IEEE P802.11
Wireless LANs

|  |
| --- |
|  TGbi Minutes Electronic **Interim Session 13-21 Sep** 2021 |
| Date: 2021-09-19 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Amelia Andersdotter | self | Brussels, Belgium |  | amelia.ieee@andersdotter.cc |

Abstract

This document contains the minutes for the IEEE 802.11bi task group meeting that took place during the IEEE 802 Electronic Interim Session 13-17 September 2021.

Note: Highlighted text are action items.

Q – proceeds a question

A - proceeds an answer

C - proceeds a comment

Yellow highlight - action point

**Chair: Carol Ansley, Cox Communications**

**Secretary: Amelia Andersdotter, self**

**Vice-chairs: Jerome Henri, Cisco; Stephen McCann, Huawei**

**Technical editor: Po-Kai Huang, Intel**

**1st slot. Wednesday 15 September 2021, 11:15 ET.**

Chair calls meeting to order at 11:17 ET.

Agenda slide deck: 11-21-1308r3:

1. Reminder to do attendance.
2. The chair mentioned the call for essential patents
	1. No one responded to the call for essential patents
3. The chair covered the IEEE copyright and participation rules.
4. **Discussion of agenda 11-21-1308r3 (slide #17)**
	1. Request to move 11-21/1396 to Wednesday slot, if possible, to better accommodate for Pacific Time Zone. Agreement in principle.
	2. Unanimous approval of the agenda.
5. **Administration**
	1. **Motion #5:** Approve previous minutes

Approve the minutes for:

2021 July 802.11 Electronic Plenary – July 12-20: 11-21/1225r0,

TGbi Teleconferences: 11-21/1359r0, 11-21/1402r0, 11-21/1469r0

Moved: Po-Kai Huang

Seconded: Dan Harkins

Approved by unanimous consent (33 participants).

* 1. **Updating the issue-tracking document** (11-21/641r3)
		1. When there has been a straw-poll for a use-case slide and it is included in the minutes as an action point to put the use-case in the use-case document, the technical editor will put it in the use-case document.
	2. **Teleconferences**
		1. The task group will try as much as possible to avoid colliding with TGbe meetings, because there is a lot of overlap among participants that go to both task groups. But teleconferences could be longer when there are no TGbe meetings scheduled for a Thursday (i.e. two hours instead of one hour). Starting later than 13h GMT is also a consideration which will be looked into.
1. Technical Presentations
	1. **View on Private Identifier (11-21/1395r2),** Po-Kai Huang (Intel)

Discussion:

C: I agree that the discussions around private identifiers to deal with state-bound conditions are very similar in TGbh and TGbi. But if we're going to ask who should be responsible for actually dealing with the introduction of a state-bound preserving identifier to be used when MAC addresses are randomized, I do think TGbh is the more appropriate group to deal with this. TGbh also may need to complete its work before TGbi can move ahead to completion.

A: I guess then you also agree that we hardly need two different solutions and that we have a challenge here. I'm just here looking for some agreement in principle on what we're looking for so that we end up with one rather than two solutions.

C: I feel that this work needs to be done in TGbi rather than TGbh. But now, for some stuff we require still that MAC addresses return to the default, like RSN, pre-authentication, PMK and such, even though we could be using PMKID or anything else. I have wanted PMK caching to work across the ESS for a long time, and still have everyone agree that the security requirements are fulfilled, ever since .11i. And so I think we need to go back and look at this and some of the more fundamental security guarantees that were previously argued over in .11aq and .11i. I do hope that there is a better scope for getting this work done in TGbi now. I mean, we're assuming that the network identifiers are always static and that we only have to deal with client side identities changing - I don't think that this is the case, and I don't think that MAC addresses are even appropriate, necessarily, as AP STA identifiers. This is work that we should be looking back at, or into.

A: I'm absolutely happy to both look into the history of this, and study the issue further but I can't make any immediate assessment. The only brief thing which I thought I understood was that .11aq was not restricted only to client STA but covered STA in general.

C: I agree that we need to define an identity for state-bound situations where state needs to be maintained. What I do want to add to this is that privacy is not only about not sharing information but also about sharing information with who you choose, so we may need an even more complex description of the general problem than what you have put in this presentation. We should also try and set our foot down on where to deal with this or these new identifiers once and for all, that's perfectly clear.

A: Point well taken. It was a simplification here in the problem description, but I hoped to achieve the clarity at least on wanting only one solution in the end.

C: About a year ago I withdrew a presentation from TGmd and put it to the study group that preceded this task group, that concerned PKMID. I am planning to bring it back into TGbi at some point in future, probably within one or two months so I just wanted to pre-announce that now in response to the earlier comment on PKMID and MAC randomization.

* 1. **Privacy Protection Gaps (11-21/1396r0),** Thomas Derham (Broadcom)

Discussion

C: One general comment, on slide 7 you talk about step 1 and step 2 and step 3 for progressive protection of PII and PCI. Am I correct in assuming that this is a post-association phase?

A: Well, step 1 is MAC pre-association, step 2 is MAC post-association and step 3 contains the more advanced cases that we may also want to delve into eventually.

C: So my understanding of step 2 is that we first need to recognise that MAC addresses should be randomized even after association.

A: So I think being able to randomize your MAC address while you are associated to an ESS is a good pre-cursor to solving a lot of problems, but I don't think it's a necessary requirement to solve problems within step 2. We should definitely talk about this PKMID ideas that were raised earlier. And also keeping the same MAC address inside of an ESS could potentially allow for longer-term fingerprinting inside of that ESS.

Q: So I saw that you are touching on PHY headers as well, and I had previously understood that this was more of a MAC amendment? Also I would like to know more about this beamforming report action frames - the CSI revealing information for instance?

A: I don't think that the PHY as such is mentioned in the PAR, but sometimes MAC items touch the PHY. We put PHY privacy implications also in here for completion but you may be right that this is not the best group to address the issue. Now, your other question - one way for an attacker to get information about CSI is simply just to sniff traffic by being sufficiently close. Another approach is that you have two peer devices exchanging CSI over the air. Of course, generally you do need quite high CSI for these attacks to work, but with two peer devices that might be even easier if the CSI is sent at a constant rate. But just for physical reasons you could of course listen to any rate of traffic and try and draw conclusions from that.

C: I'm wondering if you were thinking about using encryption for protection, for instance.

A: Yeah, that could be one way.

C: So I think step 2 problems may be easier to address because you reach an associated state and then you can use encryption or whatever to mask the data. However, in step 1 you run into problems - if all clients are masking or encrypting in the same way that just creates more PCI. So there are some identity solutions, like PASN and others, that either bring or don't much complexity, or too much, if used for every problem?

A: I didn't intend to evaluate each of the solutions by their complexity here but rather just present some different possible solutions, but you're right we should evaluate possible solution or solutions to any problem also with respect to complexity. I see that problem.

Q: Are you trying to make a chronological order on how we solve these problems? Or is it sequentialisation in some other way? Like we should solve step 1 before moving on to step 2?

A: Well, it is a sort of attempt to do a sequentialisation of the problems and when we try to approach them. Step 1 can be very challenging, and step 2 contains some more invasive problems that we might want to look into, while step 3 even contains PHY aspects that we already heard could be contentious with the PAR and go deeper if we already satisfied ourselves with the other two steps. But we're not at all suggesting that simple solutions for problems described under step 3 shouldn't be worked on only because all the issues under step 1 and 2 are not addressed - low-hanging fruit etc.

Q: But then should you not add randomized MAC under step 2?

A: In principle of course, but there is some nuance there that I would like to express and perhaps work on offline.

C: I wanted to take this opportunity just to thank Thomas for giving such a comprehensive overview of the problems at different parts of pre-association, post-association, and further PHY problems. It feels like it might be important for getting our work ahead.

A: Well, thank you for that obviously. I will speak to commenters offline to see how this can be restructured a bit, and perhaps also get some additions to the issue tracking document.

1. **Cancellation of Thursday slot**

Discussion:

Chair: Since we already covered the presentation we may not need to actually have three sessions in this week. We have some strawpolls that we could take on Friday. Is there anyone against cancelling tomorrow's session?

Chair: I hear no objections.

IEEE 802.11 Interim Session Thursday slot is cancelled.

1. **Recess at 13:02.**

**2nd slot. Cancelled.**

**3rd slot. Friday 17 September 2021 11:00 ET**

1. **Call to order 11:17 ET**
2. Reminder of policies (see also point 2-3 above).
3. **Review of agenda (11-21/1308r4 slide #17)**
	1. Agenda approved by unanimous consent
4. Administrative
	1. Teleconferencing from now on. Thursday 7 October is vacant from a TGbe perspective, which would allow a later scheduling of TGbi. However, it's also Golden Week in China and so may be conflicting with public holidays there. Another alternative is to move teleconferences to Tuesdays once TGbc is in recirc.
	2. TGbc will be in recirc three weeks in October, but will still be working on teleconference calls during that time.
5. Strawpolls
	1. **Presentation 11-21/1183r4:**
		1. **Strawpoll #1:** Does the .11bi working group wish to add to its list of data privacy concerns the inclusion of 1) SSID Elements or 2) SSID List Elements in Probe Requests which could lead to device fingerprinting and PCI or PII data being captured for devices?
		2. **Result** Yes: 14, No: 6, Abstain: 8, No answer: 19 (total participants: 47)
	2. **Presentation 11-21/1246r1:** *Remote stalking in public spaces, where static MAC address used to track individual devices that are associated.*
		1. **Strawpoll #2:** Do you agree adding "Remote stalking in public spaces" (as defined in 11-21/1246r1) use case into TGbi proposed issues document (11-21/641)?
		2. Discussion:

C: What are these strawpolls meant to achieve? Do they make decisions? Should we then use motions?

C: We just need to have an event that is recorded in the minutes that assists the technical editor in actually revising the issue tracking document without making personal assessments.

C: We can't adopt a strawpoll by unanimous consent, so if we want unanimous consent or no objections to adding something to the issue tracking document, then the strawpoll is not the tool for achieving this. Motions can be adopted by unanimous consent.

C: Going all the way to motions for these use-cases and updating an issue tracking document is needless formality. We should not over-formalize at this point since the issue tracking is only meant to be indicative of work we may be doing later in the process. It does not relate to specification text.

C: This process needs to be clarified. What kind of strawpoll result would imply that a use-case gets added to the issue-tracking document?

**Chair: If the number of yes is larger than the number of no, with no relevance given to abstains or non-voters. If you care, vote yes or no. If you don't care, well, you don't care.**

* + 1. **Result:** Yes: 25, No: 4, Abstain: 4,
		2. Use-case can be added to issue-tracking document.
1. **Presentations.**
	1. **Changing STA MAC addresses per association (11-21/1328r1),** Duncan Ho, Phil Hawkes (Qualcomm)
		1. Wants to add use-case to issue-tracking document (11-21/1328r1 slide #7).
		2. Discussion:

Q: There is a potential conflict with TGbh work. How will this be resolved?

A: This is related to TGbe work as well, and might be a timing issue. Whether .11bh should wait for .11be or can move ahead regardless is another question, but I think this should be in TGbh.

C: Some agreement that fixed addresses need to be protected. But if you have a mobile phone providing internet connectivity to other devices, then that is a personal device and should be able to change MAC address too in spite of being an AP. So we should not lose track of that.

A: For this document there is a focus on the client side, not the AP side, but it's noted that APs are also trackable.

C: AIDs, package numbers, sequence numbers and such are also trackable and so we cannot be satisfied with just changing MAC. This is also discussed in 11-21/1396r0 (see above point 6.2).

C: that can be done if both AP and STA agree on a function that will help them identify (even though the MAC addresses may change every frame of will change in fixed times or change every association) and use that in future

Q: This is light on issues. So could you clarify perhaps the issues that you wanted to address here?

A: We could try to specify.

Q: Is this concerned with allowing changing MAC address even when associating with a previous AP (at the moment we keep same MAC for each ESS), or is this also to allow changing MAC while associated?
C: changing MAC addr for each association; not during an association; and to provide means for DS to be able to follow the STA within an ESS even if it changes the over-the-air addr

C: I think changing TA/RA is 11bh issue, but the fact that TA is coupled w/ SA and is not protected in the header might be a 11bi/privacy issue. DS probably does not care about TA, but only about SA (if they can be different, and SA does not have to keep changing)

C: In my opinion: TGbh is scoped to "fix" issues that arise from changing a MAC address. So, the TA/SA coupling woudl be included in that

C: perhaps. Privacy of SA (e.g. encrypting or something) would be 11bi? or will 11bh cover that also?

C: TGbh does make any distinction between changing the TA or the SA. (In fact, currently, when devices "randomize their MAC" they are changing both.) This could be a question of scope between TGbi and TGbe?

C: How would we deal with legacy devices after TGbe if some devices change their TA/SA identifiers?

C: It's possible that a software solution could be implemented to deal with legacy devices.

Q: does it or does it not seek to cover the idea that the MAC address can change wile associated?

A: I think they should be changeable during association.

A: Agree. Post-association too.

C: We could at least adopt this preliminary issue, and then further down the line we should be looking not just at client side problems but also at AP side problems for the reasons mentioned earlier.

C: Post-association change of MAC address would definitely be within TGbi scope.

C: It seems that if this were described as "a new mechanism that allows a non-AP STA to change its MAC address(es) and stay associated", that does sound like a privacy enhancement and TGbi scope. But, the presentation talks about the "impacts" of changing a MAC address, which is a bit confusing

* + 1. **Strawpoll #3:** Do you agree to include this “STA MAC address persistence within an ESS” issue in document “21/641 Proposed Issues”?
		2. **Result:** Yes: 21, No: 0, Need more information: 11, Abstain: 3, No answer: 14
		3. Use-case to be added to issue tracking document.
		4. More information might be needed in future. However, we should not be adding more information to the strawpolls for adding things to the issue tracking document - such as new answering alternatives. It will make things procedurally more difficult.
		5. Discussion about using straw-polls to add use-cases to issue tracking document. Underlined that the procedure needs to remain the same through-out.
	1. **SA/DA Hiding (11-21/1464r0),** Duncan Ho, Phil Hawkes (Qualcomm)
		1. Discussion:

Q: In practice it may not be so easy to map MLD to randomized MAC. So why is this important?

A: Its about information being over the air accessible to third parties. That's why we should do something about this.

C: There are no reasons to send these in the clear over the air. We can put them in MPDUs or other protected frames so the general solution is already there. This is important that we continue to address this.

C: I agree basically that we're not protecting the network address here, but the TA and DA fields here would be fixed like if you have a TV and you're streaming to it. Then the privacy of the STA transmitting that stream is compromised even though it has a randomized MAC. That is something we should be looking more at. Where I'm less hesitant is if this formulation of the use-case captures that entire problem.

C: We should generally recognize that sending SA & DA clear OTA is unnecessary.

* + 1. **Strawpoll #4:** Do you agree to include this “Tracking SA and DA OTA ” issue in document “21/641 Proposed Issues”?
		2. **Result:** Yes: 13, No: 12, Abstain: 7, No answer: 14
		3. **Chair reminds that if the number of "yes" is larger than the number of "no" it goes in the issue tracking document.**
		4. Use-case to be added to issue tracking document.
		5. Further discussion about close-call straw polls. In the preliminary phase of the group's work it might be better to cast a broad net, so that issues can be sorted out and removed from the group's agenda later. There should be no need for a too rigid threshold for putting stuff in the issue tracking document at this time. Underlined that it's important for procedure to remain the same through-out.
1. Running out of meeting time. Other presentations postponed until the next meeting.
2. AoB.
	1. No AoB.
3. Chair adjourned the meeting at 13:17 ET.