Minutes IEEE P802.11
Wireless LANs

|  |
| --- |
| IEEE 802.11 TGbh Meeting Minutes, December 7, 2021Randomized and Changing MAC addresses (RCM) |
| Date: 2021-12-07 |
| 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 December 7, 2021.

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer

C- proceeds a comment

**Meeting Dec 7, 2021 9.00 to 11.00 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 9.03 hrs. EDT,**

Agenda slide deck 11-21/1953r0

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: [11-21/0332r25](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-25-00bh-issues-tracking.docx)
	+ Suggest changing “post-association” to indicate after security complete
	+ Section 5 review led to “requirements” – or are these section 6 analysis criteria?
* Evaluation of proposed solutions (next slide)
	+ Complete section 5 review; consider section 6 solutions analysis
	+ Contribution: [11-21/1634r0](https://mentor.ieee.org/802.11/dcn/21/11-21-1634-00-00bh-private-identifier-requirements-for-tgbh.docx) – Private Identifier Requirements
* Next meetings: Dec 16, Jan 6, Jan 11

One contribution not presented yet “Private Identifier Requirements”. Noted that author is not present.

1. **Non-AP STA Identification**

Proposals received:

* [11-21/1083r0](https://mentor.ieee.org/802.11/dcn/21/11-21-1083-00-00bh-a-signature-based-method-for-identifying-stas-with-randomized-mac-addresses.pptx): A Signature-based Method for Identifying STAs with Randomized MAC Addresses (reviewed July 15)
* [11-21/1585r11](https://mentor.ieee.org/802.11/dcn/21/11-21-1585-11-00bh-identifiable-random-mac-address.pptx): Identifiable Random MAC address (reviewed Nov 10, updated);
	+ [11-21/1673r8](https://mentor.ieee.org/802.11/dcn/21/11-21-1673-08-00bh-proposed-text-for-irma.docx): Proposed Text for IRMA (briefly reviewed Oct 21, updated)
	+ [11-21/1720r1](https://mentor.ieee.org/802.11/dcn/21/11-21-1720-01-00bh-irm-advantages-and-use-cases.docx): IRM advantages and use cases (reviewed Nov 4)
* [11-21/1378r0](https://mentor.ieee.org/802.11/dcn/21/11-21-1378-00-00bh-client-id-query-concept.pptx): Client ID query concept (reviewed Aug 19);
	+ [11-21/1379r3](https://mentor.ieee.org/802.11/dcn/21/11-21-1379-03-00bh-proposed-text-for-id-query-action-frame.docx): Proposed text for ID Query Action frame (reviewed Oct 21)
	+ [11-21/1853r0](https://mentor.ieee.org/802.11/dcn/21/11-21-1853-00-00bh-id-query-analysis.docx): ID Query analysis (not reviewed yet)
* [11-21/1839r0](https://mentor.ieee.org/802.11/dcn/21/11-21-1839-00-00bh-transient-sta-id.pptx): Transient STA ID

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 0332r25**

Objective - Look at section 5 and consider section 6. Check that criteria discussed in Section 5, is captured in Table 2 (section 6)

Front page shows the updates for each revision.

Section 5.

Use Case 4.2

Chair – We evaluated points that seem to be guidance as to how solutions could be evaluated. This is more of evaluation criteria for a solution rather than a Use Case in itself. Suggestion is that we agree that this is in scope but we come up with criteria that we want to consider to evaluate solutions as they are proposed.

C – Yes agree. Some use cases that are not in scope but are solved by a solution is still OK. Maybe coming down to Use Case 4.2 must be solved and Use Case 4.17 (Intercept) is not solved (i.e., made more difficult) then we are 99% of the way there.

C – Agree that Use Cases tend to overlap. Are we ready to jump to list on Table 2?

No objection

Chair split screen for the document looking at Use Cases (4.2) and Table 2.

Started at “Third parties cannot track” in Table 2. Chair edited document on screen.

C - We are trying to enable a second (wanted) party to track a device. Maybe say “a party not intended to have the information” rather than “third party”.

Chair – Looking at “Confidentiality, integrity, authentication of identifier” for 4.2.

C – Problem with “authentication”. Most use open Authentication,

C – We are not talking about Authentication, this is concerned with authentication of the STA.

C – Do we need to look at the Association of the device, or the User association to the device?

C – This is looking like protection against spoofing. Spoof AP and spoof STA.

C – Please add row numbers so that we can refer better to the criteria.

This was done. Row 22 changed for spoofing.

C – Nothing here for the client to trust the network. May not be in our scope but certainly relevant.

A - Yes, it is in 4.2. status column “Client authenticates AP”

Chair – “Active attack”. (active and PSK attacks). Is that covered by row 2? Yes.

C – Captive portal case?

C – A certificate could be held by a device

C - You have jumped to a solution, but the cookies idea also does that.

C – Does considering this use case as a captive portal add to this.

C – Not always an open network.

C – It came out in discussions on the IRMA solution that we need to consider when a rogue STA can get on the network. Client knows if network is “open” or “low security” so can use an ID accordingly

Chair – Added row for open or known PSK.

C – If not a secure network, is ID protection higher than data? Hesitate to have higher identity protection than data.

C – Using the same address for a network would suffer from this attack, so maybe if a solution did help then, good, but maybe not the end of the world.

C – If network is weak anyway, why design for it? Client has a choice.

C – Most networks use AAA server to authenticate the user. Really outside of correlating a RMA with a user if the network security is weak.

C – Need to look how the network uses the identifier. If network knows the identity before Association, then a different problem. No handshake has taken place. Looking to ID the user at that point even though using a different MAC address. Secure ID for billing and such, and ID for simpler uses. Maybe two classes of ID.

C – Maybe 3 IDs, level of trust.

C - Pre-association we have kept as a separate case. Most discussions have been based on Associated, and “secure”. Need to check we have captured this. Row 7 gets close, but classed as “nice-to-have”.

C- Each level of security changes what STA expects.

C – If you join an open network, then no expectation of security. ID is same protection as data.

C – Pre-association ID is a different beast. We do have Use Case 4.1.

C – Need to be careful. What states are we considering? Big difference between State 1 and 2/3. FILS for example in state 1 has not selected a network, but state 2 selects the network.

C – Trying to fix MAC ID but is that not at state 4?

C – Need to be careful in general as to how we address pre and post association.

C – 4.1 is pre-association client steering. This is different to the state discussion. Are we trying to steer prior to state 1?

C – “User control over identifier”, what if network deletes identity? Control over lifetime may be added as a criteria?

C – User identifier or device ID? Before RCM, MAC address did both.

C – Use case of hotel, all devices get associated with room. Maybe a 3rd choice

C – I think at layer 2 it is the device, then user ID is at higher layer.

C – Starts to creep into TGbi.

C – If sticking to RCM then probably need to stick to device identification.

C – Higher layer relates the identifiers to one account, say.

C – Think it is higher layer for user. Even if ID is say “Smith 1”, and then “Smith 2” is it not a higher layer thing to note they are same account?

C – If this is a requirement then hesitate that it is possible. OK for discussion. Don’t think can have a solution, for example same IPad could be used by different persons in family. Do not see reason to define spec.

C – Before RCM the MAC was ID for the device. No recognition of groups of devices.

Chair looked at other Use Cases to see if the Criteria list is complete in Table 2.

Chair – Is it OK to delete the discussion text in Table in section 5 for Use Case 4.2, added at last meeting, as covered now in Table 2?

No objection.

Chair deleted selected text in the section 5 table, on screen. Each use case looked at in Section 5.

C – “Out of scope” maybe two sides to this? Definitely don’t want to make possible, or simply not bothered as not our problem.

Chair – Yes, add “can’t track” or such. Covered OK in Table 2.

Chair – 4.7. not our problem to solve. This is the second “Out of scope” type.

C – 4.12. What about network spoofing, is this new? Did not worry about this before.

C – If STA can “test” the AP before providing information, then that may be an advantage.

C – Anything linked to money is important. Identifier must not be used by someone else.

C – What about “virtual APs”?

Discussion “virtual APs”. BSSID for every association.

C – Virtual BSSID. BSSID follows the user or device, remains the same as it transitions from AP to AP. As long as association not broken, RCM is not a problem. If association breaks and re-makes then it has a new MAC and new BSSID. If MAC changes during association, then there is a problem.

**Out of time**

**Meeting adjoined at 11.00am ET.**

|  |  |  |  |
| --- | --- | --- | --- |
| Breakout | Timestamp | Name | Affiliation |
| TGbh | 12/7 | Ansley, Carol | Cox Communications Inc. |
| TGbh | 12/7 | baron, stephane | Canon Research Centre France |
| TGbh | 12/7 | Hamilton, Mark | Ruckus/CommScope |
| TGbh | 12/7 | Hervieu, Lili | Cable Television Laboratories Inc. (CableLabs) |
| TGbh | 12/7 | Huang, Po-Kai | Intel Corporation |
| TGbh | 12/7 | Kneckt, Jarkko | Apple, Inc. |
| TGbh | 12/7 | Lu, Liuming | Guangdong OPPO Mobile Telecommunications Corp.,Ltd |
| TGbh | 12/7 | Lumbatis, Kurt | CommScope, Inc. |
| TGbh | 12/7 | Orr, Stephen | Cisco Systems, Inc. |
| TGbh | 12/7 | Shalom, Hai | Google |
| TGbh | 12/7 | Smith, Graham | SRT Wireless |
| TGbh | 12/7 | Smith, Luther | CableLabs |
| TGbh | 12/7 | Torab Jahromi, Payam | Facebook |