Minutes IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IEEE 802.11 TGbh Meeting Minutes, January 6, 2022  Randomized and Changing MAC addresses (RCM) | | | | |
| Date: 2022-06-01 | | | | |
| 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 January 6, 2022.

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer

C- proceeds a comment

**Meeting Jan 6, 2022 19.00 to 21.00 am 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 11-22/0010r0

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)
* Issues Tracking updates/status: 11-21/0332r28
  + “Post-association” implies both association \_and\_ security complete
    - Is this really RSNA established (as suggested on previous call)? Is RSNA required/assumed?
* Contributions:
  + 11-21/1634r0 – Private Identifier Requirements (Kurt Lumbatis)  
    Kurt stated that he was not ready to present, so this item removed from agenda.
  + 11-21/2039r0 – Random Index Assignment (Liuming Lu)
* Evaluation of proposed solutions
  + 11-21/2006r1 - Graham Smith
  + 11-22/0025r0 – Nehru Bhandara
* Next meetings: Jan 11, Jan interim session

1. **Non-AP STA Identification**
   * 11-21/1083r0: A Signature-based Method for Identifying STAs with Randomized MAC Addresses (reviewed July 15)
   * 11-21/1585r11: Identifiable Random MAC address (reviewed Nov 10, updated);
     + 11-21/1673r9: Proposed Text for IRMA (briefly reviewed Oct 21, updated)
     + 11-21/1720r1: IRM advantages and use cases (reviewed Nov 4)
     + 11-21/2006r1: IRM analysis, use cases, criteria (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)
     + 11-21/1853r0: ID Query analysis (not reviewed yet)

* 11-21/1839r0: Transient STA ID
  + - 11-22/0025r0: TSID Proposal Analysis
* 11-21/2039r0: Random Index Assignment (not reviewed yet)

Any comments? Any objections to agenda? - None

Agenda accepted.

Timeline targeted D0.1 for Nov 2021 was missed. Need to be discussed, maybe in January.

1. **Issues Tracking Document 21/0332r28**

Chair showed the editorial updates to the document. Still has many comments which need to cleaned up. Clarified “post association” meant also that security has been established.

One question, noted at last meeting that RSNA has been established is what was meant by post association. Noted that RSNA is not always in use.

C – Are you thinking also pre-RSN? TKIP?

A – Yes. Whatever security you are using is what I think is required.

C – TKIP is deprecated. What other option is there?

A – Did not really see a reason to restrict ourselves, e.g., open security. Is there anything else.

C – Just say association and security requirements complete?

A – Used security context.

1. **“Random Index Assisted Scheme”** presented by Liuming Lu

Document 21/2039r0

C – Random index list is encrypted before sending to STA. How? In What frames is this list transmitted? After association or as part of the RSNA mechanism?

A - A new format frame to be specified? This is just an outline. APs and STA can negotiate a public key, this is used to encrypt the list.

C – Need some sort of negotiation to allocate public keys. Why is this encryption needed if RSNA or is this for open network?

A – This is a general idea.

C – Random index carried in Association Request, so how can AP trust it? Request is not protected. What if another STA guesses the index?

A – AP receives and decodes.

C – What does AP do if same random index is sent (as per slide 6).

C – Believe this is on top of the MAC address Signature idea previously presented? Is this index carried on every data frame? Is the idea that the STA is changing its address on every frame?

A – MAC address is not frequently changing.

C – Please be clear for how many times address changes? Also does index get shared with another AP?

A – AP can assign different index for each STA.

C – Random index list is encrypted, but every frame carries random index which is not encrypted.

A – Correct

C – This is extension of previous contribution. Method could be used for IRMA. First time association informs public key.

C – Why index list? If STAs use the same index?

A – Privacy protection, STAs. Only one index, easy to be checked.

C – Applicable to any key based method? Nice if clarified rule for the range. What happens if each time same index? Then privacy is limited. Clever scheme but not clear of the range and size of labels – if AP gives range of say 4 or 16? What is effect of this range?

A – Need more research on this issue.

C – Random index sent on re-association in the clear? How does AP get from random key. Public key is fixed. Think it becomes trackable by observer.

A – Need to discuss further.

C – Same question as previous - how many STAs can be handled by this method, can be a big number? Confused with use of RMA, TA and address key. When is the exchange pre or post association? If sent in the clear with a public key which is known, how is it protected?

A – Need more research on the issue.

C – How does AP come up with these indices?

Suggested that more discussion required on the Reflector. Chair noted that next call is only 2 working days away.

1. **“IRM Analysis Use Cases and Criteria”**: Presented by Graham Smith

Document 21/2006r1

C – What are the memory requirements over time. What if STA changes key?

A – Same list but now 128 bits per STA. in place of 48 bits (MAC Address). STA can change key but simply replaces old key.

C – What prevents rogue STA from copying IRMA and Hash

A – Covered in the contribution, but rogue must have password to be of any use and also difficult to see what benefits can be had even if did have the key. IRMK does not identify the user and can change.

C - One STA associates with IRMA, another STA associates with same IRMA?

A – Also need the IRMK. If not then still needs to have password and AP can challenge.

C – STA must store keys and APs, AP must store keys and STA

**Out of time**

**Meeting adjoined at 20.56 am ET.**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Attendance   |  |  |  |  | | --- | --- | --- | --- | | Breakout | Timestamp | Name | Affiliation | | TGbh | 1/6 | Andersdotter, Amelia | Sky UK group | | TGbh | 1/6 | Bhandaru, Nehru | Broadcom Corporation | | TGbh | 1/6 | Coffey, John | Realtek Semiconductor Corp. | | TGbh | 1/6 | Dogukan, Ali | Koc University; Vestel | | TGbh | 1/6 | Fernandez, Olivia | SR Technologies | | TGbh | 1/6 | Hamilton, Mark | Ruckus/CommScope | | TGbh | 1/6 | Hsu, Ostrovsky | Xiaomi Inc. | | TGbh | 1/6 | Huang, Po-Kai | Intel Corporation | | TGbh | 1/6 | Levy, Joseph | InterDigital, Inc. | | TGbh | 1/6 | Lu, Liuming | Guangdong OPPO Mobile Telecommunications Corp.,Ltd | | TGbh | 1/6 | Lumbatis, Kurt | CommScope, Inc. | | TGbh | 1/6 | Luo, Chaoming | Beijing OPPO telecommunications corp., ltd. | | TGbh | 1/6 | Montemurro, Michael | Huawei Technologies Co., Ltd | | TGbh | 1/6 | Orr, Stephen | Cisco Systems, Inc. | | TGbh | 1/6 | Petrick, Albert | InterDigital | | TGbh | 1/6 | Sevin, Julien | Canon Research Centre France | | TGbh | 1/6 | Shalom, Hai | Google | | TGbh | 1/6 | Smith, Graham | SRT Wireless | | TGbh | 1/6 | Torab Jahromi, Payam | Facebook | | TGbh | 1/6 | Wang, Lei | Futurewei Technologies | | TGbh | 1/6 | Yang, Jay | Nokia | | TGbh | 1/6 | Yee, Peter | NSA-CSD | |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |