IEEE 802ECSG  
Privacy Recommendation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Minutes of EC Privacy Recommendation SG Teleconference  September 3rd, 2014 | | | | |
| Date: 3-September-2014 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Karen Randall | Randall Consulting | 20 Elana Drive  Jackson, NJ 08527 USA | +1 (609) 240 3844 | karen@randall-consulting.com |
| Juan Carlos Zuniga | InterDigital | 1000 Sherbrooke W  10th Floor  Montreal, QC, Canada | +1 (514) 904 6300 | j.c.zuniga@ieee.org |

Abstract

Minutes of the EC Privacy Recommendation SG teleconference on Wednesday, September 3rd, 2014.

**Wednesday, September 3rd, 2014**

Chair: Juan Carlos Zuniga

Recording secretary: Karen Randall

**Call to order**

* Meeting called to order on at 10:04 hrs (EDT).
* Announcement that this was the first teleconference of the IEEE 802 Privacy Recommendation SG
* The chair slides were posted:
  + <https://mentor.ieee.org/privecsg/dcn/14/privecsg-14-0004-00-ecsg-sept-3-confcall-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 |
| Antonio de la Oliva | UC3M |
| Dan Harkins | Aruba Networks |
| Paul Lambert | Marvell |
| Soo Bum Lee | Qualcomm |
| Robert Moskowitz | Verizon |
| Piers O’Hanlon | Oxford Internet Institute |
| Walter Pienciak | IEEE-SA |
| Karen Randall | Randall-Consulting |
| Max Riegel | NSN |
| Dan Romascanu | Avaya |
| Rene Struik | Struik Security Consultancy |
| Brian Weis | Cisco |

**Agenda**

* Welcome
* Chair's slides
  + IEEE Slides
  + Call meeting to order
* Group's Introduction
* Technical Topics
  1. Privacy Issues at Link Layer
  2. Threat Model for Privacy at Link Layer
  3. Proposals regarding functionalities in IEEE 802 protocols to improve Privacy
  4. Proposals regarding measuring levels of Privacy on Internet protocols
  5. Other
* Next Steps

**Review of minutes**

* No minutes exist yet (first meeting)

**Group’s Introduction**

* Juan Carlos Zuniga reported some background information about the group and scope (also from chair’s slides):
  + Privacy tutorial at the last IEEE plenary meeting in July:
    - Pervasive Surveillance of the Internet – Designing Privacy into Internet Protocols
  + Group’s plan is to use mainly teleconference and email discussions
  + The group is not chartered to draft an official IEEE 802 specification. The main output would be a PAR for Recommended Practice, should the need be determined. However, technical work can be discussed and advanced in the SG, so that upon an eventual PAR approval the work can be simply continued.

**Call for proposals/contributions**

* Currently the group is considering the following topics:
  + Privacy Issues at Link Layer
  + Threat Model for Privacy at Link Layer
  + Proposals regarding functionalities in IEEE 802 protocols to improve Privacy
  + Proposals regarding measuring levels of Privacy on Internet protocols
* Other topics can be brought up and considered by the group.

**Trial on MAC address randomization**

* Suggestion to perform an opt-in trial on IETF and IEEE meetings networks to assess performance and implications of user’s MAC address randomization
  + MAC address randomization identified as one of the potential solutions to some privacy issues at L2
  + Robert Moskowitz: personal experience has shown that it is not trivial to set this up on different Oses
  + Piers O’Hanlon: PryFi can immediately help for Android devices, although it is a black-box solution. OSx provides some flexibility, but need to assess implications, e.g. on crypto
  + Juan Carlos Zuniga: talked with network providers for both IEEE and IETF meetings. They are open to working with us to set up this trial, but need more details. For that, we need to have a set of requirements ready.

**Presentation - Bluetooth LE/Smart/v4 Privacy – Piers O’Hanlon (Oxford Internet Institute)**

* <https://mentor.ieee.org/privecsg/dcn/14/privecsg-14-0005-01-0000-bluetooth-privacy-aspects.pptx>
* Piers provided a summary of the Privacy features in the latest Bluetooth specifications, which have some modes to randomize MAC addresses
* Dan Harkins: What is the value of having resolvable random MAC addresses?
* Piers: Value is that the two parties have a shared key then they can continue to communicate; third party monitoring address, can’t necessarily work out addressees/devices.
* Juan Carlos: perhaps the value of having those resolvable is also that it allows faster reconnection?
* Paul Lambert: seems like this method would allow randomization inside the connection, i.e. during a session
* Paul Lambert: this seems like an interesting solution. However, it is not obvious how cumbersome it would be if there are multiple links
* Piers: This is a good point
* Antonio de la Oliva: Also, implications on SDN should be considered, as many times a MAC address is used to match packets.
* Juan Carlos: It has been pointed out before that randomizing all MAC addresses should not be the proposed solution. A threat analysis is needed to identify the cases where it makes sense, for instance do it at the STA and not at the AP, so that Wi-Fi Geolocation is not disturbed, etc.

**Next steps**

* EC Privacy SG updates to be presented at 802.1/802.3 interim meeting in Ottawa, Sep 8-9
* EC Privacy SG updates to be presented at Wireless 802 interim meeting in Athens, week of Sep 15
* Group will continue call for contributions/proposals and scope of recommended practice
* Antonio: Should probably ask 802 WGs about issues with MAC address randomization proposal.
* Dan: if certain 802 technologies don’t need/want MAC address randomization, should consider maybe work out earlier rather than later?
* Juan Carlos: propose discussing further this topic at Athens meeting, and report back to the group.
* Upcoming meetings
  + 1 October 2014 (10:00 AM ET), Teleconference
  + 22 October 2014 (10:00 AM ET), Teleconference
  + November 2-7, 2014, IEEE 802 Plenary meeting in San Antonio, TX, USA

**AOB**

* None

**Adjournment**

* Meeting adjourned at 11:05, EDT