IEEE P802.11
Wireless LANs

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |
| --- |
| SB CR for CID 8037 |
| Date: 2024-07-15 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Po-Kai Huang | Intel  |  |  | po-kai.huang@intel.com |
| Ido Ouzieli |  |  |  |  |
| Emily Qi |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

 |

Abstract

This submission proposes resolutions for the following comments from comment collection on P802.11-REVme D6.0:

8037

**Revision History:**

R0: Initial version.

# CID 8037

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page.Line** | **Comment** | **Proposed Change** |
| 8037 | 11.52 | 2986.43 | The added SSID verification KDE during 4-way to resolve the problem of unverified SSID during (re)association request/response exchange requires support on both AP and non-AP side to make it work. Similar to the proposed alternative solution using Beacon protection for OCVC, would like to propose to also use Beacon protection to resolve the problems without the need to have additional AP support. [Po-Kai] | Add "If SSID protection is not supported by a non-AP STA or if the current AP does not advertise support of SSID protection, but beacon protection is enabled, the non-AP STA should verify that the received Beacon frames that have been validated using BIP are consistent with the SSID that was indicated in the (Re)Association Request frame for the current association and if the non-AP STA does not receive consistent information about the SSID in protected Beacon frames, the non-AP STA should disassociate from the AP. NOTE-A matching SSID might be indicated in the SSID element or in a Nontransmitted BSSID Profile subelement in a Multiple BSSID element." after "If OCVC(#3505) is not present in a non-AP STA or if the current AP does not advertise OCVC(#3505), but beacon protection is enabled, the non-AP STA shall verify that the operating channel information in the first received Beacon frame that has been validated using BIP matches the current operating channel parameters. If there is a mismatch, the non-AP STA shall disassociate from the AP." |

## Discussion:

A proposal to protect SSID in 4-way handshake due to unprotected SSID in (Re)Association Request frame is accepted by revme D6.0 in 11-24/938r3.

The proposal requires both non-AP STA and AP to upgrade to support the additional verification in 4-way handshake.

Given that Beacon protection is going to be mandated in 11be, this document proposes to simply utilize Beacon protection to verify SSID in the protected Beacon after 4-way handshake without the need for additional upgrade from the AP to prevent the attack.

This proposal prevents the MITM attack proposed in the paper (see below) because the attacker does not have the BIGTK of the trustnet and wrongNet and can not reproduce the Beacon with the correct MIC for the client to verify. Further, client will only get the BIGTK of the wrongNet due to MITM, and will verify the Beacon from WrongNet with SSID rewrite with failure. In such case, the client can disassociate.



## Proposed Resolution: CID 8037

**REVISED**

**Instruction to TGme Editor:**

Implement the proposed text updates for corresponding CID in 11-24/1168r0

**TGme Editor: *Instruction: Modify 11.52 as shown below***

**11.52 Beacon frame protection procedures**

(…existing texts…)

If OCVC(#3505) is not present in a non-AP STA or if the current AP does not advertise OCVC(#3505), but beacon protection is enabled, the non-AP STA shall verify that the operating channel information in the first received Beacon frame that has been validated using BIP matches the current operating channel parameters. If there is a mismatch, the non-AP STA shall disassociate from the AP.

If SSID protection is not supported by a non-AP STA or if the current AP does not advertise support for SSID protection, but beacon protection is enabled, the non-AP STA should verify that the received Beacon frames that have been validated using BIP are consistent with the SSID that was indicated in the (Re)Association Request frame for the current association and if the non-AP STA does not receive consistent information about the SSID in protected Beacon frames, the non-AP STA should disassociate from the AP.

NOTE-A matching SSID might be indicated in the SSID element or in a Nontransmitted BSSID Profile subelement in a Multiple BSSID element.