IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TGbi Teleconference Minutes 25 August 2022 | | | | |
| Date: 2022-09-01 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Amelia Andersdotter | Comcast | Brussels, Belgium |  | amelia.ieee@andersdotter.cc |

Abstract

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

18 August 2022 at 10:00 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, Sky UK**

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

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

Chair calls meeting to order at 09:01 ET.

Agenda slide deck: 11-22-1322r3:

1. Reminder to do attendance
2. Review of policies and procedures.
   1. IEEE individual process slides were presented.
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 11-22-1322r3 (slide #16)**
   1. Addition of presentation 22/1367r0, Protection against Spoof AP, Graham Smith
   2. Addition of 22/1306r1 - BPE Beaconing And Discovery Requirements, Jarkko Kneckt
   3. Adoption of agenda 11-22-1322r2 slide #16 as amended by unanimous consent (XX participants).
6. **Administrative**
   1. Reminder of upcoming teleconference scheduled (two scheduled leading up to interim).
7. **Presentations**  
   1. **Protection against Spoof AP, 11-22-1367r0, Graham Smith (SR Technologies)**  
        
      The presentation contains a proposal for a new requirement that covers the spoof AP problem previously addressed in presentation 22/1253r0.  
        
      **Discussion:**  
        
      Q: So it's correct here that this tries to establish a way for the AP to communication to a non-AP STA that it's safe to connect to?  
      C: We've had these sort of suggestions already in the BPE discussions, that we could have a checksum and verify this somehow, to help establish whether there is a pre-shared key or other authentication mechanism. Then the AP could help the non-AP STA establish whether to send association frames or similar.   
      A: Yes, the AP could give a secret message or a key to STAs to help them know. We did have comments that you could copy such a secret message on the internet and use it for spoofing, and that would be very difficult to overcome.   
      Q: So is it correct that you could just relay packages from APs to spoof APs and then have the non-AP STA try to associate anyway? So could geolocation perhaps be an additional safe-guard?  
      A: I had three original solutions to this problem, with one of them including geolocation.  
      Q: How would a non-AP STA know how to determine a spoof AP from a non-spoof AP, or know what is the right location of the non-spoof AP? If we want to do something like this, let's be specific and clear. We need a message exchange then that authenticates the AP before association, right? While the AP could be privacy-enhanced, it should also provide a mechanism to authenticate itself? Right?  
      Q: Do we not want to say that we should identify the AP rather than authenticate it?  
      A: No, we do not want to identify the AP. That's what we're specifically trying not to do.  
      C: How do we separate malicious actors from non-malicious actors?  
      C: Maybe we want to be able to verify the identity of a known AP prior to transmission of pre-association PPDUs at least. Even if that identity is not per se revealed?  
      Q: Are we putting any provisions for cases of multiple APs?   
      A: Because this is a spoof AP situation, I don't know if you'd make a spoof ESS with multiple APs. But I'd guess a non-AP STA just tries to connect to the SSID of the ESS so it's the same thing and we don't need to treat it as a special case for the purpose of this requirement.   
        
      **Chair:** I will close the queue here. I will add this requirement to our proposed requirements.
   2. **Hashed SSID, 11-22-1383r0, Duncan Ho (Qualcomm)**This presentation aims to present a mechanism that could satisfy requirement 15, in order to provide further support for its inclusion in the approved requirements list.  
        
      **Discussion:  
        
      Q**: From a usability perspective this seems a bit awkward. So let's say you configure the SSID on the access point, and on the client you say "show me which SSIDs are there" and then you just click on that.  
      A: Well, we would not have that capability anymore with this solution. But many home SSIDs are hidden nowadays, and this would entail something like that - where you have to type in the SSID. This is already going on today so I don't think that is really a big change. If the SSID has to be discoverable over the air, of course it has to be in the clear and we can't protect that then.  
      C: In my experience, most of the time, I can't ever get anyone to tell me what the SSID actually is. I just have to scan and discover it myself.   
      C: I agree a lot of APs would continue to broadcast SSIDs.  
      Q: Specifically for the mobile AP use-case and BPE use-case this could work, and the intention is not here to push it to a general use-case?  
      A: That is correct.  
      C: Whatever solution we come up with here is probably not going to backwards compatible since we're trying to protect privacy from both the AP and non-AP STA side. Regular APs could continue to broadcast SSIDs then or we'd have a lot of problems, I think.  
      Q: Isn't there a similarity here with the presentation we had in 22/1306r0?   
      C: If you don't know the value of the hash here, you can't really show it to the user. You have to be able to calculate whether you know the network or AP, and that calculation needs to be specified somehow, I believe. SSIDs are typically human-picked names, and it's easy to guess them or run dictionary attacks against them. So I don't think they need to be in the hash parameters.   
      C: I think this is a better solution than hidden SSID.  
        
      Chair: I will put a strawpoll for this at the head of the agenda next week.
8. **AoB**
   1. No other business.
9. Chair adjourned the meeting at 10:01 ET.

**Attendance**

|  |  |
| --- | --- |
| **Name** | **Affiliation** |
| Andersdotter, Amelia | Sky UK Group |
| Ansley, Carol | Cox Communications Inc. |
| baron, stephane | Canon Research Centre France |
| Halasz, David | Morse Micro |
| Henry, Jerome | Cisco Systems, Inc. |
| Ho, Duncan | Qualcomm Incorporated |
| Huang, Po-Kai | Intel Corporation |
| Kneckt, Jarkko | Apple, Inc. |
| Lumbatis, Kurt | CommScope, Inc. |
| Mutgan, Okan | Nokia |
| Nezou, Patrice | Canon Research Centre France |
| Nikolich, Paul | self employed/various |
| Sevin, Julien | Canon Research Centre France |
| Smith, Graham | SRT Wireless |
| Smith, Luther | Cable Television Laboratories Inc. (CableLabs) |
| Sosack, Robert | Molex Incorporated |
| Stanley, Dorothy | Hewlett Packard Enterprise |
| Yee, Peter | NSA-CSD |