IEEE P802.11
Wireless LANs

|  |
| --- |
|  TGbi Teleconference Minutes **August 26**th 2021 |
| Date: 2021-08-26 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Amelia Andersdotter | self | 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 August 2021 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, self**

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

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

Chair calls meeting to order at 9:02 ET.

Agenda slide deck: 11-21-1309r3:

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 11-21-1309r3**
	1. Addition of straw-poll on further investigations of use-case presented in 11-21/0993r0.
	2. Adoption of agenda 11-21-1309r4 by unanimous consent.
5. Administrative:
	1. Reminder: Agreed to move a teleconference to Wednesday 8 September 2021, 09:00 ET.
	2. Reminder: three sessions during the September interim meeting (Wednesday 11:15ET, Thursday 09:00ET, Friday 11:15ET).
6. **Presentations.**
	1. **Device fingerprinting leading to PCI capture (11-21/1182r2)**, Kurt Lumbatis (ARRIS/Commscope)

**Discussion**

Q: You're teasing apart two scenarios. One is when the network is already discovered or the client is already connecting, roam scan or direct probe, and such. But the other case is when you send directed probes to each of the SSIDs that there is already a network profile for, irrespective of whether they've actually discovered such a SSID network nearby. So are you trying to cover only this latter case, or both cases, and is there still - because we tried to fix the directed scan issue already - a big problem with clients doing that?

A: These tests were done in an ARRIS facility so there was no way these devices could have detected home or telecoms operator SSIDs in the area. So that seems to be still a problem with directed probing.

C: Some of the clients do it because the SSIDs in the saved networks are hidden.

C: Ah yes, that would be a misconfiguration of the SSID as hidden. That could happen.

Q: We should also consider probe requests, not just directed probes right? All of them.

A: Yeah, it's probe requests, authentication frames, and anything which is not encrypted.

Q: If you only use the broadcast SSID you will get a lot more access points responding and so you could consider bandwidth use. And we've looked at that before, from this efficiency perspective - so it'd be funny if we have one part of the spec saying one thing for guarding efficiency and another part of the spec saying something different, for privacy reasons, for instance.

A: I'm not looking at solutions at this time, but just presenting the general problem, but it's something we should be getting back to later.

C: Going back to hidden SSIDs, actually sending out the probe requests is the only way of discovering the networks so maybe we should be doing outreach and education on the privacy disadvantages.

Q: Do you know if the devices that you measured these properties from, if they are specially configured?

A: The devices were specifically configured for the test environment where they were. A mix of bridge devices, network extenders, personal devices used in the test environments, and a mix of HT only and HE stations, and so a broad range of different devices, yeah. Lots of manufacturers too.

Q: So if I bring my everyday use device which has my home network SSID in it, would it send that out in your test environment based on your test results? I'm just trying to get a feel for whether people set up hidden SSIDs.

A: Yes, that should be the case.

C: There are definitely a lot of devices that are looking for specific networks, and there is some data collected by students of Jim Lansford, WNG Chair, on this from university campus.

C: So if you're not aware of the pre-existing materials on this fingerprinting problem you should be able to google "taxonomy" because this is what a number of papers of on this topic published around 2016 were calling this issue.

Q: I think we have a bunch of information on these topics from before so maybe we should cross-reference.

**Straw poll #1**

Is the use of directed Probes from a STA a use-case this working group wishes to address?

Q: Are you trying to get with this strawpoll question to get people to stop using directed probe requests? Or figuring out some other way of doing it? Because we try to supply functionality also with these directed probes and then sometimes we have unintended consequences from that. But like, with a MAC address the original feature was to have one device know which other device it was talking to. However, it was also used for other purposes in the end and some people found that ok, and others found it very intrusive. I'm just trying to work out in which direction you're trying to lead with this straw poll.

A: Honestly, I don't want to set out too hard of a direction at this time. Maybe I'm looking for a way to make it more optional, or have a different baseline or default.

Q: I don't think this is exactly the question you want to ask in a strawpoll but I'm happy to take it with you offline for a proposal. I think the general direction is legitimate.

Q: I'm getting confused with... I can see us making additions to the standards, or making general recommendations, and I don't see why this should be done here rather than in TGbh. I thought bh was more operational, while this group was not?

Chair: I can answer that - bh addresses operational impacts of MAC randomization, but directed probes is not related to MAC randomization. So we can solve this with a standard amendments or a recommendation.

A: But that's a bit silly. The underlying problem is we're motivated by privacy requirements for both of the groups, and so maybe I'm just still not clear on what goes in which group. MAC randomization was also motivated by privacy requirements.

C: From my perspective, it's clear that bh targets the aspects of the spec that are being disrupted by the introduction of MAC randomization - how to ensure that features enabled by MAC can be preserved in a more privacy-friendly way. But bi has a more broad scope of privacy enhancements. With the existing strawpolls, I think it'd be helpful with a more concrete direction. Strawpolls shouldn't have to be crafted, tested, or word-smithed endlessly, they're just a general direction. But I don't understand the pushback to run these strawpolls, so I just think we should run the polls so that Kurt can go ahead and formulate a use-case that we can adopt.

C: I think we are having problem with blurring lines between bh and bi. I hope to address that in a future presentation. Also on the strawpolls I sort of agree there we can just run the polls. I just proposed to add other information elements to the poll question too so we aren't needlessly restricted later.

Q: Even if we solve the fingerprinting problem, isn't the privacy problem still there?

Chair: In the interest of time, I can put your strawpolls first on our agenda for the next meeting on September 8?

A: That sounds good. I'm happy for the good discussion. But also a general question: why are all these vendor specific data elements put into probe requests to begin with? But we can talk about it later.

1. AoB
	1. None
2. Chair adjourned the meeting at 10:01 ET.

**Attendance**

|  |  |
| --- | --- |
| **Name** | **Affiliation** |
| Andersdotter, Amelia | None - Self-funded |
| Ansley, Carol | Cox Communications Inc. |
| Derham, Thomas | Broadcom Corporation |
| Halasz, David | Morse Micro |
| Hawkes, Philip | Qualcomm Incorporated |
| Henry, Jerome | Cisco Systems, Inc. |
| Ho, Duncan | Qualcomm Incorporated |
| Huang, Po-Kai | Intel Corporation |
| Levy, Joseph | InterDigital |
| Lumbatis, Kurt | CommScope, Inc. |
| Luo, Chaoming | Beijing OPPO telecommunications corp., ltd. |
| McCann, Stephen | Huawei Technologies Co., Ltd |
| Montemurro, Michael | Huawei Technologies Co., Ltd |
| Ng, Boon Loong | Samsung Research America |
| RISON, Mark | Samsung Cambridge Solution Centre |
| Rosdahl, Jon | Qualcomm Technologies, Inc. |
| Shalom, Hai | Google |
| Smith, Graham | SRT Wireless |
| Yee, Peter | NSA-CSD |