IEEE P802.11
Wireless LANs

|  |
| --- |
|  TGbi Teleconference Minutes 8 December 2022 |
| Date: 2022-12-11 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Amelia Andersdotter | Sky Group/Comcast | Brussels, Belgium | +46764266862 | amelia.ieee@andersdotter.cc |

Abstract

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

8 December 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, Comcast**

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

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

Chair calls meeting to order at 10:04 ET.

Agenda slide deck: 11-22-2107r0:

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

1. **Discussion of agenda 11-22-2107r0 (slide #16)**
	1. Adoption of agenda 11-22-2107r0 slide #16 by unanimous consent (14 participants).
2. **Administrative**
	1. Two remaining teleconferences before the January Wireless interim (Dec 15, 9 AM ET; Jan 5, 9 AM ET).
3. **Technical presentations**
	1. **User-friendly WPA3 Passwords, 11-22-2106r0, Jeff Hansen (SoundVision Technologies)**

	WPA2-PSK had the ability to route users to the correct network based on password. SAE does not have this feature. Proposal entails introducing a password hash which allows the AP to place the user in the right network. It reduces user privacy with respect to the network.

	**Discussion:**

	**C:** Adding multiple SSIDs can increase airtime utilization as well, which would support this proposal. The privacy implications you've raised would apply for multiple SSIDs with or without this password proposal.
	**C:** Binding things to an SSID is probably a bad idea, but as you say other salts can be used.
	**Q:** Are you talking about 802.11 technologies or WPA3?
	**A:** I was thinking of introducing this in 802.11bi.
	**Q:** Can you clarify the difference between this and password identifier? If we include the password identifier in the hash but we don't know the password identifier?
	**A:** The intention with using the SSID was that it's anyway public information, so that would cause the network owner to divulge information of course. But a hash would hide the routing of users from third-parties.
	**C:** I think there is already a protected password identifier proposal going through .11me at this moment.
	**Q:** Is it the case that this hash is just a new version of a password identifier?
	**A:** Existing proposals don't have a way for the non-AP STA to divulge which password it's using.
	**C:** I'm also a bit confused on the difference between hash and password identifier. Maybe you can follow up with some more concrete comparisons between these proposals?
	**A:** I can follow up.
	**Q:** What is being separated? We have a single SSID and a single beacon, so will your guests be using the same GTK on the SSID? So a group-addressed frame will be shared with guests?
	**A:** Yes. You can also have different GTK.
	Q: But what is being separated?
	A: The features of the network would be separated based on password in this proposal, not on SSID.
	Q: Using this hash function, does the hash function have a key?
	A: It would just be a hash of the password, maybe the SSID and some salt. Straight up.
	Q: No keys?
	A: No, no keys.
	2. **Pre-association management frame protection, 11-22-1666r2, Okan Mutgan (Nokia)**Proposal is to use 802.11w features to introduce pre-association management frames. For STAs which return to the same ESS, a stored key can be used to apply the .11w mechanism. The stored key can change between returns. Keys are given an index which looks arbitrary to third-parties to reduce computational complexity for AP when relocating the returning STA.

	**Q:** This looks like a pseudorandom number generator. Doesn't that imply you need to synchronize the AP and STA? How will this be done?
	**A:** This is something we can decide.
	**Q:** What stops a STA from doing a DOS attack on the AP? How can the AP know that the STA is a genuine STA?
	**A:** Based on the MIC value. If the MIC value matches, the AP will know that comes from a legitimate STA.
	**Q:** I understood this is a returning STA?
	**A:** That is the case. Privacy issues mostly arise from returning STA, so STA which come back to the same AP.
	**Q:** How many indices do you need per STA to get a reasonable privacy guarantee? For instance, once a key is recovered, can you just stop transmitting the index and encrypt?
	**A:** If you have a non-index way of identifying the STA you do not need to transmit the index.
	**C:** I think you don't need to do the whole 4-way-handshake to get a key. We can have protected management frames also for the very first association.
	**C:** We don't need RSNA established the first time. We can use authentication frames to derive keys.
	**C:** This is already one of our requirements.
	**C:** The second index here should already be encrypted as part of the MAC payload if a key has been identified. So it is not sent in the clear, or does not need to be.
	**C:** Requirement 4 as far as I understand covers also the first association, and the initial authentication exchange. So this proposal would not entirely cover it, since a first association is needed in this proposal to establish indices and keys. Some modifications to this proposal may make it more compatible with this requirement.
4. **AoB**
	1. No other business.
5. Chair adjourned the meeting at 11:30 ET.

**Attendance**

|  |  |
| --- | --- |
| **Name** | **Affiliation** |
| Andersdotter, Amelia | Sky Group/Comcast |
| Ansley, Carol | Cox Communications |
| baron, stephane | Canon Research Centre France |
| Halasz, David | Morse Micro |
| Hansen, Jeff | SoundVision Technologies |
| Henry, Jerome | Cisco Systems, Inc. |
| Ho, Duncan | Qualcomm Incorporated |
| Huang, Po-Kai | Intel Corporation |
| Kain, Carl | USDOT; Noblis, Inc |
| McCann, Stephen | Huawei Technologies Co., Ltd |
| Mutgan, Okan | Nokia |
| Sam, Harvey | Broadcom Corporation |
| Sevin, Julien | Canon Research Centre France |
| Yang, Jay | Nokia |