Minutes IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IEEE 802.11 TGbh Meeting Minutes, November 4, 2021  Randomized and Changing MAC addresses (RCM) | | | | |
| Date: 2021-11-04 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Graham SMITH | SR Technologies | Sunrise, Florida |  | gsmith@srtrl.com |
|  |  |  |  |  |

Abstract

This document contains the minutes of the IEEE 802.11bh telecom Interim meeting November 4, 2021.

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer

C- proceeds a comment

**Meeting Nov 4, 2021 7.00 to 9.00 pm ET**

**Chair: Mark Hamilton (Ruckus/CommScope)**

**Vice Chair: Peter Yee (NSA-CSD/AKAYLA)**

**Vice Chair: Stephen Orr (Cisco)**

**Secretary: Graham Smith (SRT Wireless)**

**Editor: Carol Ansley (Cox)**

**The teleconference was called to order by Chair 7.03 hrs. EDT,**

Agenda slide deck 11-21/1767r0

1. **Policies and procedures were presented by the chair. (Slides 4 to 14)**

There were no Patent declarations.

Copyright policy slides were presented (Slides 10 and 11)

1. **Agenda:**

* Attendance, noises/recording, meeting protocol reminders
* Policies, duty to inform, participation rules
* Organization topics (see Backup slides)
* Response to WBA liaison (contribution needed)
* Issues Tracking updates/status: 11-21/0332r20
* Evaluation of proposed solutions (next slide)
* Next meetings: Nov Plenary (Wed, Thur, Fri)

Nothing submitted on the WBA Liaison response

No objections, Agenda accepted.

Any comments on the latest Issue Document revision? - None

1. **Proposals received:**

* 11-21/1083r0: A Signature-based Method for Identifying STAs with Randomized MAC Addresses (reviewed July 15)
* 11-21/1585r8: Identifiable Random MAC address (reviewed Oct 21, updated);
* 11-21/1673r6: Proposed Text for IRMA (briefly reviewed Oct 21, updated)
* 11-21/1720r1: IRM advantages and use cases (not reviewed yet)
* 11-21/1378r0: Client ID query concept (reviewed Aug 19);
* 11-21/1379r3: Proposed text for ID Query Action frame (reviewed Oct 21)

Comparison of solutions: 11-21/1730r0

Chair commented that all submissions are client–based with opt-in.

Several updates

**11-21/1720r1: IRM advantages and use cases,** presented by Graham Smith

C – Rogue client flood IRMKs. DoS attack

A – Unique concern. Key table management outside scope, how implemented can change. STA does need to go thru a full association so no different at all to an attack that simply keeps sending Association Requests

C – Local admin bit, should it be the four bits used in SLAP? Should say 44 bits?

A – Needs to be sorted out as presently I think at the moment it just says “out of the local admin space”

C – AP needs to do a lot of computation. Check field reveals bits,

A – Check field does not reveal bits. Field is optional, but does allow AP to down select. Need to associate before keys are exchanged. Key can be changed at any time.

C – Too complicated, too much effort.

A – Do not agree. You can’t get something for nothing and the benefits of true random address, every time, ability to declare in advance if known or not, and is secure.

(Commenter appeared to be describing a method and it was requested that, if so, a submission be made.)

C – Grocery #8 not out of scope. #18 MAC address so no difference.

A – Yes noted.

C – Key only exchanged when associated? Yes

C – Allows a returning STA to be recognized? Yes even though MAC address and hash is different

C – Can a 3rd party spoof by choosing same random MAC address and hash. Then key can be found.

A –Random Address can be spoofed anyway. Still needs to associate. IRMK has nothing to do with association. So no, spoof does not achieve anything.

C – Hotspot could do this as a replay attack. Using other methods to get pairwise keys.

A – Don’t think so as still need credentials.

C – After 4-way then already have encryption.

A - If STA always changed IRMK on association then all attempts to copy or spoof are countered.

Chair presented Issues Tracking updates/status: 11-21/0332r20

New additions on approach to assess the solutions.

Clause 6.4 Solutions analysis tables either Use Case paras, or how feature maps onto in-scope Use Case attributes?

i.e. Each Use case or each feature?

C – Like the idea of table to compare

Discussion on whether to use separate use cases, or based on the feature.

C - How do you use tables? Share ideas? Further contributions?

C – First table seems to follow use cases we discussed. Second Table seems to follow Dan’s document 1631 requirements. Is that true?

A – Dan did not intend that the statements were to be used to compare. Not sure if these are requirements. More “evaluation criteria” to be used, to assess the trade-offs.

Q – Questions on how to use these tables? How good is solution to solving these criteria? Could we add computing /memory/security?

C – Another concern is ‘can we trust the AP?’ Won’t solve problem with open networks.

Chair showed 1730r0

Computation/storage complexity. User complexity. Security (tracking)

C – Once associated MAC address is fixed. Are we considering changing?

A – Cannot change MAC address while associated. If STA changes on periodic basis, at fundamental level must make a new association. Come back with new address but need to be identified.

C – Does it depend on security of network? What about open network? Captive portal? How strong is ID bound to a user? IS AP trusted? How do I differentiate when everyone knows the password?

A – Interesting but go to the user opt-in choice.

C – Need to careful with different levels of security. If on open network, then no expectation of privacy. Also on shared key. IF you have an ID to share, does not have to be an ID that is meaningful, other than what is meaningful to that network. Does not make sense to tackle open network.

C – Gets into TGbi make sure we do not make more problems.

C – We can not cause any new privacy concerns to be added.

C - Captive portals can be directed for secure log in. Problem is they remember MAC address. Means to authenticate AP.

C – Think that is how much network can trust the AP.

C – Outside scope of 11 on how to use open mode.

1. **Next meeting Nov Plenary**

**Out of time**

**Meeting adjoined at 9.01pm ET.**

|  |  |  |  |
| --- | --- | --- | --- |
| Breakout |  | Name | Affiliation |
| TGbh | 11/4 | Bhandaru, Nehru | Broadcom Corporation |
| TGbh | 11/4 | Carney, William | Sony Group Corporation |
| TGbh | 11/4 | Hamilton, Mark | Ruckus/CommScope |
| TGbh | 11/4 | Huang, Po-Kai | Intel Corporation |
| TGbh | 11/4 | Kneckt, Jarkko | Apple, Inc. |
| TGbh | 11/4 | Levy, Joseph | InterDigital, Inc. |
| TGbh | 11/4 | Lu, Liuming | Guangdong OPPO Mobile Telecommunications Corp.,Ltd |
| TGbh | 11/4 | Lumbatis, Kurt | CommScope, Inc. |
| TGbh | 11/4 | Luo, Chaoming | Beijing OPPO telecommunications corp., ltd. |
| TGbh | 11/4 | Orr, Stephen | Cisco Systems, Inc. |
| TGbh | 11/4 | Petrick, Albert | InterDigital |
| TGbh | 11/4 | Rosdahl, Jon | Qualcomm Technologies, Inc. |
| TGbh | 11/4 | Sevin, Julien | Canon Research Centre France |
| TGbh | 11/4 | Smith, Graham | SRT Wireless |
| TGbh | 11/4 | Wang, Lei | Futurewei Technologies |
| TGbh | 11/4 | Yee, Peter | NSA-CSD |