IEEE P802.11
Wireless LANs

|  |
| --- |
| Minutes for RCM TIG - July 2019 - Vienna |
| Date: 2019-07-19 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Mark Hamilton | Ruckus/CommScope | 350 W. Java DrSunnyvale, CA 94089 | +1-303-818-8472 | mark.hamilton@commscope.com |

Abstract

Minutes for the RCM TIG meetings held during the July 2019 802 Wireless Interim Session

1. **RCM TIG – F2F, Wednesday 17 July 2019, 13:30- 15:30**
	1. **Call to Order** at 13:31 by the TIG Chair, Amelia ANDERSDOTTER (ARTICLE19)
	2. **Review Participation slide**:
		1. Agenda deck: slide 4
	3. **Review Information slides**
		1. Resource URLs
		2. Meeting Etiquette
	4. **Attendance reminder**
	5. **Review Agenda** – 11-19/0982r4
		1. <https://mentor.ieee.org/802.11/dcn/19/11-19-0982-04-0rcm-rcm-tig-july-2019-meeting-agenda.pptx>
		2. Announcement that the Chair will attend the Privacy-Enhancing Technologies Symposium on July 19 in Stockholm. See <https://petsymposium.org/2019/hotpets.php> for more information.
		3. **Agenda items for the week**
			* + Call the meeting to order
				+ Elect/call for secretary for the meeting
				+ Reminders of guidelines, policies, attendance.
				+ Agenda review
				+ Summary of May meeting.
				+ Timeline
				+ Presentations

11-19/1320r0, Assignment of Temporary Addresses, Roger Marks (EthAirNet Associates)

11-19/1314r1, Privacy protection in Wi-Fi analytics systems, Mathieu Cunche (Univ. Lyon, INSA Lyon, Inria, CITI)

11-19/1313r1, Pitfalls with address randomization, Mathieu Cunche (Univ. Lyon, INSA Lyon, Inria, CITI)

11-19/1027r0, Do Not Fear Random MAC Addresses!, Dan Harkins (HPE)

* + - * + Teleconferences
				+ AOB
				+ Adjourn.
		1. One more presentation expected (Carol ANSLEY, CommScope)
		2. 11-19/1027 is now an r1.
		3. No objection to proposed agenda, with those changes.
	1. **Summary of May meeting** (agenda deck, slide 13)
		1. Stuff
	2. **Timeline discussion**
		1. Chair’s proposal:
			1. May 2019: Fact-finding
			2. July 2019: Further fact-finding, conclusion
			3. August 2019: Draft report (to allow for comments/reaction forming in good time ahead of September F2F)
			4. September 2019: Discussion on draft report
			5. November 2019: Conclusion
		2. However, we should consider this after we’ve heard the presentations, and have a better idea of how the timeline will work out. Postponed this discussion until after presentations (tomorrow’s meeting).
	3. **Document 11-19/1320r0 –** Roger MARKS (EthAirNet Associates):
		1. <https://mentor.ieee.org/802.11/dcn/19/11-19-1320-00-0rcm-assignment-of-temporary-addresses.pptx>
		2. This presents views on the assignment of temporary addresses in 802.11.
		3. Overview of IEEE 802 (including 802c amendment). Information about 802.1CQ project. Overview of how 802 addressing works, implications on privacy, support for authentication, etc.
		4. Graphic “squares” to visualize local address assignment methods, and examples.
		5. Comment: Noted that mechanisms that do address assignment (from a server, for example), needs to be careful to not expose a client identifier in the process.
		6. Slide 10: Using the MAC address to communicate information about the device, is exposing that information to third-parties, with a clear need.
		7. Because all the MAC header addresses are in the clear, on 802.11, also addresses 3 or 4 are being exposed. 802.11 should consider if this is a concern.
		8. Should 802.11 try to address these kinds of addressing schemes, or is that a broader 802 problem to solve? A: 802.1CQ is creating a framework for such discussions, and could discuss this.
		9. When is 802.1CQ planned to finish? A: Plan is to start TG balloting this November. 802.1CQ is meeting in the 802.1 TSN slot today, PM2.
	4. **Document 11-19/1314r1 –** Mathieu CUNCHE (Univ. of Lyon, Inria):
		1. <https://mentor.ieee.org/802.11/dcn/19/11-19-1314-01-0rcm-privacy-protection-in-wi-fi-analytics-systems.pptx>
		2. Presents privacy concerns with wireless networks.
		3. Attacker can defeat MAC address randomization, by tracking packets with other content, such as UUID, tracking changing fields, or fingerprinting the packets (with content or timing).
		4. Also active attacks, such as Karma AP, RTS exploit.
		5. Consider countermeasures for all these attack vectors. Specification of these can help – don’t give vendors too much freedom to make mistakes.
		6. Comment: Device vendors are already starting to do the countermeasures, but it is sporadic so far.
		7. 802.11aq also addressed some of these concerns, where within the 802.11 scope.
		8. Maybe consider a new annex in 802.11 with guidelines for these items, where outside 80211 scope, or beyond a requirement we could create.
		9. Different kinds of privacy to consider – third-party ‘snooping’ as well as privacy from the network or components on it (like DHCP servers).
	5. **Document 11-19/1313r1 -** Mathieu CUNCHE (Univ. of Lyon, Inria):
		1. <https://mentor.ieee.org/802.11/dcn/19/11-19-1313-01-0rcm-pitfalls-with-address-randomization.pptx>
		2. Principles for privacy protection.
		3. Wombat, experimental Wi-Fi tracking system. Used as an experiment on user opt-in/opt-out, in Paris.
		4. Also need to protect stored information about users, with anonymizing/hiding methods.
		5. Comment: Doesn’t have any trust relationship with the opt-in/opt-out system, already break the privacy it is supposed to protect?
		6. Some (many?) users will never trust anyone that doing tracking, and would never opt-in.
		7. TGaz has added mechanisms to opt-out, too.
	6. **Document: 11-19/1027r1** – Dan HARKINS (HPE):
		1. <https://mentor.ieee.org/802.11/dcn/19/11-19-1027-01-0rcm-do-not-fear-random-macs.pptx>
		2. Presents motivations for MAC randomization. Considerations of concepts being discussed: how many bits of randomization (802c SLAP), etc.
		3. Comment: The points in the WBA liaison are (or can be) good to help shine light on issues that have always been present but were (more) ignorable until MAC randomization exacerbated them.
	7. **Group members need to consider our scope. How much to we consider privacy issues in general, versus just effects of MAC randomization?**
	8. **Reconvene tomorrow in AM1.**
	9. **Recessed 15:28 pm**
1. **RCM TIG – F2F, Thursday 18 July 2019, 8:00 - 10:00**
	1. **Call to Order** at 8:01 by the TIG Chair, Amelia ANDERSDOTTER (ARTICLE19)
	2. **Review Participation slide**:
		1. Agenda deck: slide 4
	3. **Review Information slides**
		1. Resource URLs
		2. Meeting Etiquette
	4. **Attendance reminder**
	5. **Review Agenda** – 11-19/0982r5
		1. <https://mentor.ieee.org/802.11/dcn/19/11-19-0982-05-0rcm-rcm-tig-july-2019-meeting-agenda.pptx>
		2. **Agenda items for the week** (note moved Timeline to near the end)
			* + Call the meeting to order
				+ Elect/call for secretary for the meeting
				+ Reminders of guidelines, policies, attendance.
				+ Agenda review
				+ Summary of May meeting.
				+ Presentations

11-19/1320r0, Assignment of Temporary Addresses, Roger Marks (EthAirNet Associates)

11-19/1314r1, Privacy protection in Wi-Fi analytics systems, Mathieu Cunche (Univ. Lyon, INSA Lyon, Inria, CITI)

11-19/1313r1, Pitfalls with address randomization, Mathieu Cunche (Univ. Lyon, INSA Lyon, Inria, CITI)

11-19/1027r0, Do Not Fear Random MAC Addresses!, Dan Harkins (HPE)

11-19/179r3, IDQuery Query Message Proposal, Carol Ansley (Commscope)

11-19/496r1, ID\_Query\_Proposal, Carol Ansley (Commscope)

* + - * + Timeline
				+ Teleconferences
				+ AOB
				+ Adjourn.
	1. **Document 11-19/179r3 –** Carol ANSLEY (CommScope):
		1. <https://mentor.ieee.org/802.11/dcn/19/11-19-0179-03-0arc-idquery-query-message-proposal.pptx>
		2. Provides a way for a device to provide a (presumably unique), stable and secured (against third-party eavesdropping) identifier.
		3. Since last time, added an Extended Capability bit to indicate the non-AP STA’s support for this feature.
		4. Should the STA just send this information (unsolicited) instead of being queried by the AP? It is costing a bit in every Beacon, due to being a capability bit. Instead the non-AP STA could provide this in a KDE in the fourth EAP frame, for example. Or, could still be an Action frame, but unsolicited.
		5. Since this is an unstructured ID, how is it really used? A: The utility is just the ability to track the device in the ESS, so even an ID that isn’t understood is helpful. If the client wants additional value (like returning to a known hotel), it can arrange to use an understood ID. But, this is being solved by vendors already, outside the 802.11 scope.
		6. What are you doing to keep privacy? A: The message will be encrypted. But, the variable length of the information could be uniquely identifying – may need to have a fixed length for all devices.
		7. Is there a way for the AP to tell the client that this is the “same network” so the client knows to reply with the same ID as last time it visited? A: Since the AP asked for the information, the client can decide, whether to provide the response to this AP, and what ID to provide. Could add policy information coming from the AP to give the client more guidance on how to do this.
		8. This needs to be done only over an authenticated association. But, things like Captive Portals don’t provide that.
		9. How about having the AP provide a token to the client, that the client then provides on future contacts? Something like a “token” on web sites, or maybe more like a “cookie” on a web site.
		10. We need to clarify the use cases for this, to be able to evaluate the alternative solutions.
		11. Consider the use cases the WBA threw out in their liaison to us. ARC has been through that, already. ARC Chair: But, ARC was looking at which of those concerns was a problem for an 802.11 facility, that we felt we (WG11) should consider solving. This proposal is providing a tool that might solve other problems on that list.
	2. **Document 11-19/496r1 –** Carol ANSLEY (CommScope):
		1. <https://mentor.ieee.org/802.11/dcn/19/11-19-0496-01-000m-id-query-proposal.docx>
		2. Not considered. This is detailed spec changes, that a potential project/TG could consider, but it is out of scope of the TIG to consider specific spec changes.
	3. **Timeline (and scope)**
		1. Considered 11-19/588r2 (<https://mentor.ieee.org/802.11/dcn/19/11-19-0588-02-0rcm-summary-of-discussions-on-randomized-and-changing-mac-addresses-2014-2019.odt> )
			1. There are three use cases that ARC identified.
		2. Consider privacy issues and concerns – add that to our scope? Some concern about how broad this could become. Suggestion that we comment in our report that there is a high degree of interest in privacy concerns, and that WG11 should consider forming an appropriate group to discuss it.
		3. We might want to consider how much privacy randomized/changing MAC addresses are really providing. That topic could be considered to be in our scope.
		4. There is a balance between privacy and some of these user experience desires.
		5. Different implementations are doing randomized MAC addresses differently, resulting in different privacy or user experience results.
		6. Need to be careful to consider the threat model(s) that we’re trying to solve, as we discuss these.
		7. The variety of implementations of random/changing MAC addresses seems to be a reason in itself to say in our report that we think WG11 needs to look at this, and discuss guidance, at least, for implementations.
		8. Chair: Thought was to produce draft report material by August 2019. The group could work on this, and alert the broader WG11 membership that it will be discussed in September. Goal is to have this outline level available approximately two weeks before the September F2F, to give others time to prepare.
		9. We likely need more than 2 slots in September, for that drafting and review.
	4. **Teleconferences and future meeting planning**
		1. Chair: Concern about the effectiveness of teleconferences for material this is “charged”; face to face discussion is better. Suggest no teleconferences. Instead, have a call for contributions for text, available 1-2 weeks ahead of the September meeting, so everyone can come prepared to make quick progress during the F2F.
		2. Discussion: We’ll need at least 3 slots in September for this.
		3. Do we need to assign topics/sections to individuals? If we keep a “less is more” philosophy, we’ll reach consensus on next steps more quickly, and can be more organic.
		4. We can recommend (to the WG):
			1. Do nothing further
			2. Start one or more new TIGs (on a broader privacy topic, for example)
			3. Start a Study Group to lead to a Task Group for specific changes to the Standard.
		5. Agreed to no teleconferences, and 3 slots in September F2F. Goals for September are to produce a first draft of the report. A first draft/outline in August, will be produced by the leadership, as a starting point. Request specific submissions, to be provided at least 1 week ahead of the meting to flesh out the text, and to be reviewed by everyone ahead of the meeting, for discussion during the F2F.
		6. Chair will send a call for presentations to the email reflector, with a specific deadline that is sufficiently ahead of the September F2F.
	5. **Adjourned at 9:45am**

**References:**

1. <https://mentor.ieee.org/802.11/dcn/19/11-19-0982-04-0rcm-rcm-tig-july-2019-meeting-agenda.pptx>
2. <https://petsymposium.org/2019/hotpets.php>
3. <https://mentor.ieee.org/802.11/dcn/19/11-19-1320-00-0rcm-assignment-of-temporary-addresses.pptx>
4. <https://mentor.ieee.org/802.11/dcn/19/11-19-1314-01-0rcm-privacy-protection-in-wi-fi-analytics-systems.pptx>
5. <https://mentor.ieee.org/802.11/dcn/19/11-19-1313-01-0rcm-pitfalls-with-address-randomization.pptx>
6. <https://mentor.ieee.org/802.11/dcn/19/11-19-1027-01-0rcm-do-not-fear-random-macs.pptx>
7. <https://mentor.ieee.org/802.11/dcn/19/11-19-0982-05-0rcm-rcm-tig-july-2019-meeting-agenda.pptx>
8. <https://mentor.ieee.org/802.11/dcn/19/11-19-0179-03-0arc-idquery-query-message-proposal.pptx>
9. <https://mentor.ieee.org/802.11/dcn/19/11-19-0496-01-000m-id-query-proposal.docx>
10. <https://mentor.ieee.org/802.11/dcn/19/11-19-0588-02-0rcm-summary-of-discussions-on-randomized-and-changing-mac-addresses-2014-2019.odt>