IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Defense against multi-channel MITM attacks via Operating Channel Validation | | | | |
| Date: 2017-11-14 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Nehru Bhandaru | Broadcom Ltd. | 250 Innovation Drive, San Jose CA 95134 | +1 408 922 5924 | [nehru.bhandaru@broadcom.com](mailto:nehru.bhandaru@broadcom.com) |
| Thomas Derham | Broadcom Ltd. | 16340 W Bernardo Dr, San Diego CA 92127 |  | [thomas.derham@broadcom.com](mailto:thomas.derham@broadcom.com) |
| Mathy Vanhoef | KU Leuven |  |  | [mathy.vanhoef@cs.kuleuven.be](mailto:mathy.vanhoef@cs.kuleuven.be) |
| Ido Ouzieli | Intel Ltd. | 94 Em Hamoshavot Way, Petach-Tikva Israel 4970602 | +972 3 920 5700 | ido.ouzieli@intel.com |

Abstract

Several possible MITM attacks [1] that force an IV reset of a key, with associated security ramifications, have recently been disclosed against implementations of RSN specified in the 802.11 standard [2]. While there is no immediate known threat from deficiencies in RSNA protocols as currently specified, it would be prudent to provide some protection against MITM, in particular multi-channel MITM [3], in a future revision of the standard to protect against transparent (undetected), reliable and targeted MITM attacks. This submission provides normative language and recommendations to proactively provide protection against potential MITM in an RSN where an attacker can masquerade as a legitimate AP on one channel and a legitimate non-AP STA on another channel in a network. In this document, IEEE 802.11 draft revision ‘Draft P802.11REVmd\_D0.3.pdf’ [7] is used as the base version when describing the proposed changes.

**Comments addressed in r9 and r10 based on feedback during IEEE May 2018 meeting – May 8 PM1**

Ap should perhaps deauthenticate rather than disassociate if non-AP STA did not send the SA query. There should be a timeout for this – not the same as SA query timeout – The timeout is implementation specific (as it depends on channel condition, number of STAs, medium access time) It is hard to predict how many STAs are contending.

We are running out of RSNE capabilities. Need to wait/check if the assignment is available for OCVC. Also need an extension mechanism [to be handled separately]. If this document is adopted, ANA will be requested for the capabilitiy bit

**Comments addressed in r8 based on feedback from IEEE Mar 2018 meeting**

Modified approach for WNM Sleep Mode to use OCI element, only include for sleep mode exit

Clarified description for protected and unprotected channel switch cases

Introduced random delay or setting backoff counter for sending SA query subsequent to channel switch

Clarify leave/deauthenticate language if STA does not receive SA query response

Added clarification in discussion section that the proposal is not intended to address any known deficiencies in RSN protocols, but rather to make it harder for currently unknown vulnerabilities to be exploited using multi-channel approach

Renamed field containing secondary segment channel number for 80+80 to be consistent with 802.11 terminology

Improved language for validation of OCI

**Comments addressed in r4 based on feedback from IEEE Jan 2018 meeting**

Remove country string and use global operating class

Add OCI validation in mesh peering

Add OCI validation in WNM Sleep Mode frames

Concern related to switching back to pre-channel switch channel upon SA query timeout – propose leaving the BSS because there is an issue.

Octets for OCI in SA query – use fixed number instead of 0 or N – use 6

Add PICS support

Add page and line numbers where changes apply

**Editorial Instuctions**

Sections starting with Discussion – are outline discussion related to a topic

There are very few deletions, but the text is struck out

If text is added, it is underlined

***pnnnn.ll*** indicate location of change – *nnnn* is the page, *ll* is the line

**Discussion - General**

Several possible MITM attacks [1] that force an IV reset of a key, with associated security ramifications, have recently been disclosed against implementations of RSN specified in the 802.11 standard [2].

Proposals exist for emphasizing the requirement of nonce uniqueness and preventing IV reset [4] in the standard.

Multi-channel MITM is a way to **reliably** and **transparently** be in the middle of most of 802.11 data and management frame exchanges [5] and **target** specific receiving STAs. Slide 3 of [3] illustrates a multi-channel MITM attacker.

Some protection against multi-channel MITM is prudent, to proactively add hardening in order to alleviate the impact of the next potential significant disclosure. In Nov 2017 IEEE plenary, strawpolls indicated that TGm is generally supportive of defining a mechanism to protect aginst multi-channel MITM (See [6], Slide 18)

There is no (or very limited) cryptographic validation of Operating Channel information in the standard. This allows for a multi-channel MITM attacker to **transparently perpetrate attacks,** including but not limited to DOS**. For example**

* Buffer and replay frames
* Force retransmissions
* Suppress/discard specific frames – e.g. SA query responses can be discarded to remove PMF protection against unprotected disassociation or deauthentication
* Change unvalidated information in Beacons and Probe responses – e.g. capabilities, rates
* Alter AMSDU present in QoS data frames (when SPP AMSDU is not negotiated)
* Alter the timing measurement via FTM dependent range estimation

802.11 standard has limited protection against DOS – e.g. PMF use to detect injection of deauthentication or disassociation messages, RSNE confirmation (including capabilities PMF, SPP AMSDU).

It is noted that, in principle, the security properties of an RSNA should be unaffected by MITM manipulations such as those listed above – for example, the attacker should be limited to blindly repeating encrypted frames between the two peers. However, since a multi-channel MITM position may facilitate and reduce detectability of attacks using potential new vulnerabilities that might be found in the future against RSN protocols, the addition of multi-channel MITM protection would help reduce or prevent the viability of such vulnerabilities.

Multi-channel MITM protection can be facilitated by including and cryptographically integrity protecting Operating Channel Information (OCI) in all of the RSNA handshakes and other notifications that indicate a channel switch. In particular

* 4-way handshake (also covers PeerKeySTK handshake)
* GTK handshake
* FT handshake
* FILS key confirmation
* AMPE handshake
* WNM Sleep Mode exchange

An attacker may still get into MITM position temporarily – say by selectively jamming channel switch notification/messages for example, until the next handshake, BA agreement etc. that directly or indirectly validate the OCI. Such an attack would be detectable. Note that if both the AP and client pause data frame transmissions until the SA query has completed, the temporary MITM position caused by channel switches could be avoided in most situations.

When a STA supporting OCVC receives messages from a peer STA that advertises OCVC

* Any message where OCI is expected without an OCI is discarded.
* Any message with an OCI that does not match (same channel, and less than or equal to the indicated bandwidth of the operating class) the operating channel and bandwidth over which the frame is received is discarded.

***Instruct the editor to add to section 3. Definitions… definitions for OCI and OCVC***

***p198.35***

OCB outside the context of a BSS

OCI operating channel information

OCT on-channel tunneling

OCVC operating channel validation capable

OFDM orthogonal frequency division multiplexing

***Instruct the editor to add a subsection 12.2.x after 12.2.8 Requirements for robust management frame protection p2349.32***

**12.2.x Requirements for Operating Channel Validation**

When OCVC capability is present, a STA shall advertise this capability in RSNE and shall include operating channel information and validate the Operating Channel Information (OCI) received from an OCVC capable peer in certain protected messages used for key establishment and confirmation.

A STA with OCVC capability validates that the channel information in received OCI matches its current operating channel parameters by:

* Verifying that the maximum bandwidth used by the STA to transmit or receive PPDUs to/from the peer STA from which the OCI was received is no greater than the bandwidth of the operating class specified in the Operating Class field of the received OCI
* Verifying that the primary channel used by the STA to transmit or receive PPDUs to/from the peer STA from which the OCI was received is equal to the Primary Channel Number field (for the corresponding operating class)
* Verifying that, when 40 MHz bandwidth is used by the STA to transmit or receive PPDUs to’from the peer STA from which the OCI was received, the non-primary 20 MHz used matches the operating class (i.e. upper/lower behavior) specified in the Operating Class field of the received OCI
* Verifying that, if operating an 80+80 operating class, the frequency segment 1 channel number used by the STA to transmit or receive PPDUs to/from the peer STA from which the OCI was received is equal to the Frequency Segment 1 Channel Number field of the OCI.

If a STA with OCVC capability receives a frame from a peer STA which is not on the same primary channel (or frequency segment 1 channel number) used by the STA to receive PPDUs from the peer STA, or has bandwidth that exceeds the maximum bandwidth used by the STA to receive PPDUs from the peer STA, the frame is discarded.

**Discussion – Capability Indication**

In order to support the new feature in 802.11 standard to detect a multi-channel MITM, and be interoperable with implementations that do not support the feature some capability indication and configuration support is needed.

A new MIB variable dot11RSNAOperatingChannelValidationActivated is proposed along with capability advertisement over the air. The capability advertisement naturally fits into RSN capabilities – a new capability OCVC (Operating Channel Validation Capable) is proposed.

***Instruct the editor to modify MIB entry for dot11StationConfigEntry p3514.62 as indicated:***

*Add* ‘dot11RSNAOperatingChannelValidationActivated TruthValue’ *to the entry*

***Instruct the editor to add to management frame protection MIBS p3538.52***

dot11RSNAOperatingChannelValidationActivated OBJECT-TYPE

SYNTAX TruthValue

MAX-ACCESS read-write

STATUS current

DESCRIPTION

"This is a control variable.

It is written by an external management entity.

Changes take effect as soon as practical in the implementation.

This variable indicates whether this STA has enabled operating channel validation in an RSNA"

DEFVAL { false }

::= { dot11StationConfigEntry **TBD**}

***Instruct the editor to add*** dot11RSNAOperatingChannelValidationActivated ***to dot11DMGComplianceGroup object group p4013.5***

***Instruct the editor to add*** dot11RSNAOperatingChannelValidationActivated ***to dot11ProtectedManagementFrameGroup object group p4015.14***

***Instruct the editor to replace the reserved block B14-B15 in Figure 9-285 p1036.34 reproduced below***

****

with the following (subject to ANA assignment)

B14

B15

|  |  |
| --- | --- |
| Operating Channel Validation Capable (OCVC) | Reserved |

1 1

***Instruct the editor to add a description for bit 14 as follows on p1038.9***

--- Bit 14: Operating Channel Validation Capable. This subfield is set to 1 to indicate that the STA supports operating channel validation by including Operating Channel Information (OCI) in RSNA exchanges and validates the information when received from another STA that indicated this capability.

**Discussion – OCV Required (Policy)**

The standard could also support advertisement and enforcement of Operating Channel Validation Required (OCVR) policy.

A STA can enforce this policy based on some configuration outside the scope of the standard. Such as STA can discard the frames where the peer STA does not support OCVC or OCI is expected but missing without any further indication to MLME or the peer STA over the air.

This document does not propose this capability.

**Discussion – Operating Channel Information (OCI)**

Channel information, that needs to be validated, is typically specified by operating class (Annex E [7]) and channel number in the standard e.g. Extended Channel Switch Announcement (Figure 9-360 [7]). Since use of the country string is being deprecated in favor of sole use of the global operating classes table, operating classes from the global table are advertised in Beacons and probe responses. Thus validating OCI includes validating the global operating class (that also defines bandwidth and primary channel upper/lower behavior), and channel number. Specifying operating class, primary channel and the frequency segment 1 channel number should be sufficient to indicate the operating channel information to cover 80MHz and 80+80/160MHz cases where only center frequency indices are specified in the operating class table.

For example, for a VHT 80MHz BSS operating with 80 MHz Ch 155 (i.e. 5735-5815 MHz), which is operating class 128, channel center frequency index 155.

* An AP can choose its primary 20 anywhere in the 80 MHz, so let's say it chooses Ch 153 (the 2nd 20 MHz channel). OCI can have the following values set:
  + Operating Class field = 128
  + Primary Channel Number = 153
  + Frequency Segment 1 Channel Number = 0 (since not 80+80)

A VHT 80+80 MHz BSS operating with 80 MHz Ch 155 (i.e. 5735-5815 MHz), which is operating class 128, channel center frequency index 155 for the primary segment (frequency segment 0) and 42 for the secondary segment (frequency segment 1).

* An AP can choose its primary 20 anywhere in the primary 80 MHz, so let's say it chooses Ch 153 (the 2nd 20 MHz channel). OCI can have the following values set:
  + Operating Class field = 128
  + Primary Channel Number = 153
  + Frequency Segment 1 Channel Number = 42

The Operating Class indicated in the OCI element must represent the widest bandwidth currently being used by the transmitting STA. For example, if a VHT 80 MHz AP has an associated STA that only supports 20 MHz, the OCI element from the AP must indicate the 80 MHz Operating Class. On the other hand, if a non-AP STA supports 80 MHz but the AP supports only 40 MHz and the AP is sending the PPDU containing OCI element at 20 MHz bandwidth in the primary sub-channel, the OCI element must indicate the 40 MHz Operating Class since that is the widest bandwidth the AP (transmitting STA) is using.

It is not clear any existing information element can be used as is for this purpose. It does not appear so, for example in the Extended Channel Switch Announcement element, there is extraneous information related to applicable operation which is not relevant for this purpose.

This information needs to be validated at least in 4-way handshakes, GTK handshakes, FT re-association, FILS key confirmation.

There is a need to define an information element, KDE and FTIE subelement to carry the operating channel information.

Another possibility is to include include OCI information or OCI element directly in the handshakes(EAPOL) messages, but OCI KDE provides better interoperability with existing implementations that use key descriptors– in that OCI KDE can simply be inserted by an OCVC STA, and the non-OCVC STA will ignore it.

***Instruct the editor to add a row for OCI element to Table 9-88 Element IDs in section 9.4.2 Elements, subsection 9.4.2.1 General***

******

add the row ***p926.38***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Operating Channel Information (OCI) Element | 255 | ANA | Yes | No |

***Instruct the editor to add the subsection 9.4.2.xxx OCI Element description as follows p1347.19***

9.4.2.xxx OCI Element

The OCI element is shown in Figure TBD (OCI element format)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Element ID | Length | Element ID Extension |  | Operating  Class | Primary Channel Number | Frequency Segment 1  Channel  Number |

Octets: 1 1 1 1 1 1

**Figure 9-XXX OCI element format**

The Element ID and Length fields are defined in 9.4.2.1 (General)

Operating Class field is set to the global operating class that corresponds to the widest bandwidth currently being used by the transmitting STA. See Annex E, Table E-4 for description of the global operating classes.

Primary Channel Number field is set to the primary channel being used currently. Primary Channel Number is one of the channels from the row corresponding to the operating class as defined in Annex E or the primary 20 MHz (sub)channel allowed for HT or non-HT operation for operating classes that specify only channel center frequency indices.

Frequency Segment 1 Channel Number field is set to the channel center frequency index of the secondary segment (frequency segment 1) being used currently, if applicable, or set to 0 otherwise. Frequency Segment 1 Channel Number is one of the center frequency indices from the row corresponding to the operating class as defined in Annex E.

***Instruct the editor to add a row for OCI KDE in table 12-7 --- KDE after the Multi-band Key ID KDE and adjust the reserved elements accordingly p2453.50***

******

|  |  |  |
| --- | --- | --- |
| 00-0F-AC | ANA | Operating Channel Information (OCI) KDE |

***Instruct the editor to add the following description for the OCI KDE at the end of section 12.7.2 p2457.11***

The format of the OCI KDE is shown in figure 12-XX (OCI KDE)

|  |  |  |  |
| --- | --- | --- | --- |
|  | Operating Class | Primary Channel Number | Frequency Segment 1 Channel Number |

Octets: 1 1 1

The definitions of Operating Class, Primary Channel Number, and Frequency Segment 1 Channel Number are the same as those described in section 9.4.2.xxx OCI Element.

***Instruct the editor to add a row for OCI FTE subelement in table 9-175 --- Subelement IDs after IGTK subelement and adjust the reserved elements accordingly p1089.58***

******

|  |  |
| --- | --- |
| ANA | Operating Channel Information (OCI) |

***Instruct the editor to add description of OCI subelement format at the end of section 9.4.2.48 Fast BSS Transition Element (FTE) as follows p1091.4***

OCI subelement contains the operating channel information which is integrity protected (see procedures in x.x.x FT re-association) as defined in Figure 9-xxx (OCI subelement format)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Subelement ID | Length | Operating Class | Primary Channel Number | Frequency Segment 1 Channel Number |

Octets: 1 1 1 1

The definitions of Operating Class, Primary Channel Number, and Frequency Segment 1 Channel Number are the same as those described in section 9.4.2.xxx OCI Element.

**Discussion – What frames/exchanges include OCI**

OCI should be included in 4-way handshake M2 and M3 messages

OCI should be included in GTK handshake messages

OCI should be included in FT re-association messages – request and response

OCI should be included in FILS re-association messages – request and response

OCI should be included in AMPE handshake messages, i.e. Mesh Peering Management Frames

OCI should be included in WNM Sleep Mode messages – request and response

OCI is probably not needed in TDLS messages – as it would be validated on Infra initially, and subsequent channel switch request contains channel/operating class information that can be validated.

Channel switch announcements contain target/new channel information. These would be protected by PMF – assuming PMF is being used, but PMF does not apply to beacons/probe responses which can contain a channel switch announcement element. A reasonable position is to require PMF when OCV protection is required for channel switch – at least protect PMF environments – PMF is likely to be available in most devices now or in the near future. SA query can be extended and used after a channel switch to validate OCI

FTM exchanges would be indirectly protected as they do not negotiate the channel currently. If channel is confirmed by another secure handshake, multi-channel MITM threat would be alleviated.

***Instruct the editor to add the following at the end of section 12.7.4 EAPOL-Key-frame notation to the list of possible DATAKDs p2459.39***

OCI KDE is a KDE containing Operating Channel Information

***Instruct the editor to modify 4-way handshake subsection 12.7.6.1 General as follows p2460.4***

Message 2: Supplicant  Authenticator: EAPOL-Key(0,1,0,0,P,0,0,SNonce,MIC,DataKD\_M2)

where DataKD\_M2 = RSNE for creating PTK generation or peer RSNE, Lifetime

KDE, SMKID KDE (for sending SMKID) for STK generation, and OCI KDE when dot11RSNAOperatingChannelValidationActivated on the Supplicant

Message 3: Authenticator  Supplicant:

EAPOL-Key(1,1,1,1,P,0,KeyRSC,ANonce,MIC,DataKD\_M3)

where DataKD\_M3 = RSNE,GTK[N] for creating PTK generation or initiator RSNE,

Lifetime KDE for STK generation, and OCI KDE when dot11RSNAOperatingChannelValidationActivated on the Authenticator

…

Here, the following assumptions apply:

…

— Lifetime represents the expiration timeout used for exchanging SMK expiration value.

— OCI KDE represents the current operating channel information using which the EAPOL frame is sent

***Instruct the editor to modify subsection 12.7.6.3 4-way handshake message 2 by adding at the end of*** Key Data = ***text at the end of page 2462.64***

— OCI KDE when dot11RSNAOperatingChannelValidationActivated on the Supplicant

***Instruct the editor to modify subsection 12.7.6.4 4-way handshake message 3 by adding at the end of Key Data = text on page 2465.25***

— OCI KDE when dot11RSNAOperatingChannelValidationActivated on the Authenticator

***Instruct the editor to modify Group key handshake subsection 12.7.7.1 General as follows p2471.35***

Message 1: Authenticator  Supplicant:

EAPOL-Key(1,1,1,0,G,0,Key RSC,0, MIC,GTK[N],IGTK[M], OCI)

Message 2: Supplicant  Authenticator: EAPOL-Key(1,1,0,0,G,0,0,0,MIC,~~0~~ OCI)

…

Here, the following assumptions apply:

…

The MIC is computed over the body of the EAPOL-Key frame (with the MIC field zeroed for the

computation) using the KCK defined in 12.7.1.3 (Pairwise key hierarchy).

— OCI KDE represents the current operating channel information using which the EAPOL frame is sent. OCI KDE is included when dot11RSNAOperatingChannelValidationActivated is true on the STA sending the message.

***Instruct the editor to modify subsection 12.7.7.2 Group key handshake message 1 by adding at the end of*** Key Data = ***text on page 2472.41***

— OCI KDE when dot11RSNAOperatingChannelValidationActivated on the Authenticator

***Instruct the editor to modify subsection 12.7.7.3 Group key handshake message 2 by adding at the end of*** Key Data = ***text on page 2473.36 as follows***

Key Data = ~~none required~~

— OCI KDE when dot11RSNAOperatingChannelValidationActivated on the Authenticator

**Discussion – How is OCI validation performed in each case**

In 4-way handshake and GTK handshake, OCI is obtained from OCI KDE

In FT re-association messages – OCI is obtained from FTIE OCI subelement

In FILS re-association messages – OCI is obtained from OCI element

In mesh AMPE handshake – OCI is obtained from OCI element

In WNM Sleep Mode messages – OCI is obtained from OCI element

Channel switch announcements via announcement frames using PMF – OCI is obtained from the channel switch information in the frame

Channel switch announcements via announcement using the channel switch announcement element and not PMF, but PMF applies to the association - SA query follows – SA query frame contains the OCI element.

TDLS channel switch request – if response is not received, shoud the link be torn down? An attacker may block the request or response but not be able to generate a response. If attacker blocked request, no channel switch will take place. If attacker blocks response channel switch will take place on the respondor, but not on the requestor because it did not get a response. It would be reasonable to teardown the link if there is no response to the request.

To avoid unnecessary complexity of specification and implementation, it should not be permitted to switch channels during the 4-way handshake or other security handshakes

FT initial association also uses the 4-way handshake (FT 4-way handshake - 13.4.2 FT initial mobility domain association in an RSN). FTE is already present in M2 and M3 messages. The validation should be the same using OCI subelement in FTE

***Instruct the editor to modify subsection 12.7.6.1 General (4-way handshake) as follows***

***p2460.57***

If dot11RSNAOperatingChannelValidationActivated is true and a channel switch is requested while the handshake is in progress, the handshake should be aborted.”

***Instruct the editor to modify subsection 12.7.6.3 4-way handshake message 2 p2463.6 starting with*** On reception of message 2… ***as follows***

On reception of message 2, the Authenticator checks that the key replay counter corresponds to the

outstanding message 1. If not, it silently discards the message.

If dot11RSNAOperatingChannelValidationActivated is true and Supplicant RSNE indicates OCVC capability, the Authenticator silently discards message 2 if any of the following are true

* OCI KDE or FTE OCI subelement is missing in the message
* Channel information in the OCI does not match current operating channel parameters (see clause 12.2.x)

Otherwise, the Authenticator:

***Instruct the editor to modify subsection 12.7.6.4 4-way handshake message 3 p2466.28 starting with*** On reception of message 3… ***as follows***

***2466.28***

On reception of message 3, the Supplicant silently discards the message if the Key Replay Counter field

value has already been used or if the ANonce value in message 3 differs from the ANonce value in

message 1.

If dot11RSNAOperatingChannelValidationActivated is true and Authenticator RSNE indicates OCVC capability, the Supplicant silently discards message 3 if any of the following are true

* OCI KDE or FTE OCI subelement is missing in the message
* Channel information in the OCI does not match current operating channel parameters (see clause 12.2.x)

The Supplicant also:

***Instruct the editor to modify subsection 12.7.7.1 General (Group Key Handshake) as follows***

***p2471.59***

If dot11RSNAOperatingChannelValidationActivated is true and a channel switch is requested while the handshake is in progress, the handshake should be aborted.”

***Instruct the editor to modify subsection 12.7.7.2 Group key handshake message 1 p2472.49 by adding bullet b) in the paragraph starting with*** On reception of message 1… ***as follows***

b) If dot11RSNAOperatingChannelValidationActivated is true and Authenticator RSNE indicates OCVC capability, the Supplicant silently discards message 1 if any of the following are true

* OCI KDE is missing in the message
* Channel information in the OCI KDE does not match current operating channel parameters (see clause 12.2.x)

***and appropriately renumber bullets b, c, and d and c, d and e respectively***.

***Instruct the editor to modify subsection 12.7.7.3 Group key handshake message 2 p2473.42 by adding bullet b) in the paragraph starting with*** On reception of message 2… ***as follows***

b) If dot11RSNAOperatingChannelValidationActivated is true and Supplicant RSNE indicates OCVC capability, the Authenticator silently discards message 2 if any of the following are true

* OCI KDE is missing in the message
* Channel information in the OCI KDE does not match current operating channel parameters (see clause 12.2.x)

***and appropriately renumber the current bullet b as c***.

**Discussion – OCI validation for FT**

FTE is already present in initial mobility domain associatiation – M2 and M3 messages

OCI should be included in FT subelement and validated, similar to OCI KDE validation in non-FT 4-way handshake messages. See proposed changes related to 4-way handshake

FT authentication sequence message 3 and message 4 contain FTE and FTE is included in the MIC calculcation. Similarly, FT re-association request and response also contain FTE and the corresponding MIC that includes FTE.

FT OCI element should be included in the FTE that is present messages 3 and 4 or FT authentication sequence as well as FT re-association request and response frames. OCI should be validated during FT negotiations.

Over the DS FT protocol does not use FT authentication sequence. FT requests forwarded to target AP by the current AP do not have a MIC.

***Instruct the editor to modify subsection 13.7.1 FT reassociation in an RSN as follows***

…

The elements in the frame, the element contents, and the MIC calculation shall be as given in 13.8.4 (FT authentication sequence: contents of third message).

***p2555.52***

The R1KH of the target AP verifies the MIC in the FTE in the Reassociation Request frame and shall

discard the request if the MIC is incorrect. If dot11RSNAOperatingChannelValidationActivated is true and the FTO indicates OCVC capability, the target AP shall ensure that OCI subelement of the FTE matches by ensuring that all of the following are true

* OCI subelement is present
* Channel information in the OCI matches current operating channel parameters (see clause 12.2.x)

Otherwise, the AP shall reject the Reassociation Request frame with status code STATUS\_INVALID\_FTE

…

The S1KH of the FTO verifies the MIC in the FTE in the Reassociation Response frame and shall discard

the response if the MIC is incorrect. If dot11RSNAOperatingChannelValidationActivated is true and the target AP indicates OCVC capability, FTO shall ensure that OCI subelement of the FTE matches by ensuring that all of the following are true

* OCI subelement is present
* Channel information in the OCI matches current operating channel parameters (see clause 12.2.x)

Otherwise, the FTO reject the Reassociation Response frame by discarding the frame.

***Instruct the editor to modify subsection 13.8.4 FT authentication sequence: contents of third message*** ***as follows***

The FTE shall be present only if dot11RSNAActivated is true…

— (#114) When the negotiated AKM is 00-0F-AC:16 or 00-0F-AC:17, the MIC field is set to 0. ***p2560.27***

— If dot11RSNAOperatingChannelValidationActivated is true and Authentictor indicates OCVC capability, the supplicant shall include FT OCI subelement in FTE.

…

***Instruct the editor to modify subsection 13.8.5 FT authentication sequence: contents of fourth message*** ***as follows***

The FTE shall be present only if dot11RSNAActivated is true…

… ***p2561.11***

— If dot11RSNAOperatingChannelValidationActivated is true and Supplicant indicates OCVC capability, the Authenticator shall include FT OCI subelement in FTE.

— When this message of the authentication sequence appears in a Reassociation Response frame, the

Optional Parameter(s) field in the FTE may include the GTK and IGTK subelements. If a GTK or an

IGTK are included, (#114) it shall be encrypted.…

**Discussion – OCI validation for FILS**

FILS has an authentication phase that exchanges nonces, etc including agreement on PMK to use. Key confirmation phase follows using (re)association messages.

(re)association frames have clear AAD and encrypted data following FILS session element.

OCI element should be added to these frames and OCI validated relative to channel in use and channel used for the authentication messages.

***Instruct the editor to modify the element table for reassociation request Table 9-35—Reassociation Request frame body (continued) – on page 817.16 by adding a row for OCI element***



|  |  |  |
| --- | --- | --- |
| ANA | OCI Element | OCI element is present if dot11FILSActivated and dot11RSNAOperatingChannelValidationActivated are both true; otherwise not present. |

***Instruct the editor to modify the element table for association response Table 9-36—Reassociation Response frame body (continued) – on page 820.32 by adding a row for OCI element***

******

|  |  |  |
| --- | --- | --- |
| ANA | OCI Element | OCI element is present if dot11FILSActivated and dot11RSNAOperatingChannelValidationActivated are both true; otherwise not present. |

***Instruct the editor to modify subsection 12.12.2.6.2 (Re)Association Request for FILS key confirmation as follows***

The STA constructs a (Re)Association Request frame for FILS authentication per 9.3.3.6 (Association

Request frame format) and 9.3.3.8 (Reassociation Request frame format). Hash algorithms(#307) are used to

generate the FILS Key Confirmation element and the specific hash algorithm(#307) depends on the AKM

negotiated (9.4.2.25.3 (AKM suites)). **p2529.54**

If dot11RSNAOperatingChannelValidationActivated is true and AP indicates OCVC capability, the STA shall include OCI element in the request

…

***p2530.58***

(#114) The AP compares FILS session of the received (Re)Association Request frame with the FILS session

that was used to identify the FILS session in the Authentication frames. If they differ, authentication

exchange fails.

If dot11RSNAOperatingChannelValidationActivated is true and the STA indicates OCVC capability in the RSNE in the request, AP shall validate the OCI element in the request by ensuring that all of the following are true

* OCI element is present
* Channel information in the OCI matches current operating channel parameters (see clause 12.2.x)

Otherwise, the AP rejects the request by discarding the frame.

***Instruct the editor to modify subsection 12.12.2.6.3 (Re)Association Response for FILS key confirmation as follows***

…

The AP constructs a Key Delivery element indicating the current GTK and Key RSC, the current IGTK and

IPN if management frame protection is enabled. The GTK is carried in a GTK KDE with Tx subfield equal

to 0. The IGTK and IPN are carried in an IGTK KDE. The AP puts this element into the (Re)Association

Response frame.

***p2531.62***

If dot11RSNAOperatingChannelValidationActivated is true and STA indicates OCVC capability, the AP shall include OCI element in the response.

…

If dot11RSNAOperatingChannelValidationActivated is true and the AP indicates OCVC capability in its RSNE, the STA shall validate the OCI element in the response by ensuring that all of the following are true

* OCI element is present
* Channel information in the OCI matches current operating channel parameters (see clause 12.2.x)

Otherwise, the STA shall discard the frame.

***p2532.64***

The STA decrypts and verifies the received (Re)Association Response frame with the AEAD algorithm as

defined in 12.12.2.5 (Key establishment with FILS authentication) with the KEK as the key. The AAD is…

**Discussion – OCI validation after unprotected or protected channel switch**

First, it is noted that unprotected CSA channel switches that occur during handshakes may be vulnerable. In principle, while it may be an edge case, the following type of attack may be possible:

AP sends Msg1 to the client

Client sends Msg2 to the AP

Attacker forges CSA to make the client switch channels. No keys are installed yet, so client might just accept the CSA

AP sends Msg3. Does not arrive, and AP will retransmit another Msg3.

Attacker forges another CSA to make the client switch back to the original channel

Attack forwards both Msg3’s to the client (possibly after manipulating them).

The channel used to send Msg2 is the same as the channel that Msg3 is received on, so even with OCI validation the two Msg3’s would be accepted. (Note this would have resulted in a key reinstallation for old vulnerable clients).

Therefore, it should be stated that the handshake needs to be aborted if that happens during the handshake.

Second, although a channel switch announcement can be PMF protected by sending it in a robust (group) Action frame (e.g. Extended Channel Switch Announcement frame), many implementations (also) send the announcement unprotected in beacons. A STA that switches channel in response to an unprotected channel switch announcement (without verifying it against a protected announcement – if such exists) is susceptable to the multi-channel MITM attacker.

Therefore, a STA should initiate SA Query procedure with OCI after an unprotected channel switch to confirm the operating channel. It is necessary to specify a randomized delay before initiating SA Query, to prevent a collision scenario where a large number of associated STAs switch channel at the same time (in response to CSA), hear the first Beacon on the new channel at the same time, see the channel idle and then all attempt to transmit SA Query request at the same time. An AP may choose to disassociate or deauthenticate OCVC capable STAs if such an SA Query was not received (or it receives it but its decoding/decryption fails).

If a valid response is received with OCI information that does not match the current operating channel, the STA should leave the BSS.

Should there be a timeout for SA query response? If valid response is not received after certain time, the STA should deauthenticate from the BSS.

Any ongoing SA queries for older channel switch announcements should be abandoned when initiating a SA query to validate a new channel switch announcement.

In addition, it is possible that even if the channel switch announcement was sent protected, an attacker might target and intercept the packet, allowing the attacker to assume a MITM position on the AP’s original channel once the AP has switched to its target channel. Although this is a co-channel attack which is not in general in the scope of this submission, it may result in a multi-channel MITM position. Therefore, the STA should also perform SA query after channel switch even if the CSA was protected, and the AP may pause data transmission/reception until it receives the SA query to ensure the STA has also moved to the new channel.

Note that, even with SA Query and pause of data transmission/reception in place, an edge case may still be possible as follows:

1. Attacker blocks CSA frames towards the client (e.g. using a selective jammer)

2. AP switches channels

3. Client sends data frames on old channel, they don’t reach the original AP, and attacker stores these frames

4. Attacker now sends CSA frames to the client

5. Client switches channel and performs SA query successfully

6. Attacker can manipulate the previously stored data frames and forward them to the AP

Approaches to address this use case could include the AP explicitly confirming (using protected exchange) that the STA received the CSA prior to making the channel switch, or including Tx replay counter values in the SA query so that the delayed frames would not be accepted. However, introducing additional exchanges with each STA prior to channel switch may not be appropriate when channel switch timing is bound by regulatory requirements, and additional checks on replay counters add complexity. It is noted that typically (unprotected) CSA is sent in multiple consecutive beacon frames (in some cases supplemented by protected unicast CSA transmission), and therefore blocking of all CSA elements/frames is practically hard without causing the STA to detect beacon loss and initiate scan and (re)association in any case.

To summarize:

1.      If STA received a protected CSA – the STA should perform SA Query after switching

2.      If a protected CSA was not sent, or the STA missed the protected CSA but identified the not-protected CSA (Beacon) – the STA should perform SA Query after switching

3.      If STA missed all protected and/or unprotected CSAs due to being in WNM sleep – WNM OCI solves this case: if MITM attacker is on the original channel, OCI validation will fail; if STA scans and discovers the AP on the new channel, WNM OCI will succeed or the STA will re-attempt association anyway

4.      If STA missed all protected CSA and unprotected CSAs due to other reasons (including block by the attacker) – STA has no reason to transmit SA query, AP can take action based on SA query not being received. In typical case, it is unlikely all CSA transmissions will be missed or can be blocked

***Instruct the editor to modify the section 11.9.8.2 Selecting and advertising a new channel in a non-DMG infrastructure BSS as follows***

A STA that receives a Channel Switch Announcement element may choose not to perform the specified switch, but to take alternative action. For example, it may choose to move to a different BSS. An AP shall deauthenticate non-AP STAs that have indicated OCVC capability, are not in WNM Sleep, and have failed to send an SA query within an implementation specific timeout following a channel switch. An AP should pause the transmission and reception of Data frames until the SA query procedure has completed successfully for additional protection.

***p2107.18***

If dot11RSNAOperatingChannelValidationActivated is true and a channel switch is requested while the handshake is in progress, the handshake should be aborted

***Instruct the editor to modify the MBSS section 11.9.8.4.3 Processing channel switch announcement***

***p2110.19***

A mesh STA that receives a Channel Switch Announcement element may choose not to perform the

specified switch, but to take alternative action. For example, it may choose to move to a different MBSS.

If dot11RSNAOperatingChannelValidationActivated is true and a channel switch is requested while the handshake is in progress, the handshake should be aborted

***Instruct the editor to modify the section 11.10.3.2 Selecting and advertising a new channel in an infrastructure BSS as follows***

…

When a STA with dot11DSERequired equal to false receives an Extended Channel Switch Announcement

element, it may choose not to perform the specified switch, but to take alternative action. For example, it

might choose to move to a different BSS.

***p2114.35***

If dot11RSNAOperatingChannelValidationActivated is true and a channel switch is requested while a security handshake is in progress, the handshake should be aborted.

If the STA chooses to perform the specified switch and dot11RSNAOperatingChannelValidationActivated is true and the AP has indicated OCVC capability, after switching to the new channel and allowed to transmit on the new channel, the STA shall wait a random uniformly-distributed delay between 0 and 5 TUs, and then initiate the SA query procedure. This procedure shall be initiated whether or not the switch was based on a protected management frame that contained the new operating channel information. The STA may pause Data frame transmission and may drop any received Data frames until the SA query procedure has completed successfully for additional protection.

If a STA initiates SA query procedure to validate a channel switch, any existing SA query procedure for channel switch validation shall be abandoned.

***Instruct the editor to modify the subsection 11.14 SA Query procedures as follows***

…

***p2153.1***

A STA that supports the SA Query procedure and receives an SA Query Request frame shall respond with

an SA Query Response frame if none ~~unless either~~ of the following are true:

— the STA is not currently associated to the STA that sent the SA Query Request frame

— the STA has sent a (Re)Association Request frame within dot11AssociationResponseTimeOut but

has not received a corresponding (Re)Association Response frame

— dot11RSNAOperatingChannelValidationActivated is true and the sending STA had indicated OCVC capability in its association and either

* OCI element is not present in the request
* Operating channel information indicated does not match the current channel information (see clause 12.2.x)

A STA that responds with an SA Query Response frame to a STA that indicated OCVC capability shall include OCI element in the response frame if dot11RSNAOperatingChannelValidationActivated is true.

When a non-AP or non-PCP STA receives the SA Query Response frame from a STA that indicated OCVC capability, it shall ensure that OCI element is present in the response and the channel information in the OCI element matches current operating channel parameters (see clause 12.2.x); Otherwise, the receiving STA shall deem the response as invalid and discard it.

If a non-AP or non-PCP STA initiated an SA Query procedure following a channel switch and does not receive the SA Query Response frame from a STA that indicated OCVC capability within dot11AssociationSAQueryMaximumTimeout TUs from the beginning of the SA Query procedure, it shall deauthenticate from the BSS.

…

***Modify Figure 9-824—SA Query Request frame Action field format as follows p1450.7***



|  |  |  |  |
| --- | --- | --- | --- |
| Category | SA Query Action | Transaction Identifier | OCI Element |

Octets: 1 1 2 6

***Modify Figure 9-825—SA Query Response frame Action field format as follows p1450.24***



|  |  |  |  |
| --- | --- | --- | --- |
| Category | SA Query Action | Transaction Identifier | OCI Element |

Octets: 1 1 2 6

***Instruct the editor to modify subsection 9.6.10.2 SA Query Request frame as follows p1450.23***

…

The Transaction Identifier field is a 16-bit non-negative counter value set by the STA sending the SA Query

Request frame to identify any outstanding request/response transaction.

OCI element field is OCI Element (section 9.4.2.xxx OCI Element) and is included if dot11RSNAOperatingChannelValidationActivated is true.

***Instruct the editor to modify subsection 9.6.10.3 SA Query Response frame as follows p1450.46***

…

The Transaction Identifier field is set to the same value as the Transaction Identifier field in the

corresponding SA Query Request frame.

OCI element field is OCI Element (section 9.4.2.xxx OCI Element) and is included if dot11RSNAOperatingChannelValidationActivated is true

**Discussion – OCI validation for Mesh**

When security is enabled for Mesh peering, the security association is established using Authenticated Mesh Peering Exchange (AMPE), subsequent to SAE or 802.1X authentication.

In the AMPE handshake, OCI element should be added to the Mesh Peering Open and Confirm frames. It is not required for the Close frame. The OCI element should be positioned (when present) above the MIC element so that it is part of the input AAD when calculating the value of the MIC field in the MIC element – therefore it will be MIC protected but not encrypted.

Note: Per Section 14.5.3, the third component of the input AAD is equal to the contents of the mesh peering Management frame from the category (inclusive) to the MIC element (exclusive).

***Instruct the editor to modify the section 9.6.16 Self-protected Action frame details as follows***

* Mesh Peering Open frame details

***p1493.56***

The MIC element appears prior to the Authenticated Mesh Peering Exchange element in the Mesh Peering Open frame. The information following the MIC element through to the end of the Mesh Peering Open frame body is encrypted and authenticated (see 14.5 (Authenticated mesh peering exchange (AMPE))).

The OCI element appears prior to the MIC element in the Mesh Peering Open frame, and as part of the input AAD is authenticated by the MIC element (see 14.5 (Authenticated mesh peering exchange (AMPE)).

* Mesh Peering Confirm frame details

***p1495.18***

The MIC element appears prior to the Authenticated Mesh Peering Exchange element in the Mesh Peering ~~Open~~ Confirm frame. The information following the MIC element through to the end of the Mesh Peering Confirm frame body is encrypted and authenticated (see 14.5 (Authenticated mesh peering exchange (AMPE))).

The OCI element appears prior to the MIC element in the Mesh Peering Open frame, and as part of the input AAD is authenticated by the MIC element (see 14.5 (Authenticated mesh peering exchange (AMPE)).

* Mesh Peering Close frame details

***p1495.60***

The MIC element appears prior to the Authenticated Mesh Peering Exchange element in the Mesh Peering ~~Open~~ Close frame. The information following the MIC element through to the end of the Mesh Peering Close frame body is encrypted and authenticated (see 14.5 (Authenticated mesh peering exchange (AMPE))).

***Instruct the editor to modify the section 14.5.5 Mesh Peering Management framse for AMPE as follows***

* Processing Mesh Peering Open frames for AMPE

On receiving a Mesh Peering Open frame, the mesh STA shall verify the received frame. If AES-SIV returns the symbol “FAIL” the OPN\_RJCT event shall be invoked to the corresponding AMPE finite state machine and the reason code “MESH-INVALID-GTK” is generated. Otherwise, processing continues.

The received frame shall be rejected if the security capability selection fails (see 14.5.2 (Security capabilities selection)). The OPN\_RJCT event shall be invoked to the corresponding AMPE finite state machine.

***p2602.25***

If dot11RSNAOperatingChannelValidationActivated is true and the received RSNE indicates OCVC capability, the mesh STA shall validate the OCI element in the Mesh Peering Open frame by ensuring that all of the following are true

* OCI element is present
* Channel information in the OCI matches current operating channel parameters (see clause 12.2.x)

Otherwise, the mesh STA shall discard the frame.

The peer mesh STA’s MGTK extracted from the Mesh Peering Open frame shall be added to the Receive MGTK SA in which the peer’s MAC address equals the MGTK Source mesh STA MAC address.

If all operations succeed, the mesh STA shall proceed to process the Mesh Peering Open frame on basic parameters as specified in 14.3.6.2 (Mesh Peering Open frame processing).

* Processing Mesh Peering Confirm frames for AMPE

On receiving a Mesh Peering Confirm frame, the mesh STA shall verify the received frame. The received frame shall be discarded if AES-SIV returns the symbol “FAIL.”

If AES-SIV returns plaintext, the following operations shall be performed in order:

a) The Selected Pairwise Cipher Suite is checked. If the security capability selection has been done and the received value from Chosen Pairwise Cipher Suite field is not the same as the agreed pairwise cipher suite, the STA shall reject the received frame and the CNF\_RJCT event is invoked to the corresponding AMPE finite state machine with the failure reason code MESH-INVALID-SECURITY-CAPABILITY.

b) If dot11MeshSecurityActivated is true the group cipher suite is checked. If the received group cipher suite is not supported by the mesh STA, the mesh STA shall reject the received Mesh Peering Confirm frame and the CNF\_RJCT event is invoked to the corresponding AMPE finite state machine with the failure reason code MESH-INVALID-SECURITY-CAPABILITY.

**p2603.13**

c) If dot11RSNAOperatingChannelValidationActivated is true and the received RSNE indicates OCVC capability, the mesh STA shall validate the OCI element in the Mesh Peering Confirm frame by ensuring that all of the following are true

* OCI element is present
* Channel information in the OCI matches current operating channel parameters (see clause 12.2.x)

Otherwise, the mesh STA shall discard the frame.

If none of the cases is true, the mesh STA shall proceed to process the Mesh Peering Confirm Action frame on basic parameters as specified in 14.3.7.2 (Mesh Peering Confirm frame processing).

**Discussion – OCI validation for WNM Sleep Mode exchanges**

WNM Sleep Mode exchanges use WNM Sleep Mode Request/Response frames, containing a WNM Sleep Mode element. The OCI element can be added to WNM Sleep Mode Request/Response frames. It is only necessary to include OCI information for the sleep mode exit request/response, since no rekeying is performed at the time of entry to WNM sleep. Since GTK/IGTK rekeying is only used together with management frame protection, the OCI element is encrypted and integrity protected by PMF.

***Instruct the editor to modify the section 9.6.14 WNM Action details as follows***

* WNM Sleep Mode Request frame format

The WNM Sleep Mode Request frame is sent by a non-AP STA to the AP to enter the WNM sleep mode. The format of the WNM Sleep Mode Request frame is defined in Figure 9-847 (WNM Sleep Mode Request frame format).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  | one or more TFS Request elements |  |
|  | Category | WNM Action | Dialog Token | WNM Sleep Mode Element | TFS Request Elements | OCI element (optional) |
| Octets: | 1 | 1 | 1 | 6 | variable | 0 or 6 |
| * WNM Sleep Mode Request frame format | | | | | |  |

The Category field is defined in 9.4.1.11 (Action field).

The WNM Action field is defined in 9.6.14.1 (WNM Action fields).

The Dialog Token field is a nonzero value chosen by the non-AP STA sending the WNM Sleep Mode Request frame to identify the request/response transaction.

The WNM Sleep Mode Element field contains a WNM Sleep Mode element that is requested by a non-AP STA, as described in 9.4.2.82 (WNM Sleep Mode element).

The TFS Request Elements field contains one or more TFS Request elements to specify the traffic filters that are requested by a non-AP STA, as defined in 9.4.2.80 (TFS Request element).

The OCI Element field is optionally present, and contains an OCI element as defined in section 9.4.2.xxx OCI Element.

* WNM Sleep Mode Response frame format

The WNM Sleep Mode Response frame is sent by an AP in response to a WNM Sleep Mode Request frame or is sent without solicitation by an AP to a non-AP STA upon the AP’s deletion of all traffic filter sets established according to the traffic filtering agreement between the AP and the non-AP STA. The format of the WNM Sleep Mode Response Action field is defined in Figure 9-848 (WNM Sleep Mode Response Action field format).

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  | Category | | WNM Action |  | Dialog Token | Key Data Length | Key Data |
| Octets: | 1 | | 1 |  | 1 | 2 | variable |
|  |  | | one or more TFS Response elements |  |  |  |  |
|  | WNM Sleep Mode Element | | TFS Response Elements | OCI Element |  |  |  |
| Octets: | variable | | variable | 0 or 6 |  |  |  |
|  | | * WNM Sleep Mode Response Action field format | | | | | |

The Category field is defined in 9.4.1.11 (Action field).

The WNM Action field is defined in 9.6.14.1 (WNM Action fields).

When the WNM Sleep Mode Response frame is transmitted as a response to a WNM Sleep Mode Request frame, the Dialog Token field is the value in the corresponding WNM Sleep Mode Request frame. When the WNM Sleep Mode Response frame is transmitted as an unsolicited response, the Dialog Token field is set to 0.

The Key Data Length field is the length of the Key Data field. If the management frame protection is not used, this field is 0.

The Key Data field contains zero or more subelements that provide the current GTK and IGTK to the STA. The format of these subelements is shown(#243) in Figure 9-849 (WNM Sleep Mode GTK subelement format) and Figure 9-850 (WNM Sleep Mode IGTK subelement format). The subelement IDs for these subelements are defined in Table 9-405 (Optional subelement IDs for WNM Sleep Mode parameters). Each subelement starts with the ID and Length fields. The Length field in the subelement is the length of the contents of the subelement. When management frame protection is not used, the Key Data field is not present.

|  |  |
| --- | --- |
| * Optional subelement IDs for WNM Sleep Mode parameters | |
| Value | Contents of subelement |
| 0 | GTK |
| 1 | IGTK |
| 2–255 | Reserved |

The GTK subelement contains the Group Key as shown in Figure 9-849 (WNM Sleep Mode GTK subelement format).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Subelement ID | Length | Key Info | Key Length | RSC | Key |
| Octets: | 1 | 1 | 2 | 1 | 8 | 5 to 32 |
| * WNM Sleep Mode GTK subelement format | | | | | | |

The Subelement ID field is set to 0.

The Length field is defined in 9.4.3 (Subelements).

The Key Info field is defined in Figure 9-353 (GTK subelement’s Key Info subfield).

The Key Length field is the length of the Key field in octets.

The RSC field contains the receive sequence counter (RSC) for the GTK being installed. The RSC field gives the current message number for the GTK to allow a STA to identify replayed MPDUs. If the RSC field value is less than 8 octets in length, the remaining octets are set to 0. The least significant octet of the TSC or PN is in the first octet of the RSC field.

NOTE—The RSC field value for TKIP is the Transmit Sequence Counter (TSC) and is stored in the first 6 octets; for CCMP it is the Packet Number (PN) and is stored in the first 6 octets; see Table 12-6 (Key RSC field).

The Key field is the GTK being distributed.

The IGTK subelement contains the Integrity GTK as shown in Figure 9-850 (WNM Sleep Mode IGTK subelement format).

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Subelement ID | Length | Key ID | PN | Key |
| Octets: | 1 | 1 | 2 | 6 | 16 |
| * WNM Sleep Mode IGTK subelement format | | | | | |

The Subelement ID field is set to 1.

The Length field is defined in 9.4.3 (Subelements).

The Key ID field indicates the value of the BIP key identifier.

The PN field indicates the receive sequence counter for the IGTK being installed. The PN field gives the current message number for the IGTK, to allow a STA to identify replayed MPDUs.

The Key field is the IGTK being distributed.

NOTE 1—There might be multiple GTK and multiple IGTK subelements if a group rekeying is in process when the non-AP STA wakes up from WNM sleep mode.

NOTE 2—Management frame protection is used to provide confidentiality, replay, and integrity protection for GTK/IGTK update in WNM Sleep Mode Response frames.

The WNM Sleep Mode Element field contains a WNM Sleep Mode element, as described in 9.4.2.82 (WNM Sleep Mode element).

The TFS Response Elements field contains one or more TFS Response elements to specify the traffic filters, as defined in 9.4.2.81 (TFS Response element).

The OCI Element field is optionally present, and contains an OCI element as defined in section 9.4.2.xxx OCI Element.

***Instruct the editor to modify the section 11.2.3.18 WNM Sleep Mode as follows***

* WNM sleep mode
* WNM sleep mode capability

Implementation of the WNM sleep mode capability is optional for a WNM STA. A STA that implements WNM sleep mode has dot11WNMSleepModeImplemented equal to true. When dot11WNMSleepModeImplemented is true, dot11WirelessManagementImplemented shall be true. A STA where dot11WNMSleepModeActivated is true is defined as a STA that supports WNM sleep mode. A STA supporting WNM sleep mode shall set the WNM Sleep Mode field of the Extended Capabilities element to 1. When dot11WNMSleepModeActivated is true, dot11TFSActivated shall be true.

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.

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.

* WNM sleep mode non-AP STA operation *p2023.38*

To use the WNM sleep mode service, the non-AP STA’s SME shall issue an MLME-SLEEPMODE.request primitive to send a WNM Sleep Mode Request frame. The MLME-SLEEPMODE.request primitive shall include a valid SleepMode parameter with a WNM Sleep Mode element. The Action Type field in the WNM Sleep Mode element shall be set to “Enter WNM sleep mode” and the WNM Sleep Interval field shall be included. The WNM Sleep Interval field shall be less than the BSS max idle period (see 11.23.13 (BSS max idle period management)). The MLME-SLEEPMODE.request primitive shall also include a valid TFSRequest parameter as defined in the TFS Request element that the AP shall use as triggers to set the STA’s TIM bit.

When a traffic filter for group addressed frames is enabled at the AP, the STA may request a notification frame (see 11.23.12.2 (TFS non-AP STA operation)) be sent when requesting the establishment of the traffic filtering agreement.

On receiving a WNM Sleep Mode Response frame with Action Type field in the WNM Sleep Mode element set to “Exit WNM sleep mode”, if dot11RSNAOperatingChannelValidationActivated is true and the AP’s RSNE indicated OCVC capability, the STA shall validate the OCI information by ensuring that all the following are true:

* OCI element is present
* Channel information in the OCI matches current operating channel parameters (see clause 12.2.x)

Otherwise, the STA shall discard the frame.

The receipt of an MLME-SLEEPMODE.confirm primitive with a valid SleepMode parameter indicates to the STA’s SME that the AP has processed the corresponding WNM Sleep Mode Request frame. The content of the WNM sleep mode parameter in the WNM Sleep Mode Response frame provides the status of WNM Sleep Mode elements processed by the AP. The non-AP STA shall delete the GTKSA if the response indicates success. If RSN is used with management frame protection, the non-AP STA shall delete the IGTKSA if the response indicates success.

While in WNM sleep mode, the non-AP STA need not wake up every DTIM interval for group addressed frames.

The STA wakes up at intervals not longer than the value indicated by the WNM Sleep Interval field to check whether the corresponding TIM bit is set or group addressed traffic is pending. The non-AP STA does not participate in GTK/IGTK updates.

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 dot11RSNAOperatingChannelValidationActivated is true and the AP’s RSNE indicated OCVC capability, the WNM Sleep Mode Request frame shall include an OCI element.

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, and the frame is not discarded due to OCI validation, the STA exits WNM sleep mode.

* WNM sleep mode AP operation *p2024.17*

On receiving a WNM Sleep Mode Request frame with Action Type field in the WNM Sleep Mode element set to “Exit WNM sleep mode”, if dot11RSNAOperatingChannelValidationActivated is true and the non-AP STA’s RSNE indicated OCVC capability, the AP shall validate the OCI information by ensuring that all the following are true:

* OCI element is present
* Channel information in the OCI fields matches current operating channel parameters (see clause 12.2.x)

Otherwise, the AP shall discard the frame.

When an AP’s SME receives an MLME-SLEEPMODE.indication primitive with a valid SleepMode parameter and an Action Type in the WNM Sleep Mode element of “Enter WNM sleep mode”, it shall issue an MLME-SLEEPMODE.response primitive with SleepMode parameters indicating the status of the request.The value of the Action Type field of the WNM Sleep Mode element in the WNM Sleep Mode Response frame shall be set to “Enter WNM sleep mode”.

When an AP’s SME receives an MLME-SLEEPMODE.indication primitive with a valid SleepMode parameter and an Action Type in the WNM Sleep Mode element of “Exit WNM sleep mode”, if the frame is not discarded due to OCI validation, the AP shall disable WNM sleep mode service for the requesting STA, and the AP’s SME shall issue an MLME-SLEEPMODE.response primitive with a SleepMode parameter indicating the status of the associated request. When all traffic filter sets established for a STA are deleted upon frame matches, the AP shall also disable the WNM sleep mode service and transmit to the STA 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)) set to 1. When an AP sends a WNM Sleep Mode Response frame with Action Type field in the WNM Sleep Mode element set to “Exit WNM sleep mode”, if dot11RSNAOperatingChannelValidationActivated is true and the non-AP STA’s RSNE indicated OCVC capability, the WNM Sleep Mode Response frame shall include an OCI element.

**Discussion – PICS**

PICS should be added to indicate support for operating channel validation and the OCI element. OCI validation is an optional capability in an RSN.

***Instruct the editor to add the following to the MAC protocol capabilities section Annex B.4.4.1 p3310.52:***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Item | Protocol capability | References | Status | Support |
| PC XX <to be assigned> | Operating Channel Information Validation | 9.4.2.25(RSNE), 12.7.6 (4-way handshake), 12.7.7 (Group key handshake), 14.5 (Authenticated mesh peering exchange (AMPE)), 11.2.3.18 (WNM sleep mode), 9.6.10 (SA Query Procedure), 13.7.1 (FT reassociation), 13.8.4 (FT authentication sequence), 12.12.2.6.2( (Re)Association Request for FILS key confirmation) , 12.12.2.6.3 ((Re)Association Response for FILS key confirmation), 11.10.3.2 (Selecting and advertising a new channel in an infrastructure BSS), 12.7.2 (EAPOL-Key frames), 9.4.2.48 (Fast BSS Transition Element (FTE) | PC34:O | Y or N |
| PCXX.1 | OCI Element | 9.4.2.XXX OCI Element | PCXX:M | Y or N or N/A |
| PCXX.2 | OCI KDE | 12.7.2 (EAPOL-Key frames) | PCXX:M | Y or N or N/A |
| PCXX.3 | OCI FTE sublement | 9.4.2.48 (Fast BSS Transition Element (FTE) | PCXX:M | Y or N or N/A |

**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. <https://papers.mathyvanhoef.com/ccs2017.pdf>

[2] IEEE Std 802.11-2016

[3] Defense Against Multi-Channel Man-in-the-Middle (MITM) – IEEE SA Document – Nehru Bhandaru - <https://mentor.ieee.org/802.11/dcn/17/11-17-1606-03-000m-defense-against-multi-channel-mitm.pptx>

[4] Nonce Reuse Prevention – Dan Harkins – Nov 2017 - <https://mentor.ieee.org/802.11/dcn/17/11-17-1602-03-000m-nonce-reuse-prevention.docx>

[5] Mathy Vanhoef and Frank Piessens. 2014. Advanced Wi-Fi attacks using commodity hardware. In ACSAC.

[6] TGm IEEE Nov 2017 Agenda - <https://mentor.ieee.org/802.11/dcn/17/11-17-1556-07-000m-november-2017-tgmd-agenda.pptx>

[7] IEEE P802.11-REVmdTM/D0.3, September 2017