IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| RCM SG Minutes Interim Meeting Jan 12, 14, 2021 | | | | |
| Date: 2021-01-14 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Graham SMITH | SR Technologies | Sunrise, Florida |  | gsmith@srtrl.com |
|  |  |  |  |  |

Abstract

This document contains the minutes of the IEEE 802.11 RCM SC meetings held on 12 and 14 January, 2021 (Webex)

Note: Highlighted text are action items.

Q- precedes a question asked at the meeting

A- precedes an answer given by the presenter

C- precedes a comment

Chair –precedes an answer or comment by Chair

Rev 1 – Corrected spelling mistakes on Huawei and SR Technologies.

**Tuesday 12, January 2021, 13-30 hrs ET**

**Chair Carol Ansley (self)**

**Acting Secretary Graham Smith (SR Technologies)**

**1 Meeting called to order at 13.30 hrs**

Chair called for secretary and Graham Smith (SR Technologies) volunteered.

**2 AGENDA**

Chair went through the Policy and Procedure slides 20/1629r3, slides 6 to 9

**Administrative**

* + **PARs and CSDs are still in process, waiting on comments**

**Discussion**

* + **Address any comments received on PARs/CSDs**
  + **Review submissions:**
  + **11-21-0336r1** 
    - * <https://mentor.ieee.org/802.11/dcn/20/11-20-0336-01-000m-mac-privacy-and-pmksa-caching.pptx>
  + **11-21-0069r1** 
    - * <https://mentor.ieee.org/802.11/dcn/21/11-21-0069-00-0rcm-privacy-for-password-identifiers.docx>

Any questions/comments?

Q – Under administration are you approving any minutes?

Chair – have approved Minutes up to previous Plenary, and mixed messages as to need to approve minutes for a SG. Intended to approve minutes at next Plenary if needed.

Q – Usually minutes are referenced in reports, recommend that any Minutes on server be approved. Not sure if a hard rule. No reason why you cannot approve in a future minute but then WG minutes may be out of sync. Will investigate.

Chair – Welcome guidance.

Comments – Not unusual for set of minutes to be approved, do not see an issue.

* Can’t find 21-0336 in Mentor.
* Should be 11-20 0336 but r2 being posted.

Chair– Any objections to proceeding? None

**3. Presentations:**

**Presentation 1** “MAC Privacy and PMKSA Caching” 11- 20/0336r2, presented by Michael Montemurro (Huawei)

Originally presented in 11md, but decided to wait for RCM.

Presented for discussion purposes then decide which TG to apply.

Slide 5 shows basic solution:

* AP advertises support for rPMKSA caching in Extended RSNE
* STA associates and signals intention to use rPMKSA caching
* A new PMKID will be generated for each subsequent association (to prevent tracking)
  + The STA and AP generate a new PMKID (rPMKID) each association
* If this feature is supported by both STA and AP, the STA includes the rPMKID in the PMKID List field at Association.
* NOTE: The feature expedites the establishment of a security association – changing the MAC address will affect bridging and higher layer communications.

Which project would this fit into? Needs to be discussed.

Q – Slide 7, option 1 would produce the same PTK each time? Option 2 produces a different PMK.

A – Yes option 2 is probably preferable, but would look to expertise.

Q – Agree, need to address this, KDK needs to be a new value. One corner case, PMKID can be shared between APs. Need a paragraph adding who needs to know the PMKIDs.

Discussion ensued on details (highly technical so details are not 100% captured, just outlines reported):

Q – How long does and AP have the PMKID. How long, days? (default is 43200 seconds)

A – Lifetime is indicated sometimes. Hard to put a time to it. Dependent upon deployment.

Q – Slide 4, changing MAC address effect bridging and higher layer comms.

A – Just stating the problem this is solving.

Q – Tear down. Do you protect against attacker tear down?

A – Once successfully associated, still need 4 – way handshake.

Q – is existing PMKID protected? No

Q - Is there a new PMKID for each AP?

A - Feature OKC (opportunistic key caching) could be used. STA should create new PMK for each association hence FT was created to get around this.

Q – Protecting pre-association? Just trying to fix broken PMK caching.

**Presentation 2** “Privacy for Password Identifiers” 21/0069r0 – presented by Dan Harkins (HPE)

Originally presented in 11md in response to deleting Password Identifiers. Instead of doing away with them, it is proposed to actually provide a way of providing a STA with a pseudonymous, and stateless identity that can be used for one-time access and a way to obtain a new pseudonym for use with a single subsequent connection.

I.e., generate a protected (encrypted) password identifier.

Text presented was generated for 11md so will need modifying.

No questions

**4. Next Meeting:**

Upcoming schedule during plenary:

Wednesday January 13 at 13:30ET

Thursday January 14 at 13:30ET

No requests for presentations so Chair propose cancel Wednesday, keep Thursday.

Any objections? None

**Next Meeting Thursday Jan 14, 13.30 ET**

**5. Any further business?**

Yes – A clarification was given that Minutes from prior telecons can be posted and approved, no need to wait. Need to post and review. If posted it is well in order to consider them.

No further business,

**6. Recess, at 2.26pm**

**Thursday 14, January 2021, 13-30 hrs ET**

**Chair Carol Ansley (self)**

**Acting Secretary Graham Smith (SR Technologies)**

**1 Meeting called to order at 13.30 hrs**

Chair called for secretary and Graham Smith (SR Technologies) volunteered.

**2 AGENDA**

Chair went through the Policy and Procedure slides 20/1629r3, slides 6 to 9

**Administrative**

* + **PARs and CSDs are still in process, waiting on comments**
  + **Approve minutes from November session.**
    - [**https://mentor.ieee.org/802.11/dcn/20/11-20-1788-00-0rcm-minutes-rcm-sg-4-november-2020.doc**](https://mentor.ieee.org/802.11/dcn/20/11-20-1788-00-0rcm-minutes-rcm-sg-4-november-2020.doc)

Q – is this only session for Nov.

A - Will check

Q – Can Chair please bring a private motion at Closing Plenary on the Minutes (if necessary after checking)?

A – If possible will bring motion.

C- Minutes exist for Nov 3 and 4 sessions. Will check record.

A – Will update 1788 to include existing minutes (if they exist).

**3. Discussion**

* + Address any comments received on PARs/CSDs

None received

**4. Telecon schedule**

Upcoming teleconference schedule:

* + Friday 22 January at 10am ET – Comment resolution, if needed
  + Monday 1 February at 10am ET – Technical submissions
  + Monday 1 March at 10:00am ET – Planning for Plenary (TGbh)
  + Monday 1 March at 11:00am ET – Planning for Plenary (TGbi**)**

Q – March 1st 2 meetings are they back-to-back?

Chair – Yes

Q – CAC meets at 9 am. Hopefully does not go over 1 hour. Also what is duration of these meetings

Chair – 1 hour

C – Monday CAC on 1st March may well run long

Chair – Could start 30 minutes later as meetings not anticipated to take 1 hour.

C – OK if we have Chairs ready to go

C – Please do not schedule 0.5 hour calls as boilerplate can use up time. Stick to 1 hour.

Proposed change to

* + Monday 1 March at 11:00-12:00am ET – Planning for Plenary (TGbh)
  + Monday 1 March at 12:00-1:00 pm ET – Planning for Plenary (TGbi**)**

Q – Unfriendly for participant in Australia

Chair – Up to now calls have been at 10 am ET. Possibly 2pm? Move

Any objections to changing call to 2pm.

C – may not have people on this call who would object.

C – Not entirely true as I am on this call (European participant)

Call for 1 Feb is changed:

* + Monday 1 February at 2pm ET – Technical submissions

New schedule is

* + Friday 22 January at 10:00-11:00am ET – Comment resolution, if needed
  + Monday 1 February at 2:00-3:00pm ET – Technical submissions
  + Monday 1 March at 11:00-12:00am ET – Planning for Plenary (TGbh)
  + Monday 1 March at 12:00-1:00 pm ET – Planning for Plenary (TGbi**)**

**5. Any other business**

C – have further info on the Minutes, but suggest taken off line

Chair – We will take this off line

No other Business.

**6. Meeting Adjoined at 2.06 pm ET**