IEEE 802ECSG  
Privacy Recommendation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Minutes of EC Privacy Recommendation SG Teleconference  December 10th, 2014 | | | | |
| Date: 13-January-2015 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Karen Randall | Randall Consulting |  |  | [karen@randall-consulting.com](mailto:karen@randall-consulting.com) |

Abstract

Minutes of the EC Privacy Recommendation SG teleconference on Wednesday, December 10th, 2014.

**Wednesday, December 10th, 2014**

Chair: Juan Carlos Zuniga

Recording secretary: Karen Randall

**Call to order**

* Meeting called to order on at 10:10am EDT.
* The chair slides were posted:
* <https://mentor.ieee.org/privecsg/dcn/14/privecsg-14-0024-00-ecsg-dec-10-conf-call-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**

* A call for an EC SG Secretary was made, but no one volunteered for the position
* Karen Randall volunteered to take notes
* No one opposed to recording meeting for keeping minutes

**Roll call**

|  |  |
| --- | --- |
| **Name** | **Affiliation** |
| Juan Carlos Zuniga (Chair) | InterDigital |
| Mathieu Cunche | INRIA |
| Brian Weis | Cisco |
| Dan Harkins | Aruba Networks |
| Carlos Bernardos | UC3M |
| Soo Bum Lee | Qualcomm |
| Guillermo Llosa |  |
| Piers O’Hanlon | Oxford Internet Institute |
| Bob Moskowitsz | Verizon |
| Karen Randall | Randall-Consulting |
| Roger Marks | EthAirNet |
| Jouni Malinen | Qualcomm |
| Rene Struik | Struik Security Consultancy |
| Peter Yee |  |
| Yungsong Yang |  |

**Agenda**

* Welcome
* Chair's slides
  + IEEE Slides
  + Call meeting to order
* Group’s updates
  + Local Space Address Usage SG (802c PAR)
  + IETF MAC address randomization trial preliminary results
* Technical Topics
  + Threat Model for Privacy at Link Layer
  + Privacy Issues at Link Layer
  + **Proposals regarding functionalities in IEEE 802 protocols to improve Privacy**
  + Proposals regarding measuring levels of Privacy on Internet protocols
  + Implications of MAC address changes
  + Other

Next Steps

Agenda reviewed and approved no changes.

2 presentations planned for this meeting: Bob M and Carlos & JC

**Reports**

* **802c PAR**

Juan Carlos provided an update on IEEE 802C PAR Discussions

outcome – PAR not submitted to EC. A Study Group was formed to look at addressing issues from all the different points of view and potentially propose a new scope for the work (PAR). SG will meet at the interim meeting in Atlanta. Will coordinate agendas with ECPriv SG because of interest to participants of both groups.

* **IETF Trial – preliminary results**

Juan Carlos reviewed the preliminary results from the MAC Randomization trial at IETF 91 meeting

Still waiting on some of the results so a more detailed summary will be available later.

Carlos Bernardos (UC3M, Universidad Carlos III de Madrid) presented slides: <https://mentor.ieee.org/privecsg/dcn/14/privecsg-14-0025-00-0000-wifi-privacy-network-experiment-at-ietf91.pptx>

Goal - experiment on WiFi MAC randomization in Windows, MAC OSX, and Linux

Analyze impact of L2 MAC randomization on the user experience and network infrastructure (especially in case of L2 collision).

Specific SSID deployed at IETF meeting.

Operating Systems – some worked; but some didn’t - the connection manager on some of the Ubuntu Linux versions did not support the trial.

Most users on MAC OS and Linux, just a few on Windows (7%).

50 participants

* number of “seen” L2 addresses appx 60% higher than with no address randomization.
* collisions were forced - both devices were impacted.

Next steps:

* awaiting final logs
* prepare “wish” list for network admins for future experiments
* address randomization tools for other platforms (e.g., Android)
* more extensive study of collision effects in diff scenarios

Piers: did you look at PryFi app? or not supported for this

didn’t look at this time/trial.

Dan H had looked at for Nexus devices and it didn’t work. looks promising. would be interesting to see what does it work on?

Piers – on Ubuntu issue, commented that he has MAC change working okay on Ubuntu 12 – could be network configurator that interfered with the changes.

Bob M – had extremely inconsistent results with Fedora

* **Secure Moderated Random MAC Addresses**

Bob Moskowitz presentation: Secure Moderated Random MAC Addresses .

<https://mentor.ieee.org/privecsg/dcn/14/privecsg-14-0026-00-0000-secure-moderated-random-mac-addresses.ppt>

His presentation is a collection of “thought” slides for consideration. For the “free for all” in Local Scope MAC address space, randomized address selection has no method of dealing with collisions. Client informs moderator of MAC address it will use. Moderator either accepts or rejects. Proposed crypto/secure exchange.

Dan H – questions about how the moderator recognizes different clients

discussion

could pull crypto out completely. may not add as much as originally thought.

goal – create a larger trusted space for the clients to use.

Piers – protects/ give you privacy in case of a third party that is preying on the identities. Individual gets certain level of privacy. but not if moderator or AP owner is party to the tracking.

Bob will revise presentation and upload a new version.

**Next steps**

Juan Carlos reviewed Next Steps for ECPriv SG:

* Compile results from MAC privacy experiment and produce a report and follow up steps
* Consider developing a PAR on recommended privacy practices for IEEE 802 protocols
* Continue call for proposals to discuss technical topics

**Upcoming meetings**

12-15 January 2015, IEEE Interim meeting in Atlanta, GA, USA

2 sessions on Tue/Thur evening – 730-930pm.

4 February 2015, (10:00 AM ET), Teleconference

If planning PAR/CSD - submission needed out of this meeting

25 February 2015, (10:00 AM ET), Teleconference

March 8-13, 2015, IEEE 802 Plenary meeting in Berlin, Germany: continue SG, submit PAR?

**AOB**

* None

**Adjournment**

* Meeting adjourned at 11:07 hrs