IEEE 802 EC SG
Privacy Recommendation

|  |
| --- |
| Minutes of EC Privacy Recommendation SG Teleconference November 3-7, 2014 |
| Date: 13 January 2015 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Joseph Levy | InterDigital |  |  | joseph.levy@interdigital.com  |
| Karen Randall | Randall Associates |  |  | karen@randall-consulting.com  |

Abstract

Minutes of the EC Privacy Recommendation SG face-to-face meeting during the IEEE 802 November 2014 Plenary in San Antonio, TX, USA.

**Tuesday, November 4th, 2014**

Chair: Juan Carlos Zuniga

Recording secretary: Joseph Levy and Karen Randall

**Call to order**

* Meeting called to order at 19:35 hrs EDT.
* The chair slides were posted:
* <https://mentor.ieee.org/privecsg/dcn/14/privecsg-14-0021-00-ecsg-nov-plenary-meeting-slides.pptx>

**IEEE WG Guidelines**

* The chair read the IEEE guidelines and asked for declaration of Potentially Essential Patents.
	+ No IPR issues were brought up

**Appointment of recording secretary**

* Joseph Levy and Karen Randall volunteered to take notes

**Agenda**

* Welcome
* Chair's slides
	+ IEEE Slides
	+ Call meeting to order
* Group’s updates
	+ 802c PAR update / comments to be submitted
	+ EC Closing Report
* Technical Presentations
	+ Separation of Access and Core Partitioning in the Local Space
	+ Privacy Threat Model
	+ IETF MAC Address Randomization Trial Status & Wiki Page
* Next Steps

**Group’s updates**

* **IEEE 802c PAR**
* Amendment to IEEE Standard 802-2014
* Local address space usage recommendations and rules
* PAR: <http://www.ieee802.org/1/files/public/docs2014/new-addresses-thaler-local-address-par-v01.pdf>
* CSD: <http://www.ieee802.org/1/files/public/docs2014/new-addresses-thaler-local-address-csd-v01.pdf>
	+ Juan Carlos pointed out that EC will accept comments from us as long as they are submitted by 24:00 hours tonight.
	+ Roger Marks presented: <https://mentor.ieee.org/privecsg/dcn/14/privecsg-14-0019-01-0000-separation-of-access-and-core-partitioning-in-the-local-space.pdf>

Pat – I think the end use – I don’t know if the same protocol that are using them even have to know that how to use them .

Ans – the enable is to enable 802 protocols that can use these addresses.

Pat  - the existing PAR does say there is a block for local assignment. One could talk about other uses.  I don’t know how big a block we would need for reserved use or another need.

Ans – all the space is the sid space, the RAC says it is all their space. All I am saying is that some space should be reserved.

Dan Harkens – your presentation started really well – with the stations arbitrarily choosing a mac address and the it is translated to the core.  Then you started talking about allocation of the local address space.

Ans –This is not advocacy – it is just my view on what could happen.

Geoff – RAT member – the purpose of the CID was for people who needed a corporate identifier – who did not manufacture and needed a number. So this proposal is a miss application of the intent of the CID.  My understanding of the PAR – currently the local administrator controls all the local addresses, the PAR is to enable some of that space not be under the control of the local administrator.

Paul Lambert – I am very against any of this type of assignment.  For privacy the more addresses the better for privacy.   I am not sure why you can’t have private agreements.   I would like to see us go back to the PAR and address the privacy issues.

Pat – It is impossible of putting everything in the PAR – it is about protocols and the need for blocks defined for protocols.   I don’t think there is a privacy if ¼ the address are not available.   I think there still will be a low probability of collision.   This really does not make it any less private as there is no way to associate the random address to the user.  Disagreed with Geoff with the meaning of the CID and the purpose of the CID – this has been the use of CID address from the beginning.   I presented this to the RAC and there were no issues from the RAC.

Bob – I know there are networks out there 30,000 addresses.  Regarding security, I have been working on provable addresses.  We can define a coordinator which can vet a MAC address, on a particular network.   I think we can do this from a security and collision view. We want to play in the local space, we should be able to define a way to all play well in the space.  We should do this cryptographically.

Roger – I only care of a small space for 802 to be able to build protocol on.

* Comments  on the 802c PAR and CSD “Local media Access Control (MAC) Addressing”
* The 802c recommendations should allow (i.e. should not prevent) random assignment of MAC addresses for first time communications over-the-air, without the need to implement either a claiming or an assignment protocol.
	+ Does this need to be over the whole space
	+ Pat – I think it could be constricted without is hurting anything, and I also believe it need not be constricted.
	+ Andrew – I don’t think we would really need all 48 bits, for first access.  Also I see privacy for first connection, but we don’t see why we are not concerned about privacy while we are connected.  Privacy is a social issue, one potential social solution is the law.  If the law said this, there will be bad actors, but most will not and hence privacy will improve.    JCZ – response – we are doing both probing connected MAC address.
	+ Andrew – I think if we want to make this comment we need to turn it into a real sentence.
	+ Dan – I think we are concerned beyond access, and do want to address connected devices.  We could do some type of address assignment – I don’t see a need to limit the address space.  All of the issues that have been brought up in the PAR can be dealt with, without dividing the address space.
	+ PAT – we need the subdividing in the wired world.   We have the need for protocols. As of now there are not rules and random blocks are currently assigned.  The block is chosen when the protocol is written.   So if we get a handle on this we will get control on this.
	+ Dan – this seems to say there are protocols that are currently doing this without allocation of MAC address.
	+ Andrew – I’m hearing a lot of passion.  We may be getting to the end point way to prematurely.  And we all have different views of the problem, let alone the solution.  I would like to see the stakeholders to reach some consensus on what the problems are.
	+ Joseph ??? – I think having random mac address would complicate who is connected to the network. -  I think it has to say local space in this bullet.
	+ Pat – some of the users need to use an allocation plan that will work.
	+ Bob – wireless devices MAC address end up on wire – and just because you v-LAN –doesn’t mean that I should put everyone on their own physical network and bridge them to the rest of the network.  There are too many conflicting view out there to create rules that will work.   We know what will be put on the network.
	+ Pat – FCOE is already doing this, not doing nessicaraly doing the band plan.   This is already going on, and we are trying to organize this so we can move forward in the future.
	+ Paul – I don’t see that this solves the problem – defining address with protocols, if there are multiple instances of the same protocol.   Having people pay for a virtual protocol does not seem to be the best way forward.   Leaving to the vendors to deal with this, is a trivial and unimportant problem.
	+ Pat – there are existing protocols – the talk to each other and divide up the space.   It is for protocol using B and can divide up the space.
	+ Joni – I don’t see way the solution is in the PAR – if people need a globally unique address – locally administrated addresses are not unique.   I think this statement should be removed from the PAR, and dealt with within the group.
	+ Chair – three questions
		- Is there is a need to allocate a portion of the address space for protocols using an IEEE Registration Authority assigned Company ID. Another r portion of the local address space will be allocated for assignment by local administrators”?
			* Y/N/A – 2/7/10
		- Are there a privacy issue with allocating portions of the local address space?
			* Y/N/A – 8/4/9
		- Should the 802.1 working group consider postpone submitting the RAR for approval?
			* Y/N/A – 13/1/4
		- The SG recommends that the 802.1 working group develop a MAC management protocol.
			* Y/N/A – Not taken
		- Minimum number of bits required for a WiFi deployment with random MAC addresses?
	+ Chair – two comments – slide 3, and slide 4. y/n/a: 16/1/3
* Comments from Privacy EC SG to 802.1 about 802c PAR were compiled and submitted before the deadline on the evening of Nov 4: <https://mentor.ieee.org/privecsg/dcn/14/privecsg-14-0022-01-ecsg-comments-to-802c-par-csd.pptx>
* Meeting recessed at 21:30 hrs

**Thursday, November 6th, 2014**

**Call to order**

* Meeting called to order at 19:31 hrs EDT.
* An updated version of the chair slides was presented:
* <https://mentor.ieee.org/privecsg/dcn/14/privecsg-14-0021-01-ecsg-nov-plenary-meeting-slides.pptx>

**Review of minutes**

* Oct 1 <https://mentor.ieee.org/privecsg/dcn/14/privecsg-14-0016-00-ecsg-minutes-of-ec-privacy-recommendation-sg-teleconference-october-1st-2014.docx>
* Oct 22 <https://mentor.ieee.org/privecsg/dcn/14/privecsg-14-0018-00-ecsg-minutes-of-ec-privacy-recommendation-sg-teleconference-october-22nd-2014.docx>
* Juan Carlos: Approval of minutes from Oct 1 and Oct 22, 2014 teleconferences were approved by vote: 12 in favour, 0 against 0, 1 abstained.
* **802c PAR Report – follow up**

An updated slide on IEEE 802c par with the final comments that were submitted on Tuesday night was shown.

Juan Carlos reported that at the 802.1 WG meeting it was decided not to submit the PAR at this meeting; instead, a request to form a Study Group will be made.

* **IETF MAC address randomization trial**

Discussion about MAC randomization trial at IETF 91. Will be inviting attendees to participate in the trial by following instructions in the wiki page. JC showed the Wiki page and summarized the details about the trial. He reviewed the trial setup (e.g., different SSID: separate VLAN, DHCP, Switching and AAA infrastructure; etc.) and the statistics to be collected (both network and client metrics).

Dan: why client report which MAC address used?

Reply: if they can provide client ID, the server will have the correlation. yes. this is a backup?

Dan commented that he has been using a random MAC all this week.

Andrew: is there a test hypothesis associated w/each of the variables? it might be useful to have some formal hypotheses.

* **Privacy Threat Model**

Privacy Threat Model. JC reviewed the presentation (<https://mentor.ieee.org/privecsg/dcn/14/privecsg-14-0014-00-0000-802-privacy-threat-model.pptx>) that had been quickly presented during the last teleconference. It is envisioned that this is a draft privacy threat model that can be used as a baseline or reference.

Roger Comment – intrusion (slide 11) – not necessarily just the initiator (in the last bullet)

Dan Harkins – comment on Secondary Use (slide15). thinks it may be in IEEE 802 scope (point made in last bullet item on the page that there are secondary uses made of link layer identifiers).

Andrew Myles – moving forward, are proposals being judged against the model?

Response – idea would be to adopt some sort of threat model

It will be important to know which are the “important” threats.

Proposed next steps. most of the work of this group has been on the email exploder or in the teleconference. this has worked well.

* **Privacy EC SG extension**

Request extension of the Privacy Recommendation EC SG until the end of the March ‘15 meeting

Develop a PAR/CSD on recommended privacy practices for IEEE 802 protocols

Continue call for proposals to discuss technical topics

* 10 December 2014, (10:00 AM ET) Teleconference
* January
	+ 12-15 January 2015, IEEE Interim meeting in Atlanta
* 4 February 2015, (10:00 AM ET) Teleconference
	+ Potential PAR/CSD submission
* 25 February 2015, (10:00 AM ET) Teleconference
* 8-13 March, 2015, IEEE 802 Plenary meeting in Berlin, Germany

Andrew –any plans to rotate the times/pain around.

do we want to change any of the times? n America: 15; Europe: 4; asia 2

withdraw comment this time but consider for future teleconference planning.

Proposed Next Steps:

request extension, develop PAR, proposed plan.

SG votes:

Request extension of the Privacy Recommendation EC SG until the end of the March ‘15 meeting

20/0/0

Should we work on developing a PAR/CSD on recommended privacy practices for IEEE 802 protocols.

Think request may be premature now. Appears to be active interest in this topic, with a goal of writing the PAR.

Approval of plan for upcoming meetings and teleconferences.

Y: 20/0/0

JC will generate report to EC and request and extension of SG until March meeting.

**AOB**

* None

**Adjournment**

* Meeting adjourned at 20:30 hrs