IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TGbh CIDs related to STA generate ID pre-association and PASN | | | | |
| Date: 2023 - March | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Graham SMITH | SR Technology | Sunrise, FL, USA. | 916 799 9563 | gsmith@srtrl.com |
| Kurt Lumbatis | ARRIS/CommScope | Suwanee, GA, USA |  | Kurt.lumbatis@commscope.com |

Abstract

Satisfying CIDs related to STA generated ID pre-association and PASN with proposed text for IRM scheme 23/0129r1.

IRM text 23/0129r1 was prepared with input from Jay Yang and Okan Mutgan (Nokia)

CIDs for STA ID and Pre-Association

|  |  |  |  |
| --- | --- | --- | --- |
| **CID** | **Commenter** | **Comment** | **Proposed Change** |
| 7 | Jay Yang | Device ID only can be used in post association, we need to a solution to cover the probing case. | the commenter will provide a solution. |
| 9 | Jay Yang | an AP may not grant an identifier to some STAs once it's recognized via the MAC address. RMA causes such implement broken, need to provide a solution to address it. | the commenter will provide a solution on it. |
| 36 | Julien Sevin | No privacy enhancement mechanism is specified for covering the pre-association use cases specified by the 11bh group in the document 332r37. | Specify a privacy enhancement mechanism for identifying a STA operating with a Random MAC Address before the association |
| 40 | stephane baron | Issue tracking document contains scenario (especially 4.2 : returning device) agreed by the group and that is not addressed by the current draft. | Provide a mechanism that supports scenario 4.2 by providing a MAC address based mechanism that allows a returning station to be recognized. |
| 41 | Patrice Nezou | The document 332r37 describes some scenarios related to the pre-association procedure. The current draft does not propose any privacy enhancement during this procedure. | Need additional mechanisms to enhance the privacy during the pre-association procedure. |
| 42 | Mikael Lorgeoux | A mechanism for privacy enhancement is missing for the coverage of pre-association use cases specified in the doc 332r37. | Specify a privacy enhancement mechanism for covering pre-association use cases of doc 332r37. |
| 61 | Mark Hamilton | With majority support for a STA-generated device ID (for example, Motion #3, although not 75% on a particular proposal, yet) and evidence that both network-generated and STA-generated can coexist (cf 11-22/0908), add a STA generated ID variant. | Add a STA-generated Device ID variant, and appropriate mechanism (if needed) to select an operating mode. |
| 64 | Jarkko Kneckt | The 802.11bh should define a protocol that allows STA to provide STA ID that the STA uses to identify itself to the AP in the following authentications/associations. | Please allow STA to have a possibility to provide to AP the STA Identifier that is used to identify the STA. |

DISCUSSION

The Identifiable Random MAC (IRM) scheme is proposed in order to satisfy these CIDs. Basically IRM is a scheme where each time a non-AP STA associates to an AP, it sends a new (random) MAC address to the AP in msg 4 of the 4w HS. The STA and the AP remember this address, and the next time the STA wants to associaite to that AP (and be identified), it uses that address. Then it associates and provides another address.

IRM text for incorporation into the TGbh Draft is proposed in 23/0129r1.

PROPOSAL

CIDS 7, 9, 36, 40, 41, 42, 61, 64

Revised

Incorporate the text in 23/0129r2.

CIDS for PASN

|  |  |  |  |
| --- | --- | --- | --- |
| **CID** | **Commenter** | **Comment** | **Proposed Change** |
| 19 | Jonathan Segev | It is not clear how the Device ID mechanism supports unassociated PASN operation. the PASN operation is required to support management procedure that do not require data transfer, examples are FTM and 11ba. | Add support for Device ID in PASN. |
| 20 | Jonathan Segev | The mechanism for device ID should be such that to a single network a device  with an on going unassociated session should be identifiable as single device  to the network (ESS).  an example of such operation is the need to two way report for FTM;  The client STA reports measurement conducted to each individual AP while the  multiple outstanding FTM sessions are in progress, the NW is able to associate the measurement from  multiple sessions to be attributed to a single client and thus can identify client location.  This client may not be associated to the network. | Add a functionality that allows a device to be identified to the ESS as a single entity. |

DISCUSSION

22/1806r0 discussed exchanging the Device ID in PASN Authentication frames.

When using IRM, STA sends IRM element in Auth Msg 3. It is ebcrypted and can be decrypted by AP.

Generally, there are two different PASN scenarios:

1. **STA coming back to the same ESS uses same MAC address:**
   1. STA comes to ESS for the first time [STA uses MAC1],
   2. does PASN (sending its future IRM, e.g., IRM1)
   3. does multiple FTM sessions with different APs in the ESS [all sessions use MAC1].
   4. STA deauthenticates.

THEN

* 1. STA comes to ESS for the second time [STA uses IRM1], does PASN (sending its future IRM, e.g., IRM2) and does multiple FTM sessions with different APs [all sessions use IRM1].

Example:

Picture 1

Diagram

Description automatically generated

Observer will see same STA during each full PASN session, but does not know it ithe same one when it returns

1. **STA establishing multiple FTM sessions in ESS (without coming back)**
   1. STA comes to ESS for the first time [STA uses MAC1],
   2. does PASN (sending its future IRM, e.g., IRM1)
   3. does multiple FTM sessions with different APs in the ESS [all sessions use different IRM].

Example:

Picture 2

Diagram

Description automatically generated

ESS knows it is one STA.  Third party observer does not know it is one STA, so private.

1. STA uses IRM for each FTM session and for each return to the same ESS

ESS knows it is one STA and third party does not know.

Picture 3

Diagram

Description automatically generated

Maybe for simplicity, 1) is enough but STA is trackable by the MAC address when doing multiple sessions because of the same MAC usage.

Hence, better privacy is to use 3).

**We just need the hook(s) in the text to allow any of these.**

**Then the action is entirely up to the STA.**

**AP role in PASN with IRM**

As the IRM element is sent in Auth Msg 3, the AP does not (can not) send an IRM element at all, i.e., no status “recognized”.

PROPOSAL

CIDS 19, 20

Revised

Incorporate the text in 23/0129r2.