IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TGbi Teleconference Minutes 18 August 2022 | | | | |
| Date: 2022-08-21 | | | | |
| 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 10:03 ET.

Agenda slide deck: 11-22-1322r2:

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 11-22-1322r2 (slide #16)**
   1. Adoption of agenda 11-22-1322r2 slide #16 by unanimous consent (22participants).
6. **Administrative**
   1. Reminder of upcoming teleconference scheduled (two scheduled leading up to interim).
7. **Presentations**  
   1. **BPE Beaconing And Discovery Requirements, 11-22-1306r0, Jarkko Kneckt (Apple)**  
        
      **Discussion:**  
        
      **Chair:** We had to cut this discussion in our last meeting, so I wanted to make sure we had covered the entire queue.  
        
      No one raises additional questions.  
        
      **Chair:** If you have other comments, please bring them up directly with the presenter. I will add these requirements as proposed requirements.
   2. **Beacon Protection Against a Spoof AP, 11-22-1253r0, Graham Smith, SR Technologies  
        
      Q**: So I noticed here that you first mention the issue and then present solutions, but we're still in a requirements or problem-defining space.. So maybe we still need to boil this down to a problem and a requirement? Let's say the user connects to the network now, but what if the user goes and change the configuration? Does that mean the client ends up getting stuck because the configuration is new?  
      **A:** Good comments. I just know it's something that RCM does not solve.  
      **Q:** I wonder if this is actually an important problem to solve. I'm sympathetic with JLo, but do we need to address this? The last solution you presented here is very susceptible to an insider attack, because anyone connected to the real network would have to know the APs secret.  
      **A:** Yes.  
      **C:** I wanted to highlight that we originally did not intend to address this use-case with randomized or changing MAC address. We had originally intended to try and make sure that trashcans don't build complete profiles of people's movements in urban environments.  
      **Q:** Just for me to understand the problem here, you're saying that there is a spoof AP that tricks the client into sending an association request and this causes the client to be tracked?  
      **A:** Yes, this it the problem we consistently faced in TGbh when we were trying to make anti-RCM schemes. People are worried about this.  
      **Q:** But does the problem still persist if the association request is encrypted? What use is this information then?  
      **A:** Yes, true, but what people tell me is that the problem persists then. A spoof AP will still track you even if it doesn't accept your association. Its purpose is not to give you connectivity but to follow you around.  
      **Q:** But if you encrypt the association request then the spoof AP will not have that key? That's the core of my question here, I think. Because the whole frame is encrypted you just know it's some random client, not a specific client.   
      **A:** Yeah, but these are different scenarios which are coming up a lot in the TGbh area. If someone from JLo's home shows up at a café you know it's them.  
      **C:** I want to highlight this doesn't only apply to JLo. Any corporate or government entity that logs into a pre-determined address that identify them will be affected that. It's true that JLo got us talking about this, but the device is more generally applicable, I think. A device that looks for a home AP will have this problem. For me this falls within the parameters of what we should be doing. We could be providing one or several means to protect clients from sending or transmitting information they don't intend to transmit.  
      **C:** I agree with the previous speaker. However, on the solution proposals that were in this presentation, I'm a bit concerned with the first solution on using neighbour reports. A second concern is, if a device see a spoof device and tries to connect, and the device is not configured to stop trying to associate after it failed to do so, you would have user experience deterioration if it makes multiple attempts to connect.  
      **C:** For the case we're looking at, one thing that's unavoidable is that you have beacons that are then dropped within milliseconds. Any solution which doesn't involve some form of challenge has this weakness - we can always passively intercept connections in JLos house. The second comment is that, if we're going to provide solutions we need to be careful that we're not bringing in new problems through those solutions. If we introduce a BPPN number that increments, that gives you a way to start tracking a mobile AP - should we then also introduce a solution to that problem? We could probably get around that, by masking a BPPN, but it's a general comment on how we need to start reflecting on solutions here. But two parties working out if they know each other without revealing information about themselves is a difficult problem in general. I think that's just how it is.  
      **C:** Increasing privacy is like increasing any security capability. Nothing is 100% and if you throw enough resources at it you will always fail. It's about raising the bar.   
      **C:** Going back to our first comment, with our time-line we may want to rephrase this into a problem formulation and a requirement so that we can pass our requirements document in September. Can drop offline messages about this.
8. **AoB**
   1. No other business.
9. Chair adjourned the meeting at 10:57 ET.

**Attendance**

|  |  |
| --- | --- |
| **Name** | **Affiliation** |
| Andersdotter, Amelia | Sky UK Group |
| Ansley, Carol | Cox Communications Inc. |
| Halasz, David | Morse Micro |
| Harkins, Daniel | Hewlett Packard Enterprise (Aruba Networks) |
| Hawkes, Philip | Qualcomm Incorporated |
| Henry, Jerome | Cisco Systems, Inc. |
| Ho, Duncan | Qualcomm Incorporated |
| Huang, Po-Kai | Intel Corporation |
| Luo, Chaoming | Beijing OPPO telecommunications corp., ltd. |
| Montemurro, Michael | Huawei Technologies Co., Ltd |
| Mutgan, Okan | Nokia |
| Nezou, Patrice | Canon Research Centre France |
| RISON, Mark | Samsung Cambridge Solution Centre |
| Smith, Graham | SRT Wireless |
| Smith, Luther | Cable Television Laboratories Inc. (CableLabs) |
| Stacey, Robert | Intel Corporation |
| Stanley, Dorothy | Hewlett Packard Enterprise |
| Thakore, Darshak | Cable Television Laboratories Inc. (CableLabs) |
| Wang, Lei | Futurewei Technologies |
| Yee, Peter | NSA-CSD |