IEEE P802.11
Wireless LANs

|  |
| --- |
| Minutes of the Random and Changing MAC address (RCM) Technical Interest Group (TIG) |
| Date: 2019-05-13 |
| Author(s): |
| Name | Company | Address | Phone | email |
| Stephen McCann | BlackBerry Ltd | The Pearce Building, West Street, Maidenhead, SL6 1RL, UK | +44 1753 667099 | stephen.mccann@ieee.org  |

Abstract

This document constitutes the minutes of the Random and Changing MAC address (RCM) Technical Interest Group (TIG) for the May 2019, Atlanta, Georgia, USA meeting.

**Monday May 13th 2019**

The chair: Amelia Andersdotter (Article19) opened the meeting at 16:01 Eastern Daylight Time (EDT)

1. **Meeting Guidance Slides** (slide #4)
	1. The chair read out the current IEEE meeting guidance slides and the IEEE 802 meeting participation was also read.
2. **Approve/modify agenda** (11-19-0623r2 slide #10)
	1. Comment (C): Please can I add a submission 11-19-0179r2 to the agenda.
	2. Chair: I’ve also noticed another submission 11-19-0884r0 that needs to be added to this agenda
	3. No objection to approving the agenda.
	4. Chair: Mark Hamilton has volunteered to be the TIG vice-chair, but he is not available today, therefore he cannot be appointed at the moment.
3. **Summary of RCM TIG formation** (11-19-0854r0)
	1. The chair presented a submission summarizing the background to why the TIG has been formed.
	2. C: I think this presentation is a little one sided. I think this TIG should also consider the lack of privacy protection. PKID, identity response frames and exposure of MAC address behind the portal. Therefore, the TIG scope should be larger.
	3. C: I agree with the previous comments. In addition, have we considered the impact on third parties (e.g. the network operator)?
4. **P802.1CQ MAC Address Assignment Requirements** (11-19-0851r0)
	1. This submission is a summary of the work in P802.1CQ.
	2. Question (Q): I hope that this is an optional requirement.
	3. Answer (A): yes, it is optional
	4. C: It is possible that the MAC address can change for every frame within 802.11. This therefore would not work with the P802.1CQ scheme. Perhaps a new MAC address mapping scheme needs to be introduced in the AP.
	5. C: So perhaps the 802.1CQ text should state that “the bridge assumes”
	6. Q: So, the 802.1CQ will only operate once a static identifier has been assigned.
	7. A: Yes, that is correct. This identifier has to be transmitted out of band.
	8. Q: In addition to human users, I think that infrastructure also needs to be protected using MAC addresses.
	9. A: Yes, I agree and so perhaps the scope of 802.1CQ should consider this.
5. **IDQuery Query Message Proposal** (11-19-0179r2)
	1. The submission is about a new action frame exchange to enable an AP to obtain a unique identifier from a STA for future use.
	2. Q: This scheme is asking the STA for a unique identifier.
	3. A: It’s not necessarily unique.
	4. Q: Ok, so that could be an issue.
	5. Q: Why doesn’t the AP create an identifier for the STA to use? This would seem to be a better scheme, as it maintains local scope.
	6. C: MAC address randomization after association is problematic. Probing randomization is ok.
	7. C: I think this submission needs to be updated. For example, I don’t know how to implement a globally unique identifier.
	8. C: For this protocol to be secure, how do you protected against man-in-the-middle and replay attacks.
	9. C: As this is post-association, those attacks should not be an issue.
	10. Q: Why do you trust the STA to provide a globally unique identifier? What happens if the STA lies?
	11. A: I think the AP would not be concerned about this.
	12. Q: Is there a connection between EAP and the STA identifier?
	13. A: I don’t think there is, as the authentication does that for you. This identifier is more for a transient use.
	14. Q: Is the same identifier required for all networks? Or is this an enumerated list of new identifiers?
	15. A: I’m not sure, as it’s difficult to determine how unique it has to be.
	16. Q: I’m more concerned about defining one identifier type.
	17. A: I’m not sure about that.
	18. Q: I think a globally unique MAC address is not a good example of this identifier. You remove client privacy by doing this. I think some derivative of this would be ok (e.g. a mix of the MAC address and the SSID).
	19. A: I did consider a hash at one point.
	20. Q: Is the authentication is strong, then this scheme is not necessary
	21. A: This is for the use case where the user does not login. The authentication is between the STA and the AP, but does not go to a AAA server.
	22. Q: I’m concerned about different users using the same service. Is their data separated?
	23. A: I’m not sure.
	24. Q: STAs should behave in the same way, so that STAs with different behavior are not tracked. Therefore, this scheme does not help these privacy issues.
6. **TIG goals** (11-19-0854r0 slides #14 - #16)
	1. Chair: It would be useful to summarize some real-life use cases and descriptions of this problem area. This is to determine if there is a real problem to solve.
	2. C: I would like to see use cases of situations when MAC address randomization is not used and the consequences of this. I think this is required to define the correct scope of the TIG’s work.
7. **Recess**
	1. Meeting recessed at 17:25 EDT.

**Thursday May 16th 2019**

The chair: Amelia Andersdotter (Article19) opened the meeting at 08:05 Eastern Daylight Time (EDT)

1. **Approve/modify agenda** (11-19-0623r3 slide #10)
	1. Chair: Please do your attendance
	2. No objection to approving the agenda.
2. **Temporary Addresses** (11-19-0884r0)
	1. This contribution provides background information on the use of temporary addresses in IEEE 802, IEEE 802.11, and other standards
	2. Q: How many of these protocols are actually deployed?
	3. A: All Bluetooth devices (BTLE) all use these features. Regarding the IETF protocols, I think CGA is used, but I’m not sure about the other ones.
	4. C: CGA is used, but is not extensively deployed.
	5. C: A temporary identifier in the station seems like a reasonable idea.
	6. C: Remember there are two uses cases, privacy of devices even against the AP, and then privacy just against 3rd parties. These are different. Therefore, the BTLE scheme would be useful. In addition, a scheme that is tied into a strong authentication protocol between the device and the AP would be useful.
	7. C: The BTLE receiver is supposed to maintain a table of local identifiers and real addresses. Therefore, the source address of transmitted packets can change. These can be static or highly random.
	8. C: So this would then require AP and device changes.
	9. C: On slide #24, RFC 7217 seems similar to some OS in devices, which implies that there are indeed some implementations of this.
	10. Q: So, does RFC 7217 uniquely identify a device.
	11. C: Yes, that is correct, but that design does not allow the network to identify a device.
	12. Chair: It would be nice to see a future presentation about various OS behaviors.
	13. C: Yes, I agree.
	14. C: In 3GPP, there is a project proposal for a unique permanent identifier that cannot be exposed. So, it seems to be a similar problem.
	15. Q: Is this SUCI?
	16. A: Not sure
3. **Vice chair** (11-19-0854r0 slides #14 - #16)
	1. Chair: I would like to appoint Mark Hamilton as the RCM TIG vice-chair.
4. **TIG goals** (11-19-0854r0 slides #14 - #16)
	1. Chair: I will arrange 2 slots of the July meeting (Vienna) and no teleconferences.
	2. Regarding the TIG goals, it would be useful to consider the creation of a TIG report in the future.
5. **Adjourn**
	1. Meeting adjourned at 09:01 EDT.