Minutes IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IEEE 802.11 TGbh Meeting Minutes, May Interim 2021  Randomized and Changing MAC addresses (RCM) | | | | |
| Date: 2021-05-13 | | | | |
| 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 bh telecom Interim meeting 11 and 13 May 2021.

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer given by the presenter

C- proceeds a comment

**Meeting May 11, 2021 1.30 to 3.30 pm ET**

**Chair: Mark Hamilton**

**Vice Chair: Peter Yee (NSA-CSD/AKAYLA)**

**Vice Chair: Stephen Orr (Cisco)**

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

**The teleconference was called to order by Chair 1.39 hrs. EDT,**

Agenda slide deck 11-21/0610r3

1. **Policies and procedures were presented by the chair. (Slides 4 to 14)**

There were no Patent declarations.

Copyright policy slides were presented (Slides 10 and 11)

1. **Agenda:**
   * Attendance, noises/recording, meeting protocol
   * Policies, duty to inform, participation rules
   * Organization topics:
     + May Interim meetings: Tuesday, 13:30-15:30; Thursday 13:30-15:30
     + Approve March plenary and teleconference minutes
     + PAR: [https://development.standards.ieee.org/myproject-web/public/view.html#pardetail/8770](https://development.standards.ieee.org/myproject-web/public/view.html) , CSD: [11-20/1117r5](https://mentor.ieee.org/802.11/dcn/20/11-20-1117-05-0rcm-rcm-sg-proposed-rcm-csd-draft.docx)
   * Press release/blog for TGbh and TGbi: [11-21/0760r1](https://mentor.ieee.org/802.11/dcn/21/11-21-0760-01-0000-blog-post-for-p802-11bh-and-p802-11bi.docx)
   * Liaison from WBA: [11-21/0703r0](https://mentor.ieee.org/802.11/dcn/21/11-21-0703-00-0000-2021-april-liaison-from-wba.docx)
   * Parental controls use case: [11-21/0804r0](https://mentor.ieee.org/802.11/dcn/21/11-21-0804-00-00bh-rcm-parental-control-examples.pptx)
   * Issues Tracking: [11-21/0332r5](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-05-00bh-issues-tracking.docx)

The Chair reviewed the agenda. Any comments? None.

The proposed agenda was approved without objection.

1. **Approve the minutes of:**
   * March Plenary session: [11-21/0460r1](https://mentor.ieee.org/802.11/dcn/21/11-21-0460-01-00bh-minutes-tgbh-march-plenary-2021.docx)
   * Teleconference minutes:
     1. March 29: [11-21/0574r0](https://mentor.ieee.org/802.11/dcn/21/11-21-0574-00-00bh-minutes-tgbh-march-29-2021.docx)
     2. April 12: [11-21/0676r0](https://mentor.ieee.org/802.11/dcn/21/11-21-0676-00-00bh-minutes-tgbh-april-12-2021.docx)
   * Moved: Amelia Andersdotter
   * Seconded: Jon Rosdahl
   * Result: Unanimous consent
2. **Press Release 21/760r1**

Reviewed by EC and edits shown.

Basic introduction around privacy and random MAC.

Chair quickly went through the document pointing out the clauses.

Any comments? None

Chair encouraged members to look at the document.

1. **Liaison from WBA** “Wi-Fi Identification Scope, in a post MAC randomization world ”

Chair went quickly through document 21/703. Similar to points out of the TIG. Need to check if any new use cases not previously considered. Members encouraged to check this document and double check if any new cases we need to consider.

Similarly organized to our Tracking Document.

Anyone had chance to review document and/or comments?

C - Should we formally check through the document?

A – Good idea, any volunteers?

Graham Smith volunteered.

C – Has this document been submitted as contribution to TGbh?

A - Posted to WG, but assigned to TGbh

1. **Contribution “RCM – Parental Control examples”, Jerome Henry and Stephen Orr (Cisco)**

[**https://mentor.ieee.org/802.11/dcn/21/11-21-0804-01-00bh-rcm-parental-control-examples.pptx**](https://mentor.ieee.org/802.11/dcn/21/11-21-0804-01-00bh-rcm-parental-control-examples.pptx)

Presented by Jerome Henry:

Points from presentation:

Objective was to show if this Use Case is a real world case. Investigation showed that Parental control based on MAC address is massively present in the market.

* Most home-brand ‘wireless routers’ offer the function
* Most Service providers offer the function in their OEM ‘wi-fi routers’
* Most Enterprise-class AP vendors offer the function, typically more for classrooms than home contexts

Implemented Parental Control examples were presented.

In enterprise brands, use case is typically for small businesses and schools.

Also Apps available with client on child’s device.

MAC-Based vs App-Based:

App-based

* Pros: granular control, easy to setup
* Cons: expensive, needs a client on each device, risk of start/stops

Network-based (MAC-based)

* Pros: Usually free, easy to setup
* Cons: often more basic, easy to circumvent

Conclusion is that MAC based solutions to Parental Control is about 50% of the market. Hence considered a valid Use Case for TGbh.

Propose following straw poll:

**Straw Poll:**

**“Do you support keeping this general scenario as one of our use cases (with possible rewording):**

*Consider a parent with children of ages 10 and 7 years. The parent wants to block access to the home 802.11 network and control access to Internet content based on the user of various devices. For example, the parent has a laptop and a smartphone, and the children each have an age-appropriate laptop and the older child has a smartphone. The parent wants all these devices to be recognized when attaching to the 802.11 network, without launching an application or using a portal. And, this needs to use a method that the kids can’t hack and circumvent. When one of the childrens’ friends visits, their device(s) should be given only very limited access (if any at all) to the 802.11 network and Internet; thus unknown devices need to be distinguishable from one of the family’s devices. Parental control offered in 802.11 routers is usually based on the MAC address of the device.”*

Q – “Kids can hack and circumvent”, not sure we need to come up with solution where kids cannot hack and circumvent?

A – Yes, difficult to make such a promise. Point is that before RCM there is no problem with Parental Control, and with RCM there is a problem.

C – Where do you see parental control features built into OS? We are imagine replacing MAC with some sort of static identifier. Finding a work-around for that static identifier is similar to user changing MAC address. Should we look at other more secure approaches? No objection to the Use Case.\

A – Have no solutions at the moment. Could be many cryptographic solutions but first let’s get the Use Cases agreed upon.

Q – With RCM cannot simply use MAC addresses as the entry. Do we really have to come up with solution that can’t be hacked or circumvented? Is this really in the area for IEEE? Do we need solutions for applications that do not work anymore?

A – Scope is what is broken with RCM? Maybe we find that there is no better solution. Scope of TG is to examine cases where RCM has introduced problems, then decide if it makes sense to make changes. Maybe informative Annex? Probably some outside of our scope.

C – Did you come across any solutions to RCM?

A – Android, Apple and MS all allow switching off RCM. Have seen solutions using ISP cloud access adding another layer.

C – Maybe not all parental control need not be solved at IEEE network attachment layer, maybe time based or at operating system level.

A – With RCM not sure who is connected not just children but everyone who may connect.

C – RCM brought to light that MAC was never really intended as an ID. If you know what the device is then can control etc. Having an ID is an important capability. These are not public networks, then ability to provide a useful ID at network level is important.

C – When 802.11 started we started with WEP due to restricted key length. Thieving of high end cars by stealing key fob vulnerability. Recommendation out of this TG may be useful for a very short time.

A - Similar to license plate on cars, no way to know if this is legitimate.

C - If you want to know who someone is then you need to authenticate them using their credential. The problem becomes assignment of credentials to users. Kids get password ID "kids" and a certain password. Parents get password ID of "parents" and a different one. Access for "kids" stops at 9pm but it available for "parents" 24hrs. Kids can share their "kids" password with their friends because you know they're going to do that anyway but access stops when "kids" should be in bed so it doesn't matter if they share it or not.

A – Do we think any point in placing in informative Annex?

C – Would be helpful to provide response to WBA points. But adding to Standard I feel is not required.

A – If we use password-type protection, this works for those connected. What about other cases pre-association, steering etc. Not knowing same device coming back again.

C – We need to decide on whether we keep this Use Case?

C – Decision what goes into our Tracking Document, cases we an “cure” or only cases that we feel can be “cured”. Do we agree that an informative Annex is something we could add?

C – This is what the Straw Poll will decide.

C – Maybe record cases only that we feel we can do something in the Standard. Would not make decision at this stage on the Annex idea.

C – We need to record a case was considered even if we do nothing. Hence the Tracking document should contain all cases considered as a record of what was considered.

C – For this particular case do not feel that we would work on, but if entered into Tracking Document maybe together with something stating “no further work on solution”.

C – Tracking List should contain only issues of concern, especially as raised by WBA.

C – Everything should go into the Tracking Document. Later we add “no action”, “maybe action – further work”

C – Can we have a straw poll on what is recorded in the Tracking Document?

C - Note: We have a section in the tracking document (section 5) where we list technical solutions to the issues raised. We could agree that that section can reach the conclusion that X, Y, Z (that already exist) will solve this.

C – This is a Use Case document, should not be afraid to ask questions we do not have answer to. We will move on to an SFD and then the Tracking document may be forgotten. Having Use Cases helping us to identify some mechanism is useful.

C – Not convinced that this Use Case fits the ‘needs to be fixed” criteria.

C – “Tracking Document” is new term, so yes, let’s define it.

A – Tracking Document is a more informal document.

Chair - Proposed Straw Poll: The tracking document can (should) include use cases that have been identified, for which we believe either the solution is outside our scope, or the solution already exists, and we can so note/respond to the use case in the “technical solutions” clause.

After discussion and wordsmithing,

**Straw Poll**:

“Should the informal tracking document also include use cases that have been identified for which we believe either the solution is outside our scope, or the solution already exists, and we will so comment on the use case?”

Yes: 25 No: 4 Abstain: 5 (23 no answer)

**Out of time**

**Meeting recessed at 3.30 pm.**

**Meeting May 13, 2021 1.30 to 3.30 pm ET**

**The teleconference was called to order by Chair 1.31 hrs. EDT,**

Agenda slide deck 11-21/0610r4

1. **Policies and procedures were presented by the chair. (Slides 4 to 14)**

There were no Patent declarations.

Copyright policy slides were presented (Slides 10 and 11)

1. **Agenda**
   * Attendance, noises/recording, meeting protocol
   * Policies, duty to inform, participation rules
   * Organization topics:
     + PAR: [https://development.standards.ieee.org/myproject-web/public/view.html#pardetail/8770](https://development.standards.ieee.org/myproject-web/public/view.html); CSD: [11-20/1117r5](https://mentor.ieee.org/802.11/dcn/20/11-20-1117-05-0rcm-rcm-sg-proposed-rcm-csd-draft.docx)
   * Issues Tracking updated Introduction: [11-21/0332r6](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-06-00bh-issues-tracking.docx)
   * Parental controls use case: [11-21/0804r2](https://mentor.ieee.org/802.11/dcn/21/11-21-0804-02-00bh-rcm-parental-control-examples.pptx)
   * Continue with Issues Tracking use cases: [11-21/0332r6](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-06-00bh-issues-tracking.docx), [11-19/1442r9](https://mentor.ieee.org/802.11/dcn/19/11-19-1442-09-0rcm-rcm-tig-draft-report-outline.odt)
   * Next Steps:
     + Timeline review – Contributions needed (starting on solutions text)!!
     + July plan
     + Teleconferences

The Chair reviewed the agenda. Any thoughts or comments? None

The proposed agenda was approved without objection.

1. **Issues Tracking Document**

21/0332r6 Added sentences into Introduction

“Section 4 has a set of use cases which provide real-world example contexts in which some issue(s) arise from randomized and/or changing MAC addresses. These include use cases that have been identified for which we believe either the solution is outside our scope, or the solution already exists, and we will so comment on the use case. (That is, the use cases list includes all the use cases that the task group has considered, even when the conclusion is that no changes are needed/appropriate in IEEE Std 802.11.)”

Any thoughts/comments?

C – Yes, like the additions, it works well, thank you.

1. **Parental Control Use Case**

Jerome re-presented 21/0804r2. Concluded that using MAC address exists today. Discussion on whether we should track this case.

**Proposed Straw Poll**

**Do you support keeping this general scenario as one of our use cases (with possible rewording):**

*Consider a parent with children of ages 10 and 7 years. The parent wants to block access to the home 802.11 network and control access to Internet content based on the user of various devices. For example, the parent has a laptop and a smartphone, and the children each have an age-appropriate laptop and the older child has a smartphone. The parent wants all these devices to be recognized when attaching to the 802.11 network, without launching an application or using a portal. And, this needs to use a method that the kids can’t hack and circumvent. When one of the childrens’ friends visits, their device(s) should be given only very limited access (if any at all) to the 802.11 network and Internet; thus unknown devices need to be distinguishable from one of the family’s devices. Parental control offered in 802.11 routers is usually based on the MAC address of the device.*

C – Hesitant to add use case that we won’t be working on but do want to have the use case to show we considered it. Hence not happy with the wording as shown.

A – Shall I reword.

C – Want it re-worded that we won’t be working on it.

A – Hoping for a two-step approach. First the Use Case, then decision.

C – As written would vote no, but changes to the “Hacking” and “friends’ visits” need to be taken out. This method of using MAC addresses will be abandoned.

C – I think this is important for many Wi-Fi Users and should be kept.

C – We said we will include all use cases and so comment.

On line editing:

**Do you support document this scenario in our tracking document:**

*Consider a parent with children of ages 10 and 7 years. The parent wants to block access to the home 802.11 network and control access to Internet content based on the user of various devices. For example, the parent has a laptop and a smartphone, and the children each have an age-appropriate laptop and the older child has a smartphone. The parent wants all these devices to be recognized when attaching to the 802.11 network, without launching an application or using a portal. ~~And, this needs to use a method that the kids can’t hack and circumvent~~. When one of the childrens’ friends visits, their device(s) should be given only very limited access (if any at all) to the 802.11 network and Internet; thus unknown devices need to be distinguishable from one of the family’s devices. ~~Parental control offered in 802.11 routers is usually based on the MAC address of the device.~~ Many 802.11 routers provide capabilities to restrict network access based on the MAC address of the device.*

*Documenting this scenario does not imply that 802.11bh has any action to take to resolve it.*

Q – Fundamental function to be examined is device based restriction. If broken, then fix it. Make use case more general for cases of device based restrictions.

A – Yes, we do have others, parental control is an existing case that can be well described.

C - As an aside, Wi-Fi Easy Connect could easily address this use case - even the friends visiting part.

C - There are multiple ways to provide this feature today. We don't need to work on this.

C – Do we agree that RCM breaks this?

C – Kids can figure out how the change MAC address, anyhow, so was a dumb way of doing Parental Control, but RCM is still a problem

Q – 2 different straw polls, one to agree not to look at it?

A – Was original intent. But want to avoid those voting NO to the first.

C - We have Wi-Fi Easy Connect, applies policy and time limited credentials, and we have enough tools to create a solution. 802.11 is wrong place to address this, Wi-Fi Alliance is better place. We need not spend time in this Group.

C – Use Cases should be specific so as to describe clearly. As to solutions exist, not so sure, need to think about tying a human being to a device we start thing biometrics and years away from that. To figure that RCM breaks it is not really the point. But this is not the right group for that discussion.

C – Can put a note in the straw poll that we may not work on it.

(Note, presenter added sentence at end – see above)

C – The PAR is pretty clear. But getting concerned at time we are taking.

C – Volunteers produce Use Cases, then volunteers offer to produce a resolution. If someone brings up a Use Case, then it should go into the Tracking Document.

Straw Poll

**Do you support document this scenario in our tracking document:**

*Consider a parent with children of ages 10 and 7 years. The parent wants to block access to the home 802.11 network and control access to Internet content based on the user of various devices. For example, the parent has a laptop and a smartphone, and the children each have an age-appropriate laptop and the older child has a smartphone. The parent wants all these devices to be recognized when attaching to the 802.11 network, without launching an application or using a portal. When one of the childrens’ friends visits, their device(s) should be given only very limited access (if any at all) to the 802.11 network and Internet; thus unknown devices need to be distinguishable from one of the family’s devices. Many 802.11 routers provide capabilities to restrict network access based on the MAC address of the device.*

*Documenting this scenario does not imply that 802.11bh has any action to take to resolve it.*

RESULT: Yes: 15 No:5 Abstain:3 Did not vote:16

Chair – Hopefully, although we don’t think TGbh should solve this, there are solutions and these should be documented against this Use Case. Anybody can bring forward responses to this Use Case.

C – Technically possible to address this, but should we do that here? No. If someone does something to document this elsewhere then OK.

C – We must have some response that says why we ae not considering, same as a reject to a comment, we always say why.

**Back to Tracking Document**

Chair went through the Introduction to the document. Skipped Terminology. Section 3 Brainstorming is to keep ideas that come up. If any ideas or additions, please come forward.

**Airport security queue**, probably not to be worked on, so need volunteer to draft case.

Jerome volunteered

Section 4 gathers Use Cases. Lots of wordsmithing already taken place.

Left off previously at 4.3 ***“Post-association home automation (including arrival detection)”***

Any thoughts or comments?

C – This is a different case. STA is willing and interested in being tracked. We should work on this one.

Q – Are we happy with the text?

C – Use case makes sense but would like to see something along lines of STA is co-operative

Added text “Key Point: the device (user) is voluntarily opting-in to this system. Also key that protection from third party tracking is included.”

C – If we show solution, are we indicating how hackers could also use it? Any solution we provide should not present additional problems.

A – PAR does cover this.

Chair – This Use Case needs wordsmithing, Chair volunteered.

Chair looked at Index where Use Cases are listed. Looking for volunteers.

Looked at **Grocery store customer flow Use Case**. Referred to 19/1442r9 TIG Report.

Different to Home automation. RCM breaks this as pre-association.

C – Immediate reaction is only if this is voluntary,

C – Require a phone for the feature. Most phones do RCM (for several years) so not a real world examples of things breaking with RCM. So if it was a problem people would be screaming. Is this really a problem?

A – Have heard of this problem for several years. Counting MAC addresses, then RCM happened. Just used people who came before, now saying can’t rely on that anymore. But do want this, so new methods arisen, e.g. using cameras. Definitely should see if there is an 802.11 solution.

A – Have heard of systems that do it and have heard of the complaint. Worried about alternatives.

C – Will install security cameras anyway.

A – Cost. Camera installation and use for tracking people is costly. Simple security is different.

C – Use case is good example of tracking against person’s will. Not in our PAR. Anything involuntary we should not do, need to opt-in.

C – Agree on privacy issue. If store offers a network, they get information.

C – Sympathetic, but in walking into a store already agreed to be tracked, by camera for example.

C - Do not want to enable involuntary tracking. But Customers can find this convenient. We don’t need to come up with new systems to make it easier.

C – Store is not tracking individuals, it is tracking trends, patterns. There is no sense of involuntary tracking.

C – Store does not need to have any information about the actual identity.

C – Do not want in any form anyone tracking me without my consent.

C – There are many features with tracking, GPS in every phone, not always simple to state Wi-Fi is all bad if used for tracking. Every phone has a static phone number, records position when taking a photo. Need to keep Use Cases and then have a proposed discussion with a recommendation.

Chair – Volunteer to take this and provide and analysis and recommendation?

C – Should document and provide reasons to not do anything.

Chair – Volunteers? No response. Chair MAY do it.

Chair – Have heard “where is limit of our PAR?”. Will take this as action to clarify the PAR. ACTION ALL

**Use Case “Grocery Store frequent shopper notifications”**

Definitely an opt-in, but does have a trust issue i.e., definitely in the store.

C – Similar to Home Automation case.

C – Opt-in to being tracked or opt-in to the store so only they can track me. Or being trackable by anyone while in the store?

A – If involves associating to the store network, then trackable anyway.

C – Tracking has to be by a single entity and user agrees (opt-in to that specific store while in that store).

C – Install app on phone with SSID of store, then connect automatically. App records what you buy, for example

1. **Teleconferences**

Teleconferences through July session:

* 2 slots? 3 slots? (not May 31, not July 5)

C - Suggest 3, see how submissions do.

Settled on 3.

Avoid conflicts with (TGs): TGbi, REVme, ARC, TGbe(MAC/Joint)

C – please avoid TGbc

* Monday 1pm (alternate with ARC)?
* (Not May 31, not July 5)

C – Mondays tend to be Bank Holidays in UK/Europe.

**Out of agenda and time**

**Meeting Adjoined at 3.31 pm ET.**