IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TGbi Teleconference Minutes 21 April 2022 | | | | |
| Date: 2022-04-25 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Amelia Andersdotter | Sky UK Group | Brussels, Belgium |  | amelia.ieee@andersdotter.cc |

**Chair: Carol Ansley, Cox Communications**

Abstract

This document contains the minutes for the IEEE 802.11bi task group meeting that took place on 21 April 2022 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

**Secretary: Amelia Andersdotter, Sky UK**

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

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

Chair calls meeting to order at 09:03 ET.

Agenda slide deck: 11-22-622r4:

1. Reminder to do attendance
2. Review of policies and procedures.
3. The chair mentioned the call for essential patents
   1. No one responded to the call for essential patents
4. The chair covered the IEEE copyright and participation rules.
   1. No questions
5. **Discussion of agenda 11-22-624r4 (slide #16)**
   1. Adoption of agenda 11-22-622r4 slide #16 as amended by unanimous consent (20 participants).
6. **Review of proposed requirements from document 11-22-1848r7**
   1. **Requirements related to issue 1**There are two requirements related to issue 1. Password identifiers are currently sent in the clear.  
        
      Discussion:  
        
      Chair: Any comment on first requirement?  
      Q: I'm not sure how to interpret the backwards compatibility. Not all clients will be able to use this capability of course, but I don't know if this also includes the possibility of having a BSS which includes both legacy and enhanced devices? The language as such is fine though, and I think we've discussed these topics in different groups over a long time. I'd assume the current language enjoys a broad agreement.  
      Q: I would suggest to add what the CPE acronym means somewhere? Otherwise I have no specific other comments, and the text is fine.  
      Chair: Any comment on second requirement? I understood from previous two commenters that both requirements are fine? We could run a strawpoll or just mark that we will be motioning them in the interim, agreed by unanimous consent.  
      C: I agree with the chair.  
      Chair: We can mark these requirements as ready to be motioned in the May 2022 interim meeting.
   2. **Requirements related to issue 2**  
        
      There are eleven requirements related to issue 2.  
        
      Discussion:  
        
      C: I think the difference here between requirement 3 and 20 is capitalisation in the word "probe request". But it's an editorial issue more than anything else. Maybe we can also extend requirements not just to apply "prior to authentication".   
      C: Why are we discussing whether two requirements are similar? Eventually we need proposals for spec text that fulfill requirements, but I don't think we need to delve into the details of requirement similarity at this point at this level.  
      C: I agree in requirement 3 we could remove "prior to authentication" but I don't have a strong objection to either 3 or 20.  
      C: I agree with previous speakers. Both 3 and 20 are acceptable to me as they are. However, post-association I'm not sure we need probe requests for CPEs at all, but we can discuss that at a later time.  
      C: I want to voice my support for the current grouping of requirements. I believe it will help us with requirements that, like requirement 3 and 20, use similar language.  
      Chair: We can mark 3 and 20 as ready to be motioned in the May 2022 interim meeting.  
      C: Requirements 4 and 5 also go in a similar direction. I'm ok with both or either.  
      C: I think we can accept 4, 5, 21, and 22 as a group.  
      C: I think these are at the same time requirements and solutions. They're subrequirements - the main thing is that we want to protect (re)association request and response fields, and then we need to do various things to accomplish that. I think the requirement we want is that we want to reduce the public accessibility of these fields and the proposed requirements are very prescriptive in how they go about doing that. I'm fine with the texts as they are in these requirements but want to have this concern noted.  
      C: I'm uncertain now if we have the agreement on the text in requirement 5, for instance? Is that sufficiently high-level, like it's the exchange of key specifically that's objectionable or are there other issues too?  
      C: I don't want to preclude pre-establishing of keys or non-key solutions to what I see as the base problem, but I'm not 100% sure of what we're doing in the solution space yet. I'm not objecting to this but I hope it doesn't tie us down also.   
      Chair: We can mark 5, 20 and 21 as ready to be motioned in the interim meeting and have further discussion requirement 4 in future.  
      C: I don't care if we discuss requirement 4 more, or if we approve it for motion today. I think the text is probably fine, and I think it's more important to move on. If we think that there will be many conflicting proposals for this mechanism we could drop it for now. We should probably better have motions between the more detailed technical contributions on how to use key material.  
      C: I agree with previous speaker.  
      Chair: Hearing no objection, I will mark requirement 4 also as ready for motion. That leaves us only with requirement 16 undiscussed.  
      C: I believe requirement 16 is too premature. It's in the right direction but we should be protecting all the elements.  
      C: I have an issue with the general direction of requirement 16 - we can always geolocate an AP if it's stationary. So I just don't see the point of this.  
      C: I have no problem discussing this requirement further, of course. The whole mobile AP topic is a new challenge.   
      C: In my view, the best privacy level is achieved by protecting both the AP and the non-AP STA. The mobile AP use-case is something very common, but it's not the only application. AP data leakage affects also non-AP STA. Traditionally, networks that tried to stay hidden used only hidden SSIDs, but here we can provide even better features for them to be hidden. So I think BSS privacy enhancement, or BPE, is for this reason very useful but we could discuss this further.  
      C: The requirements on this page only relate to issue 2, element fingerprinting, so just to highlight that the requirement here is only meant to solve exactly that issue. There could be other reasons to use this, of course, and I don't think we should preclude such additional uses in our work here in .11. In this sense, the current wording of this proposed requirement is good for me. That said, requirement 16 is different from the others on this page since it may impact the ability of non-AP STA to connect to APs - it's about APs protecting themselves, and that could negatively impact connectivity for non-AP STA. So we need to think about that.  
      Chair: I hear that we need to mark requirement 16 as needing further discussion.  
      C: On requirement 26, we could have a new frame rather than a protected version of an old type of frame?   
      C: Looking at MAC/PHY amendments in .11n/ac those amendments have all defined action frames as non-robust, and it has to do with time constraints and similar. Participants have found it very difficult to work around those problems. I think it will be still challenging to go against those already made conclusions at this point in time.  
      Chair: I hear that we need to make requirement 26 as needing further discussion.  
      Chair: Next time, we will start discussion on requirement 27. I will post an r5 of the agenda slide deck from this meeting, but action points noted here will not be transferred to the requirements tracking document yet.

1. AoB
   1. No other business.
2. Chair adjourned the meeting at 10:00 ET.

**Attendance**

|  |  |
| --- | --- |
| **Name** | **Affiliation** |
| Andersdotter, Amelia | Sky UK Group |
| Ansley, Carol | Cox Communications |
| Halasz, David | Morse Micro |
| Hawkes, Philip | Qualcomm Incorporated |
| Henry, Jerome | Cisco Systems, Inc. |
| Ho, Duncan | Qualcomm Incorporated |
| Huang, Po-Kai | Intel Corporation |
| Kain, Carl | USDOT; Noblis, Inc |
| Kneckt, Jarkko | Apple, Inc. |
| Levy, Joseph | InterDigital, Inc. |
| Malinen, Jouni | Qualcomm Incorporated |
| McCann, Stephen | Huawei Technologies Co., Ltd |
| Montemurro, Michael | Huawei Technologies Co., Ltd |
| Mutgan, Okan | Nokia |
| Nezou, Patrice | Canon Research Centre France |
| Orr, Stephen | Cisco Systems, Inc. |
| Rosdahl, Jon | Qualcomm Technologies, Inc. |
| Sam, Harvey | Broadcom Corporation |
| Smith, Graham | SRT Wireless |
| Srivatsa, Veena | Synaptics |
| Thakore, Darshak | Cable Television Laboratories Inc. (CableLabs) |
| Torab Jahromi, Payam | Facebook |
| Yee, Peter | NSA-CSD |