IEEE P802.11
Wireless LANs

|  |
| --- |
|  Minutes TGbi Interim Meeting Ma**y** 12th-14th 2021 |
| Date: 2021-05-27 |
| 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 May 12 and May 14, 2021.

Note: Highlighted text are action items.

Q – proceeds a question

A - proceeds an answer

C - proceeds a comment

r1: anticipated formatting error pre-empted.

# Wednesday May 12th 2021, 11:15 – 13:15 ET

**Chair: Carol Ansley, Cox Communications**

**Acting Secretary: Amelia Andersdotter, self**

The teleconference was called to order by Chair 11:18 ET.

Agenda slide deck: 11-21-0642r2:

1. The chair read out the policies and procedures
	1. No questions
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. **Review of the Agenda 11-21-0642r2.**
	1. Add telecon minutes in contained in document 11-21-0817r1 to motions for the interim meeting Friday slot.
	2. Agenda approved by unanimous consent without further comments.
5. **Motion #1**
	1. Approve teleconference minutes contained in documents 21/436, 21/437, 21/638 and 21/732.
	2. Moved: Mike Montemurro, 2nd: Stuart Kerry
	3. No questions or comments on the motion.
	4. Approved by unanimous consent. (79 attendees)
6. **Presentation (11-20/940r0) :** Introduction to P802E by Jerome Henri (Cisco) and Amelia Andersdotter (self).
	1. C: These guideslines are good.
	2. Q: What does it mean to have an annex detailing privacy aspects? Why an annex?
		1. A: Privacy considerations can't always be incorporated in the standard and an annex can catch nuances, settings and configurations or recommendations.
	3. C: In section 12.2.10 of the standard we do have a MAC address privacy title that covers unassociated behaviour.
	4. C: These sorts of guidelines and questionnaires seem to be in line with what is already happening in the IETF with security considerations as part of every adopted RFC. Other standards bodies may also be doing this.
	5. Q: Why is PCI not mentioned in the privacy definition?
		1. A: The privacy definition is not in the recommendations at all, since privacy is a nuanced concept and highly context-dependent. The recommendations define personal identifiable information (PII) and personal correlatable information (PCI).
	6. No other questions.
7. **Presentation (11-21/641r1):** Proposed issues by Carol Ansley (Cox Communications)
	1. Q: What is the timeframe for collecting use-cases? Should we be including reference documents in the template provided for providing a use-case and what level of maturity are we expecting from these use-cases?
		1. A: We have no exact time-frame for collecting use-cases. Reference documents are voluntary, but may help. The use-case template slide is quite free-form so feel free to write down the use-cases as you see fit.
	2. Q: The current use-case specified in the presentation references 11-21/488r0, and this document already proposes changes to the standard through work in TGme. What is the time-frame for that text?
		1. A: Towards the end of the year we should be on a stable enough footing to start writing text.
	3. Q: Maybe we could save up enough use-cases to start writing one of those informative annexes that Jerôme presented on?
		1. C: That may be a lot of work if we need to go through the entire standard.
	4. Q: How should we be dealing with PHY related tracking issues? Many tracking issues in the PHY are implementation specific, such as soft AP or CFO.
		1. C: We may be restricted to addressing MAC level issues by our PAR.
		2. C: .11aq amendment addressed scrambler issues even though the PAR was nominally related to MAC level issues.
		3. C: Lower level MAC features are not well-protected today so we have scope for improvement there.
	5. No more questions.
8. Recess at 12:30 ET.
9. Chair resumes the meeting on Friday May 14, 2021, at 11:18 ET.
10. Reminder of policies
11. **Presentation (11-21/839r0):** Privacy Enhancement to avoid Element Fingerprint by Po-Kai Huang (Intel)
	1. Q: I agree on the fingerprint use-case you presented in slide 4. But three questions. When you talk aout the private limited connection, what security credentials are you seeing being used though? Same as for the proper association?
	Second, you talked about the life-time of the PMKSA. Have you given consideration to the storage requirement on the network side for maintaining the PMKs? Since this is a pairwise connection, this will apply to each individual connection and the AP then needs to store the PMK for some time, so that when you come back you can use it again, but if you roam around you need to go through the entire procedure with each AP?
	Third, have you considered active down-grade attack, where the attacker tries to get you to reveal the information - and maybe fingerprinting is not the biggest risk there, but the AP says "ok i don't have your PMK" and then forces the STA back into insecure mode for instance?
		1. A: Your first question - depending on the authentication. In SAE you don't need to go through the association, but if you do .1X and EAP exchange, you need to consider association.
		2. C: There is also .11az work on tunnel association.
		3. A: We are open to looking at the .az procedure state machine.
		Now in relation to the second question, PMK tracking is a general question. It's called opportunistic key caching? I can't really say much about life-time and storage requirements since it will be implementation specific.
		Third, on active downgrade, we're trying to utilize the full authentication. so if somehow there is a problem you probably can't decode this exchange anyway so the worst case is that somehow there will be a mistake in the PMKID exchanges. But I'm more than happy to discuss this more offline in case I missed anything.
	2. Q: You mentioned roaming but i assume what you mean is BSS transition, correct?
		1. A: Correct.
		2. C: We probably need to look at the FT protocol and how the FT protocol impacts privacy and what we might want to do there. More generally the problems with privacy and security aren't exactly the same - they are related and sometimes the requirements are conflicting. I think we might want to take a step back and look at the exchanges pre- and post-association. Going through scanning, ANQP, and identify potential elements within those that oculd be used for fingerprinting and affect privacy, and develop a solution like what you describe here.
	3. C: There was a contribution on PMKSA caching in RevMD and basically it will be in .bi eventually, just to announce that. The spec text for PMKID is already proposed since it was targetted to RevMD, but through further discussion we may decide that in .bi we want to do it differently.
		1. A: We are really just looking for low-hanging fruit. We believe that we can advance by finding these fixable problems relatively quickly.
	4. Q: In the end you are disclosing that you are a STA changing your MAC address since you are somehow disclosing that you're a STA doing something different from the other STA. How do you foresee protecting the STA against this?
		1. A: Is this related to MAC address change rate?
		2. A: No.
		3. A: Then it's not clear.
	5. Q: Is the process you explain really a full association? Like do you exchange data frames during this association?
		1. A: This is similar to Thomas' question, how is this related to association procedure, etc. Do whatever you need up to the point where you have the PMKSA and PMKID. If you use SAE you don't need association. With EAP you need data exchange and that's what you're asking?
		2. A: Yeah.
		3. A: The point here is really just to get to the point past the first PMKID generation.
		4. Q: When you generate the key to encrypt the association keys, would these keys would specific to each association and where do you get the context data to generate this keys?
		5. A: We've really just identified minimal requirements but we can discuss this.
		6. C: The FT protocol is completely undone by this, and in some other protocols you get redundant frames - so we need to consider optimizing these exchanges to avoid breaking FT and avoiding the redundant frames. I think we need to be more open towards changing existing designs instead of just re-using.
		7. C: If you create state on the AP and you want to return to that AP you need to return back to that MAC address you used to create the state. PMKID caching as described here, requires revival of an old MAC address and not have new MAC addresses. Is this a change that you're asking for?
		8. A: We can discuss this. We're open to this.
		9. C: It's just that this was discussed, and there was not uptake. I'm entirely in favour of talking about this and deploying it but I don't know if that is what is going to happen.
		10. C: Having some level of shared state between AP and STA is probably reasonable.
		11. C: A fixed MAC per SSID is an intermediate step during a grace period until an alternative means to identify devices is found (for the use cases discussed in 11bh such as captive portal), I think.
		12. C: We could also look at randomizing within an association within an SSID.
		13. C: Captive portal is probably a large reason that vendors have done fixed MAC per SSID. And sadly, captive portal is not something defined in 802.11 so there's really nothing we can do about them. Perhaps I'm being naive but I think that if your PMKSA is established with SAE or EAP then you don't need a fixed MAC per SSID. But I don't have insight into the companies that are doing fixed MAC per SSID so I'm just speculating.
		14. C: For EAP case I agree the network already has a (unique) client identifier. I think the issue is all the other cases where there is a group credential, or no credential at all. For some subset of scenarios they could migrate to authentication mechanisms with per-device/user credential, but for other scenarios that's probably not appropriate (anyway, I guess that's mostly an 11bh discussion).
	6. No more questions.
12. **Presentation (11-21/841r0):** Smart home use-case by Antonio de la Oliva (Interdigital), Joseph Levy (Interdigital) and Amelia Andersdotter (self).
	1. Q: Are you envisioning that one of the things we could work on is randomized rotation schemes when associated? In 802.1Adk envisages a mechanism where frames can degenerate with timers and fixed size, and these frames could sometimes contain data and sometimes not - and in 802.3 these frames can be used to obfuscate traffic. Do you envisage this also? Basically they have fixed-size frames so that you can't profile the contents of the frames.
		1. A: This is something we have to look at, ways of obfuscating information within the frames. This is not exactly what you're saying. We could absolutely study fixed-size frames but we know that there are some drawbacks. I also think we should be studying randomization of MAC addresses during an association.
	2. Q: Have you also considered potential privacy impact of gathering data on power save modes and similar? Is this something that we should add to the use-case?
		1. A: Can you provide more detail?
		2. C: Sensors can go in and out of power save mode and the information about that can be used to infer that they are sensors.
		3. A: Are there not easier ways of understanding if something is a sensor? If you look at these online search engines for IoT devices you put in a MAC address, for instance. We could consider anything that releases data from the home, but the problem you describe is not the most urgent one as far as I can see.
	3. Q: I can only sniff traffic when I'm very close to my property. A lot of the analysis requires vision so if I want to know if a person is in the living room I need to already see if a person is there. Are we creating a problem that doesn't exist here? Because I guess I can already see in my drive way if I'm being attacked?
		1. A: You're missing that you're a lucky guy because the housing situation is not the same for everyone. From my home I can see about 60 networks, and i see the windows from all my neighbours. So I can already do inference on all these people.
		2. C: You could also use high-gain antennas to target your sniffing longer range.
13. AOB
	1. Q: How do we actually get the use-cases incorporated in the proposed issues document?
		1. A: Use the template use-case slide, and then organise a straw-poll with the group.
		2. A: OK.
	2. Chair: A reminder for everyone to bring presentations and issues. The next teleconference will be on 20th May 2021 at 9AM ET.
14. Chair adjourns session at 12:47 ET.