IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Telecon Minutes for REVmd CRC-March 20 2020 | | | | |
| Date: 2020-03-20 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Jon Rosdahl | Qualcomm Technologies, Inc. | 10871 N 5750 W  Highland, UT 84003 | +1-801-492-4023 | jrosdahl @ ieee.org |
|  |  |  |  |  |

Abstract

Minutes for the 802.11md – REVmd CRC Teleconference held March 20,2020.

R0: March 20th Telecon Minutes

1. **IEEE 802.11md REVmd CRC Telecon Friday March 20, 2020 10:00-12:00 ET**
   1. **Called to order at 10:06am** ET by the TG Chair Dorothy STANLEY
   2. **Attendance:**
      1. Dorothy STANLEY (HPE)
      2. Jon ROSDAHL (Qualcomm)
      3. Dan Harkins (HPE)
      4. Mark RISON (Samsung)
      5. Dennis SUNDMAN (Erricson)
      6. Edward AU (Hauwaei)
      7. Emily QI (Intel)
      8. Gabor BAJKO (Mediatek)
      9. Rojan CHITRAKAR (Panasonic)
      10. Micahel MONTEMURRO (Blackberry)
      11. Graham SMITH (SR Technologies)
      12. Stephen MCCAAN (Blackberry)
      13. Menzo WENTINK (Qualcomm)
      14. Mark HAMILTON (Ruckus/CommScope)
      15. Jouni MALINEN (Qualcomm)
      16. Jonathan GOLDBERG (IEEE-SA)
   3. **Review Patent Policy**
      1. No Objections
   4. **Review Participation Slides**
   5. **Review Agenda – 11-20/0234r17:**
      1. <https://mentor.ieee.org/802.11/dcn/20/11-20-0234-17-000m-2020-jan-mar-teleconference-and-adhoc-agendas.docx>
      2. Today’s Specific Agenda:

g. 2020-03-20 Friday 10 am Eastern 2 hours \*\*\*\*\*Teleconference announced with 10-day notice\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* (London is +4)

1. Prepared MOTIONS

i. Motion 170: PHY CIDs

a. Approve comment resolutions included in the “PHY Motion C” tab in 11-20/0145r6 <<https://mentor.ieee.org/802.11/dcn/20/11-20-0145-06-000m-sb1-revmd-phy-sec-comments.xlsx>>

ii. Motion 17x: GEN CIDs

a. Approve comments included in the “Motion Feb AdHoc” tab in 11-20/0147r4 <<https://mentor.ieee.org/802.11/dcn/20/11-20-0147-04-000m-sb1-revmd-gen-comments.xls>>

iii. Motion 17x: Editor CIDs

a. Approve comments included in the “Motion-EDITOR-T” tab in 11-20/0010r6 <<https://mentor.ieee.org/802.11/dcn/20/11-20-0010-06-000m-revmd-sa1-comments-for-editor-ad-hoc.xls>> , except CID 4800

iv. Motion 17x: Editor CID 4800

a. Approve the resolution to CID 4800 included in the “Motion-EDITOR-T” tab in 11-20/0010r6 <<https://mentor.ieee.org/802.11/dcn/20/11-20-0010-06-000m-revmd-sa1-comments-for-editor-ad-hoc.xls>>

v. Motion 17x: Editor2 CIDs

a. Approve comment resolutions included in “Motion-EDITOR2-O” and "Motion-EDITOR2-P" in 11-19/2160r7 <<https://mentor.ieee.org/802.11/dcn/19/11-19-2160-07-000m-revmd-editor2-standards-association-ballot-comments.xlsx>>

vi. Motion 17x: MAC CIDs

a. Approve comments included in the "Motion MAC-AM" tab in: 11-17-0927r57 <<https://mentor.ieee.org/802.11/dcn/17/11-17-0927-57-000m-revmd-mac-comments.xls>>

2. Comment resolution

a. Rojan CHITRAKAR – GCMP/CCMP CIDs doc 11-20/407r1 <<https://mentor.ieee.org/802.11/dcn/20/11-20-0407-01-000m-resolutions-for-some-ccmp-gcmp-cids.docx>>

b. Michael MONTEMURRO – 11-10/2024r4 <<https://mentor.ieee.org/802.11/dcn/19/11-19-2024-04-000m-mac-address-change.docx>>

c. Jon ROSDAHL – GEN CIDs

d. Mark RISON - CIDs

* + 1. Replace Michael Montemurro presentation with Dan Harkins
    2. No objection to proceed with **11-20/0234r18**
       1. <https://mentor.ieee.org/802.11/dcn/20/11-20-0234-18-000m-2020-jan-mar-teleconference-and-adhoc-agendas.docx>
  1. **Editor Report** - Emily QI (Intel)
     1. We now have d3.2 available in members area.
     2. Redline, word and pdf version posted.
     3. Potential item identified during the d3.2 review
     4. A submission will need to be prepared to fix the new items identified.
  2. **MOTIONS**
     1. **Motion 170: PHY CIDs** 
        1. Approve comment resolutions included in the “PHY Motion C” tab in 11-20/0145r7: <<https://mentor.ieee.org/802.11/dcn/20/11-20-0145-07-000m-sb1-revmd-phy-sec-comments.xlsx>>
        2. Moved: Michael MONTEMURRO
        3. Seconded: Edward AU
        4. **Result Motion #170**: 11-0-2 Motion Passes
     2. **Motion 171: GEN CIDs** 
        1. Approve comments included in the “Motion Feb AdHoc” tab in 11-20/147r4: <<https://mentor.ieee.org/802.11/dcn/20/11-20-0147-04-000m-sb1-revmd-gen-comments.xls>>
        2. Moved: Jon ROSDAHL
        3. Seconded: Stephen MCCAAN
        4. **Result Motion #172:** No objection to approve by Unanimous Consent – Motion Passes
     3. **Motion 172: Editor CIDs** 
        1. Approve comments included in the “Motion-EDITOR-T” tab in 11-20/10r6: <<https://mentor.ieee.org/802.11/dcn/20/11-20-0010-06-000m-revmd-sa1-comments-for-editor-ad-hoc.xls>>, except CID 4800 and 4375
        2. Moved: Emily QI
        3. Seconded: Michael MONTEMURRO
        4. **Result of Motion #172**: 7-0-1 Motion Passes
  3. **Change Telecon tools:**
     1. We had an issue with Join.me and had to re-establish the call on Webex Seat 4.
     2. We were not able to get everyone that was on the first call correctly.
     3. We will take up the rest of the motions on a later call.
  4. **Review doc 11-20/407r1**: Rojan CHITRAKAR (Panasonic)
     1. <https://mentor.ieee.org/802.11/dcn/20/11-20-0407-01-000m-resolutions-for-some-ccmp-gcmp-cids.docx>
     2. CID 4088 (PHY)
        1. Review Comment
        2. Review proposed change and discussion from submission.
        3. Proposed resolution: REVISED (PHY: 2020-03-20 15:02:30Z) - Incorporate the changes in document 11-20/407r1 <<https://mentor.ieee.org/802.11/dcn/20/11-20-0407-01-000m-resolutions-for-some-ccmp-gcmp-cids.docx>> for CID 4088 under "Resolution:"
        4. Discussion:
           1. There is a figure that may need correction, but it is the subject of another CID.
           2. CID 4087 will be addressed in another document.
        5. ~~No objection – Mark Ready for Motion~~ (later changed to more work needed.)
     3. CID 4089 (PHY)
        1. Review Comment
        2. Review Proposed Changes
        3. Proposed resolution: REVISED (PHY: 2020-03-20 15:02:30Z)

At P2609L8, change:

"5) The MIC is extracted for use in the CCM integrity checking."

to

"5) The encrypted MIC is extracted for use in the CCM integrity checking. “No Objection – Mark Ready for Motion

* + - 1. No objection – Mark Ready for Motion
    1. CID 4090 (PHY)
       1. Review Comment
       2. Proposed Resolution: Revised - Incorporate the changes in document 11-20/407r1 <<https://mentor.ieee.org/802.11/dcn/20/11-20-0407-01-000m-resolutions-for-some-ccmp-gcmp-cids.docx>> for CID 4090 under "Resolution:"
       3. More Work Needed
       4. Dan HARKINS will work with Rojan offline.
    2. CID 4091 (PHY)
       1. Review Comment
       2. Proposed Resolution: REVISED (PHY: 2020-03-20 15:13:10Z) - Incorporate the changes in document https://mentor.ieee.org/802.11/dcn/20/11-20-0407-01-000m-resolutions-for-some-ccmp-gcmp-cids.docx for CID 4091 under "Resolution:"
       3. No Objection – Mark Ready for Motion
    3. CID 4093 (PHY)
       1. Review Comment
       2. Review Cited figure 12-26
       3. Discussion on if the “MIC” in the figure is encrypted or not.
       4. Discussion on the order of encryption of the MIC.
       5. Needs more work.
       6. ACTION ITEM: Dan Harkins to work with Rojan CHITRAKAR
    4. Need to review the list of CIDs we talked about today
       1. 4091 Still ok
       2. 4090 still more work needed.
       3. 4089 still ok
       4. 4088 Need more work remove Ready for Motion
    5. Look to add these topics to the Friday March 27th Telecon.
    6. CID 4087 is being handled by Nehru who is on the agenda next week.
  1. **Agenda check** –
     1. Limited time remaining
     2. Move Mark RISON to Wednesday April 1st telecon.
     3. GEN CIDs will consume what is left.
  2. **Review doc 11-20/459r0** Dan HARKINS (HPE)
     1. <https://mentor.ieee.org/802.11/dcn/20/11-20-0459-00-000m-internationalized-character-support.docx>
     2. Abstract: This submission proposes the use of character pre-processing methods in order to support internationalized character sets with usernames (password identifiers) and passwords.
     3. Review submission
     4. Discussion on the citation: IETF RFC 8265, Preparation, Enforcement, and Comparison of Internationalized Strings Representing Usernames and Passwords, P. Saint-Andre, A. Melnikov, 2017.
     5. Discussion on the use of UTF-8 strings
     6. Review proposed changes
     7. Minor changes were made, so an R1 will need to be uploaded.
     8. Discussion on CID 4136 that may be relevant to this document. Mike to check this offline and coordinate with Dan and Mark R.
        1. However, it was determined that this was not similar.
     9. Discussion on the use of “UFT-8” and “process”
     10. Request to include a MIB change as well.
     11. A Separate Motion will be created to incorporate 11-20/459r1 into the draft.
     12. There may be some small amount of work to review the changes after R1, so we need to harmonize with 12.4.7.4 as well.
     13. Will schedule for return on Friday, April 3 telecon.
  3. **Review doc 11-20/351r0** Dan Harkins (HPE)
     1. <https://mentor.ieee.org/802.11/dcn/20/11-20-0351-00-000m-sae-sb1-resolutions.docx>
     2. CID 4136 (PHY)
        1. Review Comment
        2. Review submission discussion.
        3. Proposed Resolution: REJECTED (PHY: 2020-03-20 15:50:26Z) - If the protocol stack has malicious software on it then passing anything, including a “random binary representation” of a password, will be vulnerable. Doing a passphrase to PSK mapping will not make any difference security-wise. The suggested change will not increase security of any system and will make older and newer SAE implementations not interoperable.
        4. No Objection – Mark Ready for Motion
     3. CID 4190 (PHY)
        1. Review Comment
        2. Discussion on the reject reason – not enough detail not that we don’t have some idea of the topic.
        3. Proposed Resolution: REJECTED (PHY: 2020-03-20 16:00:39Z) - The comment fails to identify changes in sufficient detail so that the specific wording of the changes that will satisfy the commenter can be determined.
        4. Mark Ready for Motion
     4. CID 4491 (PHY)
        1. Review Comment
        2. Proposed Resolution: REJECTED (PHY: 2020-03-20 15:55:15Z) - There is no security vulnerability if a salt is known or short. If there are no rejected groups the salt is all zeros anyway which is a constant of all zeros, this is not a security vulnerability as the salt is used as a tweak in the KDF, not as a strengthener to a hashed password. There is no security vulnerability in the existing scheme.
        3. Mark ready for motion
     5. CID 4493 (PHY)
        1. Review Comment
        2. Proposed Resolution: ACCEPTED (PHY: 2020-03-20 15:56:05Z)
        3. No objection – Mark Ready for Motion
     6. CID 4654 (PHY)
        1. Review Comment
        2. Proposed Resolution: REJECTED (PHY: 2020-03-20 15:59:23Z) -The comment fails to identify changes in sufficient detail so that the specific wording of the changes that will satisfy the commenter can be determined.
        3. Mark Ready for Motion
     7. Will return on April 3 to continue at CID 4667
     8. An R1 may be posted, but not required as the resolutions are captured in the database and minutes.
  4. **Review Upcoming agendas**
     1. Wednesday March 25
        1. Will take the motions we did not get to today.
  5. **Discuss April AdHoc**:
     1. We can revisit this next telecon, but we can convert to telecons.
     2. Schedule some time for Adhoc telecons.
     3. Dorothy to make a proposal.
     4. No Face to Face AdHoc will be allowed, so only telecon will be viable.
     5. Would look to schedule one or two telecons (2 hour block) each of those days if we can.
     6. If people have opinion, request to give input.
  6. **Review Attendance** – 16 were on the call at some point.
  7. **THANKS to Michael MOTNEMURRO** for chairing the last few telecons.
  8. **Adjourned at 12:06pm**

**References:**

March 20th:

1. <https://mentor.ieee.org/802.11/dcn/20/11-20-0234-17-000m-2020-jan-mar-teleconference-and-adhoc-agendas.docx>
2. <https://mentor.ieee.org/802.11/dcn/20/11-20-0234-18-000m-2020-jan-mar-teleconference-and-adhoc-agendas.docx>
3. <https://mentor.ieee.org/802.11/dcn/20/11-20-0145-07-000m-sb1-revmd-phy-sec-comments.xlsx>
4. <https://mentor.ieee.org/802.11/dcn/20/11-20-0147-04-000m-sb1-revmd-gen-comments.xls>
5. <https://mentor.ieee.org/802.11/dcn/20/11-20-0010-06-000m-revmd-sa1-comments-for-editor-ad-hoc.xls>
6. <https://mentor.ieee.org/802.11/dcn/20/11-20-0407-01-000m-resolutions-for-some-ccmp-gcmp-cids.docx>
7. <https://mentor.ieee.org/802.11/dcn/20/11-20-0459-00-000m-internationalized-character-support.docx>
8. <https://mentor.ieee.org/802.11/dcn/20/11-20-0351-00-000m-sae-sb1-resolutions.docx>