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. |  |  | [thomas.derham@broadcom.com](mailto:thomas.derham@broadcom.com) |
| Mathy Vanhoef | KU Leuven |  |  | [mathy.vanhoef@cs.kuleuven.be](mailto:mathy.vanhoef@cs.kuleuven.be) |

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 protect against 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 an Infrastructure 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.

**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, alleviating the impact of the next 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)

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

* 4-way handshake (also covers PeerKeySTK handshake)
* GTK handshake
* FT handshake
* FILS key confirmation

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.

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

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***

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

When OCVC capability is present, a STA shall advertise it in RSNE and shall include operating channel information and validate the operating channel received from an OCVC capable peer in protected messages used for key establishment and confirmation.

**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.

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 the operating channel and bandwidth over which the frame is received is discarded.

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

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

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

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***

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

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

****

with the following

B14

B15

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

1 1

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

--- 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 there are country specific and global operating classes, a country is needed to interpret the operating class, and country element is advertised in Beacons and probe responses. Thus validating OCI includes validating the country, operating class (that also defines bandwidth and primary channel upper/lower behavior), and channel number. Specifying country, operating class, primary channel and a secondary center channel index 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:
  + Country = US
  + Operating Class field = 128
  + Primary Channel Number = 153
  + Secondary Channel Index = 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 and 42 for the secondary segment

* 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:
  + Country = US
  + Operating Class field = 128
  + Primary Channel Number = 153
  + Secondary Channel Index = 42

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.

Another related question is whether to use global operating classes or country specific. Annex E of [1] states “”

So, using country specific classes would cover all the cases. If no country is specified, global operating classes may be implied.

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 – 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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 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***

9.4.2.xxx OCI Element

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

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Element ID | Length | Element ID Extension | Country  String | Operating  Class | Primary Channel Number | Secondary  Channel  Index |

Octets: 1 1 1 3 1 1 1

**Figure 9-XXX OCI element format**

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

Country String field is set to the value contained in the dot11CountryString attribute.

Operating Class field is set to the operating class currently being used corresponding to the widest bandwidth used for the BSS. See Annex E for description of operating classes. A noncountry entity in the country string field (‘XX ‘) implies the use of global operating classes Table E-4

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.

Secondary Channel Index field is set to the channel center frequency index of the secondary segment being used currently, if applicable, or set to 0 otherwise. Secondary Channel Index 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***

******

|  |  |  |
| --- | --- | --- |
| 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***

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

|  |  |  |  |
| --- | --- | --- | --- |
| Country String | Operating Class | Primary Channel Number | Secondary Channel Index |

Octets: 3 1 1 1

The definitions of Country String, Operating Class, Primary Channel Number, and Secondary Channel Index 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***

******

|  |  |
| --- | --- |
| 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***

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 | Country String | Operating Class | Primary Channel Number | Secondary Channel Index |

Octets: 1 1 3 1 1 1

The definitions of Country String, Operating Class, Primary Channel Number, and Secondary Channel Index 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 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***

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***

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***

— 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***

— OCI KDE when dot11RSNAOperatingChannelValidationActivated on the Authenticator

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

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 2473***

— 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 2472 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 subelment

In FILS re-association 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 12.7.6.3 4-way handshake message 2 p2463 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
* Channel information in the OCI does not match the operating channel parameters used to send message 1

Otherwise, the Authenticator:

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

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
* Channel information in the OCI does not match the operating channel parameters used to send message 2

The Supplicant also:

***Instruct the editor to modify subsection 12.7.6.5 4-way handshake message 4 p2467 starting with*** On reception of message 4… ***as follows***

On reception of message 4, the Authenticator verifies that the Key Replay Counter field value is one that it

used on this 4-way handshake; if it is not, it silently discards the message.

If dot11RSNAOperatingChannelValidationActivated is true and Supplicant RSNE indicates OCVC capability, the Authenticator silently discards message 4 if any of the following are true

* Current operating channel information does not match the operating channel parameters used to send message 3

Otherwise:

***Instruct the editor to modify subsection 12.7.7.2 Group key handshake message 1 p2472 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

***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 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
* Channel information in the OCI KDE does not match the operating channel parameters used to send message 1

***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 requiest 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).

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
* Channel information in the OCI matches the operating channel parameters used to execute the FT authentication sequence

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
* Channel information in the OCI matches the operating channel parameters used to execute the FT authentication sequence

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.

— 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…

…

— 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 association request Table 9-35—Reassociation Request frame body (continued) – on page 817 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 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)).

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

…

(#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
* Channel information in the OCI matches the operating channel parameters used for the authentication request

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.

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
* Channel information in the OCI matches the operating channel parameters used for the association request

Otherwise, the STA shall discard the frame.

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 channel switch**

A STA should initiate SA Query procedure with OCI after an unprotected channel switch to confirm the operating channel.

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

Should there be a timeout for SA query response? If valid response is not received after certain time, it should switch back to the original channel.

If an SA query was in progress to verify a channel switch if one was in progress, that previous should be abandoned.

***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.

If the STA chooses to perform the specified switch and dot11RSNAOperatingChannelValidationActivated is true and the AP has indicated OCVC capability, it shall initiate the SA query procedure if the switch was not based on a protected indication i.e. if the switch was not based on a protected management frame that contained the new operating channel information, The STA may pause the transmit and receive of Data frames until the SA query procedure has completed successfully for additional protection.

If a STA initiates SA query procedure to validate an unprotected 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***

…

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

A STA that responds with an SA Query Response frame 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; Otherwise, the receiving STA shall deem the response as invalid and discard it.

If a non-AP or non-PCP STA 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 switch back to the channel prior to the switch based on the unprotected channel switch indication.

…

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



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

Octets: 1 1 2 0 or N

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



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

Octets: 1 1 2 0 or N

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

…

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 where N is the size of the OCI element.

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

…

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 where N is the size of the OCI element

**Discussion – OCI validation for Mesh**

Needs additional work and a separate submission.

**Discussion - PICS**

TBD if PICS needs an update OCVC capability. OCVC would be an optional feature for various features that support OCVC

**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