IEEE P802.11
Wireless LANs

|  |
| --- |
|  TGbi Teleconference Minutes 7 October 2021 |
| Date: 2021-10-08 |
| 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 7 October 2021 at 10:00 ET. Last 30 minutes notes kindly taken by Stephen McCann (Huawei).

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, self**

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

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

Chair calls meeting to order at 10:03 ET.

Agenda slide deck: 11-21-1638r0:

1. Reminder to do attendance
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. **Discussion of agenda 11-21-1638r0 (slide 16)**
	1. Postponing discussion of 11-21-1539r0 due to unavailability of presenter.
	2. Amending in agenda doc number to 11-21-1599r0 Privacy Protection Issues.
	3. Adoption of agenda 11-21-1309r1 by unanimous consent.
5. **Administrative:**
	1. Reminder: Two more teleconferences on 21 Oct and 4 Nov at regular 9AM ET slot for one hour.
6. **Presentations.**
	1. **Privacy Protection Gaps (11-21/1396r1)**, Thomas Derham (Broadcom)

Two updates from last meeting on slide 7 (clarification of before and after association in step-description); previously MAC header topics were all in step 3 (advanced topics), but now they are distributed across steps (pre-, during and post-association). It's also been clarified that the steps are not sequential in terms of relevancy in addressing. No strawpolls for these documents.

**Discussion**

No discussion.

* 1. Privacy Protection Issues (11-21/1599r0), Thomas Derham (Broadcom)

A presentation of use-cases for the issue tracking document.

**Discussion**

Q: There is always a problem of defining soft or mobile AP in the spec, so how do we want to differentiate soft AP from other AP?

A: It is not clear to me that we have to differentiate them. In the spec we could clarify that some types of AP may experience particular types of problems more than other types of AP, or that some problems arise in situations which are not universally applicable.

Q: Do we not get a legacy compatibility problem then?

A: To some extent we have interoperability issue for every new feature, but of course it may be different if we develop new features for the AP, which acts as a hub for a lot of devices. We could perhaps envisage that these soft AP are not even discoverable by non-AP STA that can't respect the soft AP protection measures. But we need to determine that this is a problem first, and then perhaps discuss specific solutions.

C: So these questions come from the introduction of this new term "soft AP", so I'm raising lots of clarifying questions to weed that out.

A: How the actual spec text will look is way down the line for me, this is just introducing some use-case documents.

C: I want to say I agree with the above responses. We could work with this as a sort of privacy-enhanced AP eventually.

C: I also agree with the use-case presented on these "soft AP" or whatever we want to end up calling them.

Q: On Client MAC address, doesn't the spec already cover randomising the scrambler seed?

A: Only when you associate with BSS, I think, but I'm currently unsure.

Q: What is it that the scrambler seed leaks, like the threat? Your argument is that even if the MAC is randomised inside of a BSS, then there could be inadvertent data leakage from the communication of scrambler seeds?

A: I think the point we're trying to make here is that scrambler seeds can be tracked, and that changing the MAC address should at least provide the option of changing the scrambler seed as well. It seems like this is causing a lot of confusion, but the main idea is that a MAC address for instance is also connected to other identifiers and information elements.

Q: Some of the information points in usecase x+4 seem a bit random to me - like any element change could be a potential pattern. Is there an actual evidential threat?

A: I want to believe that there were a bunch of papers that actually combined various information elements and other data from MAC headers. These papers didn't necessarily differentiate so much between different forms of such information elements, but just stated that they can, when combined, form a pretty good unique identifier. Power save mode for instance, some devices do it quickly, others at prompt, and others have different behaviour. Some of it is maskable with traffic streams but perhaps not all of it.

Q: Are you thinking about pinpointing a specific device here, or a group of devices from a specific vendor?

A: More the latter, but say that you have a particular model with a particular version firmware. It narrows down quickly.

Q: The same application could be ran on different devices from different vendors though. So I wonder how easy it actually is to uniquely identify.

C: But these fingerprinting issues can also be used in active attacks, if for instance a particular seed change or other state change is provoked by an antagonist. I just wanted to point that out here.

C: Getting back to the point of individual versus groups of devices, we're currently in a world of such a lot of different devices, that identifying a device from a particular group is often enough to provide a unique identification. Devices have vendors, mobile operators and there are just so many distinguishing factors and so much fingerprinting information. So being in a small group means that you are mostly uniquely identified - not with 100% statistical certainty but with sufficiently high statistical certainty that it's practically speaking always a privacy threat.

C: I feel like the active attack topic and the fingerprinting topic are a bit different. For one, the active attack situation is a bit more severe I feel.

Q: The idea here is that if something is done at a particular time, then it might be fingerprintable, like with CSI information?

A: Yeah, if every time you tap your screen your device moves a couple of millimetres that changes the CSI readings and so that can already be used to identify a device with a particular usage pattern. You could also just measure the CSI readings from the channel directly if you're sufficiently close to the monitored device - this can be used even to figure out specifically what someone is typing, not just that they are typing. It's academic, and I will not be able to completely summarize these attacks here.

C: The PHY discussion might be out of scope but for completion I think it should still be in the issue tracking document.

C: On additional information elements, it should be the case that we take care of that.

Chair: do we have final questions before we move ahead to strawpolls?

C: Let's move aside use-case x+3 (SP 3) for now, but figure out the others.

**Straw Polls**

SP 1: **Do you agree adding “x+1) Protecting authentication identifiers and key identifiers” issue into TGbi proposed issues document (DCN 21-641)?**

Yes: 16 No: 1 Abstain: 1 (No answer: 4)

Use-case to be added to issue tracking document.

SP 2: **Do you agree adding “x+2) Soft/mobile AP privacy” issue into TGbi proposed issues document (DCN 21-641)?**

Yes: 13 No: 1 Abstain: 5 (No answer: 3)

Use-case to be added to issue tracking document.

SP 4: **Do you agree adding “x+4) Protecting behavioral fingerprinting while associated” issue into TGbi proposed issues document (DCN 21-641)?**

Yes: 14 No: 2 Abstain: 3 (No answer: 3)

Use-case to be added to issue tracking document.

SP 5: **Do you agree adding “x+5) PHY/RF related privacy” issue into TGbi proposed issues document (DCN 21-641)?**

Yes: 10 No: 3 Abstain: 6 (No answer: 3)

Use-case to be added to issue tracking document.

SP 6: **Do you agree updating the “Avoid Element Fingerprint” issue in TGbi proposed issues document (DCN 21-641) per “2bis”?**

Yes: 15 No: 0 Abstain: 2 (No answer: 5)

Use-case to be added to issue tracking document.

* 1. Directed Probe Addition to Issues Tracking Document (11-21/1633r1), Kurt Lumbatis (CommScope)

**Discussion**

Q: Is this correct format of the use case?

A: I’m open to any suggested changes, before it goes into the use case document.

C: I think the issue of the fingerprint tracking needs to be brought out a little more.

Q: I think there’s an error in your references on slide #3.

A: Yes, that needs correcting.

Q: What sort of enforcement will there be on legacy devices?

A: In 802.11aq there’s a statement about when SSID elements are placed into frames, information can be leaked.

C: I think it is also a problem that needs to be solved.

**Straw Poll**

**Do you agree to add “Avoid Fingerprinting from SSID Elements or SSID List Elements in Probe Requests” into the TGbi Proposed Issues document, (DCN 21/0641) ?**

Yes: 11, No: 0, Abstain: 4 (No answer: 6)

Use-case to be added to issue tracking document.

1. AoB
	1. None
2. Chair adjourned the meeting at 11:46 ET.

**Attendance**