IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| RCM Ad Hoc January 2020 Meeting Minutes | | | | |
| Date: 2020-01-16 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Graham Smith | SRT Wireless | Sunrise, FL |  | gsmith@wi-ficonsulting.org |
|  |  |  |  |  |

Abstract

Minutes from the RCM Ad hoc meeting held during the 802.11 WLAN Working Group Session on Jan 14, 2020 in Irvine.

Note: in this document:

Q – proceeds discussion questions,

C – proceeds comments,

A – proceeds answers/replies (in response to a question or comment),

and

Chair - proceeds action or statements by the Ad Hoc Chair.

**RCM Ad-Hoc Meeting - MINUTES**

Acting Chair (“Chair”) – Mark Hamilton (Ruckus, Commscope)

Acting Secretary – Graham Smith (SR Technologies)

**Tuesday, January 14, EVE**

Chair opened meeting at 19.28 pm (19 in room)

Chair introduced topics and agenda using slides 20/0004r1

Chair went through slides 7,8 of 20/0004r1Paritcicpation and Guidelines

Chair went through slide 10 of 20/0004r1

Agenda

* Administrative
  + Review Scope and Goals
  + Presentations/discussion
  + Propose direction for next steps
  + Off-line homework:
    - Editing of recommendation
    - Logistics prep

Note: Presentation in Wednesday mid-week plenary on report and findings of RCM TIG

Thursday, January 16, AM1

* + Formulate recommendation to WG
  + AOB

Need to identify a Chair for a possible SG

**Scope and Goals**

Chair gave a background RCM (Randomized MAC)

TIG produced a report

Chair went through slides 11 and 12 of 20/0004

* **RCM TIG recommended (see report):**
  + Future work within 802.11 “on issues directly affecting the operation of MAC and PHY” due to random/changing MAC addresses. Such as:
    - Use case on Initial Infrastructure Connection Steering (section 3.1)
    - Use case on Customer Support and Troubleshooting (section 3.9)
  + Might result in amendment to 802.11.
  + Also, might consider other use cases in support of 802.11’s users, perhaps facilitated by the above work, or perhaps needs a Recommended Practice (annex?).
  + Do not compromise levels of privacy protection.
  + Consider a Study Group
* **RCM TIG also recommended (see report):**
  + 802.11 WG consider examining a broader range of privacy issues relating to 802.11 networks.
  + Out of scope of RCM
  + Happy to discuss/work with volunteers to progress this, off-line (another TIG, etc.)

Chair noted that this would require a different TIG)

Q – Is Amelia not participating?  
Chair – For the present she is not attending.

* **Goal for this ad hoc:**
* Recommend to the WG: next steps on issues due to random/changing MAC addresses, as Study Group or work within an existing TG.
* Begin logistics (identify a Chair, etc.) for the work

Chair noted that another path could be to give this task to another existing TG.

Background documents listed on Slide 13 of 20/0004.

Note that interest started with a WBA Liaison on MAC randomization impacts

Any comments or thoughts:

Q – Any interpretation of possible amendments? Might be on how randomization is done tby STAs, or protocol? What’s in scope?

Chair – Up to us to decide what is in scope. If we tried to write how to do randomization may be out of scope but a recommended practice may be OK. Minor tweeks to protocol to help solve the issues?

Q – Goals worded that we agree with them?

Chair – Proposed goals for discussion.

Q – Can’t split tasks rules and guidance, need to keep privacy requirements and might need other tools. If we do something, it could be a scope that may include both of those.

Chair – Proposing to split them just for timing reasons. Randomization is happening and need to fix problems that are happening. Not fixing privacy.

C – What’s broken is use cases that are not defined in .11. Nothing is broken in our Std.

C – 802.e group looked at privacy and reviewing 802.11. Issue of MAC address not so much it breaks Std. it was assumptions that MAC identifies the STA. Also unclear in Std. in many places when MAC is a STA ID.

C – Nothing broken but do use “beyond scope of Std”. Difficult to blame implementers when nothing specified. Using MAC as identifier, Std almost pushes this. Can’t ignore and unfair to blame them.

C – Possibility to continue work. We are debating again what’s in report. If higher layer needs an identifier. Nervous we re-write the report. Searching for mandate, is it privacy or identifier? We need to decide, is there a way to decide if we do have a problem to solve.

Chair – Report did pick up the topics that we could tackle. We need to decide if within scope. Also I have a presentation that might help and guide discussions.

C – need to decide the burning desire of action, and if so let’s do it. Not seeing a mandate of action but we have a catalog of issues.

Chair – What would a mandate look like? These issues are impacting now and companies looking for help in solving them. Recommended practices might be helpful plus possible hook in the protocol might help.

C – Don’t fear too much, no real stupid implementations.

C – Mandate or not, if possible to compromise privacy won’t be implemented. Useful to have some guidance and if that is direction might see value.

C – Prescribing a solutions perspective if it maintains privacy that is OK. History of optional ways, hence a responsibility to prescribe a solution.

C – Both sides need to decide and benefit. MAC addresses assumed they would be used forever but re-writing this may not get us far. Love interoperability when we can do it.

Q – Any work on TIG in categorizing tracking privacy?

Chair – No, did have discussion. Some use cases touch on those topics.

C – If we want to do work, need to look at what is acceptable for privacy point of view.

Chair – cannot compromise privacy.

Chair displayed 20/0120 RCM Summary and way Forward.

Background and Summary.

TIG findings:

* 11 example use cases (see next slide) were identified, where RCM could have impacts on existing systems.
* Many of the impacts from RCM are on “upper-layer” protocols and systems, arguably beyond the 802.11 (or 802) scope. A liaison was sent to WBA (from ARC, prior to RCM TIG) outlining these concerns: (11-18/1988).
* Remedial methods to mitigate the impacts of RCM were identified and reviewed.
* Recommendations (summarized):
  + Future work is needed in 802.11, resulting in an amendment to the Standard implementing some of the mitigation strategies that are within 802.11 scope.
  + There is also clear demand for broader work on privacy issues relating to 802.11 technologies, that could be explored by a more broadly scoped TIG.

Chair went through the Use Cases, Slide 5 of 20/0120. Describing each one.

Use Cases:

1. Initial infrastructure network connection steering
2. Access control and arrival detection in a home environment
3. Airport security queue measurement
4. Grocery store customer flow analysis
5. Grocery store frequent shopper notifications
6. Infrastructure (home or enterprise) with different SSIDs per band
7. Infrastructure (home or enterprise): probes use RCM, even with associated SSID
8. Rogue detection in infrastructure networks
9. Customer support and troubleshooting
10. Residential wireless gateway with Hotspot
11. Pervasive surveillance

C – Trust my home but not the grocery store. Fingerprinting methods may be used to overcome problems, may then get fixed as they are a privacy concern in themselves.

C – Need a motivating factor to show advantage for user.

C – Was Captive Portal considered?

Chair – Not seen as a .11, but yes.

C – Anything that suggest client’s implementers would be interested would be of consideration. Use cases 3, 4 and 5 client has no benefit.

Chair – but 4 could be that store puts things together so you don’t walk so far. (some derision at this), but #5 I would like to work. Don’t actually connect to the grocery network.

Chair then produced Slides which represents Chair’s personal opinion.

Proposed Plan Slide 6, 20/0120.

**The RCM ad hoc met Tuesday EVE, and proposes the following ways forward:**

* **Develop amendment text on issues directly affecting the operation of MAC and PHY due to random/changing MAC addresses. Such as:**
  + Use case on Initial Infrastructure Connection Steering (section 3.1)
  + Use case on Customer Support and Troubleshooting (section 3.9)
* **This might include**
  + Recommendations on MAC address change timing?
  + Recommendations on SSID assignments (not per-band)?
  + Other recommendations?
    - Alternative identifier(s) for device identification by trusted networks?
    - Other alternative ways to support steering, surveillance, queue/flow analysis, etc.?
    - Other standardized methods, perhaps to help facilitate other use cases beyond 802.11 scope?
* **Potential venue:**
  + Study Group?
  + “Assignment” for an existing TG? (REVmd?)
* **Separately, form a new TIG for broader work on privacy issues relating to 802.11**

Chair - Recommended practices could be in an Annex.

Q – Not included recommendations on how to select MAC address, which segment of address space do we select the MAC?

Chair – Not sure if that solves anything we consider broke.

Q – “Alternative ways”, do we intend to solve them?

Chair – All work to be done with one eye on don’t break privacy.

C – Not our job to decide if surveillance is a problem, we don’t know the reasons why. If you need to track devices for any reason we may simply find a recommendation on how to do it. Not our problem if privacy broken.

C – We must not add means for surveillance to be made easier without agreement that they want to be tracked.

C – If tracking using MAC addresses remains to be needed then maybe we do need to add alternative.

C – Tracking children?

Chair – Do we have any agreement? Need to come into our one more slot with some agreement and some direction. Can we agree on the first 2?

C – If a client uses RCM then we could provide means to improve situation that arises. A mechanism may provide the benefits identified as broken.

**Discussions and Changes to text of slide 6** .

Ended up with

* *In environments where non-AP STAs use random changing MAC addresses, develop text to improve the STA’s user experience for use cases such as:* 
  + Use case on Initial Infrastructure Connection Steering
  + Use case on Customer Support and Troubleshooting
  + Arrival detection in a home environment, or other trusted environment
* **This might include recommendations and/or normative text**
* **Potential venue:**
  + Study Group?
  + “Assignment” for an existing TG? (REVmd?)

**Straw Poll**: Do you agree to present slides, as amended during this meeting, to the mid-week plenary.

Result: 19,0,0

**Recessed at 9.32pm**

**Thursday AM1**

Chair – Mark Hamilton (Ruckus, Commscope)

Acting Secretary – Graham Smith (SR Technologies)

Chair opened meeting at 8.05 am (9 in room)

Chair went through slides 7,8 of 20/0004r1 Paritcicpation and Guidelines

Agenda

* Formulate recommendation to WG
* AOB

Agenda accepted with no objection.

Doc 29/0120r1 then introduced. This was worked on at the first session on Tuesday.

Chair went through the Background and Way Forward, side 6 as amended at first meeting.

Options are SG or incorporate into an existing TG such as Revmd. Assumption is that the SG route is assumed.

C – SG writes PAR, should we look at another TIG? First one did Use Cases, maybe look at solutions for those selected?

Chair – That can be done in a TG.

C - not sure we are agreed that text for the Std is where we are going

Chair – The agreement was that we do want to write text, maybe an Annex.

C – Fix issues and we have gone thru presentations, understanding that smallnumber of technical changes that may be useful. If MD was not in such a late stage would have preferred that route. Don’t need more study, think it is clear bu do need to study more on privacy side. So form a new group to continue work, small technical changes and study more on privacy side. So Slide 6 need to form “a group” (not a SG?).

C – not a SG as that writes PAR. SG TG route is slow.

C – Basically agree, but concerned with timing. Not sure last minute technical changes may have objections and ME is 5 years away. If just these 3 things, small amendment should not take long (12- 24 months). Don’t see any other way other than SG/TG. Look at SENS, SG for 1 meeting.

C – If in ME still WFA could have it almost straightaway.

C – Agree SG/TG can be fast.

C – Mdis preferred but with MD where it is, get a tightly focused SG/TG. If not going anywhere stop and dissolve.

C – Afraid that it culd grow. So it should be SG/TG

Chair – If SG form in March, Sept to do PAR, can still do work, TG Sept. Say 11 month from Sept.

C – Having a vehicle with ability to draft text is needed as TIG cannot draft text.

Results of discussion

TG

* March 2020 Creation of RCM SG
* Sept 2020 RCM TG
* Sept 2020 D1.0
* Earliest amendment - Sept 2021?

TIG

* March 2020
* Through July? – discussion that leads to text proposals
* Actual text (from individuals) goes to other TGs

C – Prefer TG approach. Already identified layer 2 identifier required. Not sure TIG could do as proposed. Could they?

A – Idea would be individuals from theTIG would take to other TGs.

Chair – Does anyone think TIG that individuals would have text by July?

A – We do have proposal “ID Query”. Taken to other groups but no real interest as RCM TIG started.

C – Skeptical of TIG approach is that no-one takes responsibility i.e. a clear mandate is missing.

C – Delays to agreeing to any proposals have not been agreed to maybe because RCM was formed and hence used as an excuse. Danger of repeating that.

Chair – If we go SG path, now an individual taking anything to MD would be refused because it would be referenced back to the RCM SG/TG.

C – If we do nothing today then the process is SG or fold. TIG would be a talking shop. If we fold then at least individuals are free to introduce into other TGs.

Chair – Straw Poll is in order.

Straw Poll (Chicago rules).

1. SG/TG
2. TIG
3. Stop
4. Abstain

Discussion

C – Privacy issues as well?

C – Fix places where 802.11 should take action, but privacy should be separate.

Chair – TIG approach allows individuals to take text anywhere.

C – PAR can say what you want.

C – SG can pursue what it wants, and the narrow scope would not have enough interest.

C – PAR is a project to produce a document, no such thing as “group”. Other TGs will group many projects and if in RCM with 2 projects one TG that is OK.

C – Might need 2 PARS because one is quick and the other will take longer. Not sure if ever done in .11 but certainly done in other 802 TGs.

Chair – SG/TG takes time, can create a TG directly (WG Chair can do that), can be chartered with 2 projects, or if TG exists can start with the quick stuff.

Q – Are we sure what the quick stuff it?

Chair – we do have a short list of 3 cases plus one technical solution ready to go.

Q – Can a TG form another PAR. We have the quick stuff in PAR one, do that then form a second PAR. Can you work on two PARs at same time?

A – Can work on 2 PARS at same time but need 2 documents.

C – PAR could specify that text is confined to being in an Annex. Then easy to separate.

C – Does not make sense to confine to an Annex.

C – Like idea of 2 PARs, at least can say big plan with long and short term issues.

C – Focus on what is on table, establish PAR, develop it. At beginning of privacy issues. Propose a SG for PAR for narrow scope.

C – Significant risk that privacy side would not proceed.

C – Not convinced that narrow scope has legs.

Chair – RCM TIG proposal was SG/TG and a TIG for the privacy.

Straw Poll

1. SG/TG (1 PAR quick fixes only)
2. SG/TG (privacy only, individuals for quick fixes)
3. SG/TG (2 PAR)
4. Just a TIG
5. Two Groups SG/TG plus TIG
6. Stop (let individuals)
7. Abstain

15 persons in room.

5/1/10/5/10/5/1

C and E discussion?

Chair – Not much difference in the two, as will cause problems as to where does a subject practically fall.

Q – Can we have TG with 2 PARS?

Chair – Not in .11 but certainly in other 802. TGm has had 2 PARs, maintenance and revision. Dot 1 does it all the time.

C - SG’s are given definite instructions. SG could decide if 1 or 2 PARs.

C – Develop Par for this and Par for that, or develop 2 PARs?

Chair worked on Slide for Motion to create RCM Study Group, within document 20/0192r1

Final version:

“Approve the formation of the 802.11 Randomized and Changing MAC addresses (RCM) Study Group to develop 2 Project Authorization Request (PAR) and Criteria for Standards Development (CSD) for 2 projects to:

1. Develop an amendment into IEEE Std 802.11 with modifications, feature additions, or recommendations, to improve the STA’s user experience in environments where non-AP STAs use random/changing MAC addresses. To consider use cases such as (but not limited to):
   * Initial Infrastructure Connection Steering
   * Customer Support and Troubleshooting
   * Arrival detection in a home environment, or other trusted environment

* This might include informative (recommendations) and/or normative text
* This must not compromise current levels of privacy protection afforded by the IEEE 802.11 standard or best understanding of current practices in RCM implementations

1. Develop an amendment into IEEE Std 802.11 with modifications, feature additions, or recommendations, to improve user privacy. This includes a review of IEEE P802E and its implications on IEEE Std 802.11”

Chair went through editing the slides of 20/0192r0 (to be posted as r1) “RCM Study Group Creation”, editing along with comments from the floor.

Slide 2, RCM TIG recommendations

Slide 3, RCM ad hoc recommendations

Slide 4, Motion

Straw Poll: Agree to this deck as the recommendation from the RCM ad hoc to the 802.11 WG?

Agree 13

Not Agree 0

Abstain 1

AOB?

Meeting adjoined at 10am.