IEEE P802.11
Wireless LANs

|  |
| --- |
|  TGbi Teleconference Minutes 26 May 2022 |
| Date: 2022-06-03 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Amelia Andersdotter | Sky UK Group | Brussels, Belgium |  | amelia.ieee@andersdotter.cc |

Abstract

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

26 May 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

**Chair: Carol Ansley, Cox Communications**

**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: 11-22-622r8:

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 11-22-622r8 (slide #16)**
	1. Adoption of agenda 11-22-622r8 slide #16 by unanimous consent (15 participants).
6. **Administration**
	1. Requirements document 11-22-1848r8 now in revision 8, including requirements motioned in the May 2022 interim session. Review of r8 requested by chair.
7. **Review of proposed requirements from document 11-22-1848r8**
	1. **Order of requirements to be discussed

	Chair:** We have so far postponed discussion of BPE requirements, since CPE requirements were deemed more easily implemented and interoperable with legacy devices. So should we now continue to discuss "needs more discussion" CPE items? Or move on to BPE requirements? **C:** I have a preference for discussion CPE requirements for now, since the BPE requirements are likely to require hardware changes.
	**Chair:** We will revisit the CPE requirements marked as needing further discussion then.
	2. **Requirements related to issue 7 (cont. from 11-22/0801r0 p. 20.3)**Requirements table is also presented in document 11-22-622r8.

	**Discussion:

	Chair:** Moving back to requirement 31 .
	**C:** We've seen the power save bit being used for data mining and tracking before so I think this concern is valid.
	**C:** It's only a single bit here, and I think both in requirement 31 and 32 we have that same issue that if you go into power save this bit has to be transmitted. If we start to encrypt the bit we interfere with the entire architecture. I also want to reiterate the point that it's really just a single a bit.
	**C:** Our testing so far indicates that we will need hardware changes for both the Retry bit and the +HTC and power save fields, so requirements 31 to 33.
	**C:** I currently lack an assessment of the contribution of these bits to a fingerprinting attack.
	**C:** We can also volunteer more input on these requirements and how they contribute to fingerprinting.
	**Chair:** I hear there may be further analyses coming as we move along. I will mark requirements 31-33 as needing more discussion awaiting further input.
	**C:** I would like to check that +HTC and HT Control field are both targetting the leakage of sensing information?
	**C:** The HT Control field is definitely important to protect because it carries a lot of information. The +HTC field indicates that HT Control field is present so I guess we can discuss how to protect that and if it's necessary but we can come back to it.
	3. **Requirements related to issue 2 (cont. from 11-22-665r0 p. 6.2)**

	**Discussion:**

	**Chair:** We can move back to requirement 26.
	**C:** This requirement is too broad. There are many unicast management frames and here we ask for all of them to be encrypted. I don't think encrypting authentication and probe request frames is even feasible? Maybe we should look at having a list of frames to be encrypted?
	**C:** Does this relate only to the MAC header or to the entire frame?
	**C:** In my view, it says the entire frame, so it's not restricted to the header.
	**C:** In some of the management frames the payload is already encrypted. In the case of a probe request frame when the station is not associated yet it's not possible to have encryption - where would you get the key? We could think about when we have and when we don't have keys generated. After the keys are generated nothing really stops us from encrypting though.
	**C:** In the requirement it already specifies that the CPE client is associated, so the keys would already be there. Authentication mechanisms and probe requests pre-association are complicated to encrypt, yes, but this requirement doesn't say that. This is a post-association requirement. In my view this requirement also doesn't go as far as saying encrypting all the headers, because other requirements already cover the headers in various ways that may or may not include encryption or obfuscation.
	**C:** I think we already have a lot of management frames that have an unprotected or a protected version, and that we could specify unprotected frames that do not currently allow for this option and say that they should have that option. Beamforming frames, for instance? Do you think it's feasible with a list here?
	**C:** We could work on listing those frames. Going back to mandatory versus optional features I thought it was decided that TGbi features were in general optional and that we'd let the market decide what is a good way forward after the technologies are there.
	**C:** Requirement 26 seems more security oriented than privacy oriented? What is the actual privacy problem we're solving?
	**C:** These requirements are sorted as protecting against fingerprinting. If the frames are not protected they can be intercepted and information can be gleaned about the distinctive habits of the device, and therefore the owner or user of the device.
	**C:** Just saying unicast frames and "should have a list". I honestly don't see why this is a privacy issue unless you have specific privacy threats mapped against specific types of unicast management frames.
	**C:** We should also clarify that this requirement only applies to the frame body.
	**C:** This requirement falls under issue 7 as well as issue 2.
	**C:** For me, highlighting a particular privacy with for instance beamforming frames is entirely acceptable.
	**C:** In management frames we expose parameters in general. Whenever we can avoid openly distributing our operating parameters that's both a privacy and security improvement. I don't think we have a contradiction between privacy and security here. But we can have more discussions on individual management frames and their parameters, of course.
	**C:** We already have a mechanism for protecting management frames in the baseline standard, and now we're trying to build on that to enhance privacy. So what is the specific contribution that we're trying to undertake here? That's what I need to understand.
	**C:** I think measurement reports is a good example of information that could be protected as well.
	**C:** A better wording could be "bi should defined a protected version of <this list of management frames>". That would take some research, exactly which frames this would cover, but it will be helpful for our future work if we really know what we are planning to do and why.
	**Chair:** We seem like we need more discussion on this. I will mark requirement 26 as needing more discussion in the future.
	**Chair:** With this we're probably out of time for opening a new discussion topic. How about we give ourselves back four minutes?
8. **AoB**
	1. No other business.
9. Chair adjourned the meeting at 09:56 ET.

**Attendance**

|  |  |
| --- | --- |
| **Name** | **Affiliation** |
| Andersdotter, Amelia | Sky UK |
| Ansley, Carol | Cox Communications |
| Halasz, David | Morse Micro |
| Henry, Jerome | Cisco Systems, Inc. |
| Hervieu, Lili | Cable Television Laboratories Inc. (CableLabs) |
| Ho, Duncan | Qualcomm Incorporated |
| Huang, Po-Kai | Intel Corporation |
| Kneckt, Jarkko | Apple, Inc. |
| Lumbatis, Kurt | CommScope, Inc. |
| Luo, Chaoming | Beijing OPPO telecommunications corp., ltd. |
| McCann, Stephen | Huawei Technologies Co., Ltd |
| Montemurro, Michael | Huawei Technologies Co., Ltd |
| Mutgan, Okan | Nokia |
| Petrick, Albert | InterDigital |
| Rosdahl, Jon | Qualcomm Technologies, Inc. |
| Sam, Harvey | Broadcom Corporation |
| Smith, Luther | Cable Television Laboratories Inc. (CableLabs) |