IEEE P802.11
Wireless LANs

|  |
| --- |
|  TGbi Teleconference Minutes **August 12**th 2021 |
| Date: 2021-08-15 |
| 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 on 12 August 2021 at 09:00 ET.

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**

Chair calls meeting to order at 9:02 ET.

Agenda slide deck: 11-21-1309r1:

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.
	1. No questions
4. **Discussion of agenda 11-21-1309r1**
	1. No objections to the agenda.
	2. Addition to the agenda of presentation 11-21-0993r0.
	3. Approval of the agenda.
5. **Presentations.**
	1. Proposal to enhance PASN with an FT mode (11/21-985r0), Jerome Henri (Cisco).

**Discussion**

Q: Does this establish a FT key or is it only the DS mechanism?

A: You would get a temporal key from access points AP1 and AP2, and they may in turn have a key hierarchy in the background. But in RSNA mode not really.

Q: Then these keys would only be used for re-association?

A: As currently envisaged, this is correct. Maybe we could enhance this, but it is not something that we have discussed or thought about so far.

C: The strawpoll should clarify that there is no key hierarchy in the non RSNA-forming situation envisaged in this proposal. (strawpoll clarified)

Q: In your presentation, do the multiple APs know about each other in advance (inside of an ESS for instance) or could they be unrelated?

A: We're making the assumption that AP1 and AP2 are somehow part of the same system. There's no guarantee that they are part of the same ESS, but there is an assumption they are belonging to the same trusted group.

Q: This was very interesting, thank you. With respect to PASN, I think we should pursue this. But what I hope is that we can come up with something lighter-weight than PASN to do the same privacy protection that PASN does. I think we might need to do entirely different pre-association mechanisms.

A: We designed this thinking AP and of course other AP will send MDE and such. But I'd love to work on at least use-cases where PASN works well, and where we might need alternative mechanisms.

Q: Public key information is often neatly assigned to the user. Would this proposal be exposing a potentially trackable item and should we be looking at that more closely?

A: Good question. I don't know. I will have to ask for more information. The temporal key I would assume provides protection.

C: But the communication begins with the non-AP STA sending its public key out. Any exchange that is protected by that public key is afterwards protected and the future communication after that exchange can be assumed secured. But in the initial exchange of the public key when you establish an association, you have potential data exposure.

A: The temporal key and the MAC that is established would constitute some data that could be trackable. At some point you would see them, it's true.

C: If the PASN exchanges all use a new ephemeral key then the exchanges would not necessarily be trackable over time. The exchanges as such and potential backends between APs are in that case more trackable, or provide more tracking options.

Q: I'm wondering about adoption of this mechanism - is this strawpoll about adoption of a text or is it about supporting further study of this use-case or mechanism?

C: I also think adoption is not good word. "Study the design of" or "continuing work on" I think are sufficient for the strawpoll.

A: Not a problem.

Strawpoll indicates support for continuing work on this item.

* 1. Enhancing Privacy – Following a user use case (11-21/0993r0), Antonio de la Oliva (InterDigital)

**Discussion**

Q: Isn't this the same thing that is being addressed in bh?

A: I don't think so. The mechanisms that we need are out of scope in bh.

C: For me the question is whether we are trying to fix something that is broken or whether we are trying to improve privacy. This use-case seems to me not only highlighting that we need to fix something that is being broken by MAC rotation but it is actually looking at alternatives that are still privacy preserving. If you are trying to increase the privacy by accommodating for the MAC rotation, I think that's definitely within our scope - perhaps outsourcing some of the work to bh if we need.

C: In bh there are already discussions on a stable identifier for the hotel use case so I'm not sure what is the problem here.

A: Here the proposal is for bi to study a mechanism that allows a rotating identifier while at the same time maintaining an association. It's not just about preserving existing use-cases.

C: Not sure i understand who you're trying to protect from whom.

A: For instance someone in a hotel lobby that is sniffing traffic - currently we don't rotate MAC addresses inside of the same ESS, like in the same hotel network.

C: This is sort of being addressed already in bh though, so not sure it needs to be addressed here too. We're almost already there in figuring out how we can create this stable identifier and how to render the MAC address useless.

**Chair:** We're down to our last two minutes, and I'm not sure we'll finish the discussion in these last two minutes. Let's stop here, and feel free to contact the presenter offline. We will continue this discussion in two weeks and finish it up there. Any objections to handling it this way?

**No objections.**

1. AoB
	1. None
2. Chair adjourned the meeting at 10:01 ET.

**Attendance**

|  |  |
| --- | --- |
| **Name** | **Affiliation** |
| Andersdotter, Amelia | None - Self-funded |
| Ansley, Carol | Cox Communications Inc. |
| Hamilton, Mark | Ruckus/CommScope |
| Henry, Jerome | Cisco Systems, Inc. |
| Ho, Duncan | Qualcomm Incorporated |
| Huang, Po-Kai | Intel Corporation |
| Lu, Liuming | Guangdong OPPO Mobile Telecommunications Corp.,Ltd |
| Lumbatis, Kurt | CommScope, Inc. |
| Luo, Chaoming | Beijing OPPO telecommunications corp., ltd. |
| McCann, Stephen | Huawei Technologies Co., Ltd |
| Petrick, Albert | InterDigital |
| Shalom, Hai | Google |
| Smith, Graham | SRT Wireless |
| Sun, Bo | ZTE Corporation |
| Wang, Qi | Apple, Inc. |
| Yee, Peter | NSA-CSD |