

Recent announcement of the KRACK attack [1] against implementations of the 802.11 standard [2] have highlighted the need for additional text to guide implementers. Currently, the specification of the CCMP cipher in section 12.5.3.1 states:

“CCM requires a fresh temporal key for every session. CCM also requires a unique nonce value for each frame protected by a given temporal key, and CCMP uses a 48-bit packet number (PN) for this purpose. Reuse of a PN with the same temporal key voids all security guarantees.”

And the definition of GCMP cipher in section 12.5.5.1 states:

“GCM requires a fresh temporal key for every session. GCM also requires a unique nonce value for each frame protected by a given temporal key, and GCMP uses a 96-bit nonce that includes a 48-bit packet number (PN) for this purpose. Reuse of a PN with the same temporal key voids all security guarantees.”

The requirement for nonce uniqueness needs to be repeated in the section of the standard which sets the nonce values to instruct implementers to prevent nonce resetting during key installation events.

***Instruct the editor to modify section 6.3.19 as indicated:***

**6.3.19 SetKeys**

**6.3.19.1.2 Semantics of the service primitive**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Type** | **Valid range** | **Description** |
| Key | Bit string | N/A | The temporal key value |
| Length | Integer | N/A | The number of bits in the key to be used |
| Key ID | Integer | 0-3 shall be used with WEP, TKIP, GCMP, CCMP,  4-5 with BIP; and  6-4095 are reserved | Key identifier |
| Key Type | Integer | Group, Pairwise, PeerKey, IGTK | Defines whether this key is a group key, pairwise key, PeerKey, or Integrity Group key. |
| Address | MAC Address | Any valid individual MAC address | This parameter is valid only when the Key Type value is Pairwise, when the Key Type value is Group and the STA is in IBSS, or when the Key Type value is PeerKey. |
| Receive Sequence Count | 8 octets | N/A | Value to which the RSC(s) is initialized. This parameter is valid only when the Key Type is Group or IGTK. |

**6.3.19.1.4 Effect of Receipt**

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 transmitted TSC/PN/IPN counter or the receiver replay counter values associated with that key.

**References:**

[1] Vanhoef M., and F. Piessens, “Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2”, Proceedings of the ACM Conference on Computer and Communications Security, Dallas, 2017

[2] IEEE Std 802.11-2016