IEEE 802 EC SG
Privacy Recommendation

|  |
| --- |
| Minutes of EC Privacy Recommendation SG Teleconference October 22nd, 2014 |
| Date: 22-October-2014 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Antonio de la Oliva | University Carlos III of Madrid |  |  | aoliva@it.uc3m.es |
| Karen Randall | Randall Associates |  |  | karen@randall-consulting.com  |
| Juan Carlos Zúñiga | InterDigital |  |  | juancarlos.zuniga@interdigital.com  |

Abstract

Minutes of the EC Privacy Recommendation SG teleconference on Wednesday, October 22nd, 2014.

**Wednesday, October 22nd, 2014**

Chair: Juan Carlos Zuniga

Recording secretary: Antonio de la Oliva and Karen Randall

**Call to order**

* Meeting called to order on at 10:05am EDT.
* The chair slides were posted:
* <https://mentor.ieee.org/privecsg/dcn/14/privecsg-14-0013-00-ecsg-oct-22-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**

* Antonio de la Oliva and Karen Randall volunteered to take notes

**Roll call**

|  |  |
| --- | --- |
| **Name**  | **Affiliation**  |
| Juan Carlos Zuniga (Chair) | InterDigital |
| Fabio Giust | IMDEA |
| Alissa Cooper | Cisco |
| Walter Pienciack | IEEE SA |
| Lily Chen | NIST |
| Dan Harkins | Aruba Networks |
| Soo Bum Lee | Qualcomm |
| Philip Barber | BMT |
| Piers O’Hanlon | Oxford Internet Institute |
| Karen Randall | Randall-Consulting |
| Paul Nikolich | IEEE EC |
| Dan Romascanu | Avaya |
| Rene Struik | Struik Security Consultancy |
| Hiroki Nakano | Kyoto University |
| Roger Marks | EthAirNet Associates |
| Mark Rison | Samsung |
| Carlos Bernardos | UC3M |
| Antonio de la Oliva | UC3M |
| Brian Weis | Cisco |

**Agenda**

* Welcome
* Chair's slides
	+ IEEE Slides
	+ Call meeting to order
* Group's updates
	+ 802c PAR
	+ IETF MAC address randomization trial status – wiki page
* 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. Implications of MAC address changes
	6. Other
* Next Steps

**Review of minutes**

* Juan Carlos: Approval of minutes from Oct 1, 2014 teleconference will be delayed until the face to face meeting in San Antonio.

**Group’s updates**

* **IEEE 802c PAR**

Juan Carlos reported that the email discussions have shown a number of concerns regarding the IEEE 802c PAR.

He also reported that due to the number of comments, there will be an 802-level meeting during the upcoming 802 plenary meeting, on Monday 3 Nov 2014 at 9:30 PM, to discuss the PAR.

The following considerations/questions from the EC Privacy SG point of view were raised:

* Is there a minimum number of bits required for a WiFi deployment with random MAC addresses?
* Do we need to consider co-existence scenarios, e.g. with IoT?
* Does the group want to submit PAR comments (potentially late for EC’s deadline)?

Paul Nikolich: When is the first session of the EC SG scheduled?

Juan Carlos: The first session is scheduled for Tuesday evening, which is after the EC deadline for submitting comments. If the group decides to submit comments I will request at the EC opening an extraordinary extension to submit comments by Wednesday morning.

Dan: number of bits depends on the size of network to reduce the probability to collision. Regarding the questions, I support the idea of submitting PAR comments from the EC SG point of view.

Roger: preference over using the whole local space. Possibility is to get 48-4=44 bits, decreasing. 802c is thought for IoT, this is a very different scenario from what we do.

Roger Marks: 1) PAR itself is not proposing to develop a protocol, but really talking about a formality/structure to divide the local space of MAC addresses that has the local bit set. Suggested that if this is done, could enable some protocols that run on the subset of the space. The PAR itself is focused on using CID (24 bit parameter) established by IEEE RAC. Does not preclude some other subdivision. But as PAR is written, x=24. Local space is local. Should be able to reach some consensus. Folks driving PAR are focused data center applications; very different from Wi-Fi.

Can the Exec Committee receive comments after deadline on Tuesday? Hope so. This SG does not meet until after the deadline, so would like to submit PAR comments after the SG meets.

We have two possible points: Deployment and coexistence. The group would like to do comments to the PAR so Juan Carlos will try to talk with the EC to accept late comments.

Rene asked for more information regarding 802c. Juan Carlos indicated that there is a presentation with more information in an email from Max Riegel, it can be found in the privacy archive.

* **IETF MAC address randomization trial status – wiki page**

Juan Carlos reported that there have been discussions with IETF NOC about the trial and that the plan is to go ahead with it. At the moment, client MAC randomization tool need to be identified and docuemented to allow as many people as possible to participate in the trial.

Separate SSID 🡪 Separate VLAN, DHCP, Switching and AAA infrastructure so don’t interfere with the main meeting LAN. Use only 2.4GHz and different credentials will be needed.

Require a DHCP client name/ID per user – to keep track of what’s going on so can debug and identify potential issues.
Statistics to be collected:

network: # associations in this SSID, DHCP logs (MAC, DHCP client ID, time/date), DHCP pool size in time, Switch table size in time, AAA logs

client: MAC address usage log, and DHCP client name/ID

Question re: how to set DHCP client name/ID; it is a configuration parameter to set (e.g., on MAC – it’s under Advanced Networking).

Probably worth documenting in the Wiki how to do this.

Wiki page required to register users and keep a log of used MAC addresses

* **Presentation - MAC experiments and Wiki procedures– Fabio Giust, Antonio de la Oliva, Carlos Bernardos (University Carlos III of Madrid – UC3M)**

<https://mentor.ieee.org/privecsg/dcn/14/privecsg-14-0015-00-0000-mac-experiments-and-wiki-procedures.ppt>

Fabio presented for the group. He outlined the Wiki status (e.g, tests already performed for MAC randomization and the results). Options for the type of MAC generated by the tool: Manually set, Random set, Number of changeable bits.

The table on the wiki page is a framework that collects the test information and results and documents notes and usage instructions. For the Wiki page:

* Registered users only can post new content
* Non-registered users can only browse the wiki
* Registrations are moderated by the wiki’s admin

Assess whether allow other OS (e.g., MAC OS or Windows) to participate in the trial.

Expect to provide an update by end of the week.

Piers – what’s the plan for the actual output? What will it be used for? Tool applicability is still questionable depending on OS, etc.

JC – provide as many guidelines as possible to participate in the trial. Outcome – gather all the statistics that are meaningful. Once all the information is collected, a report can be generated.

* **Presentation - Threat Model for Privacy at Link Layer – Juan Carlos Zuniga (InterDigital) and Alissa Cooper (Cisco)**

<https://mentor.ieee.org/privecsg/dcn/14/privecsg-14-0014-00-0000-802-privacy-threat-model.pptx>

Juan Carlos and Alissa were asked at the IEEE-IETF Exec meeting to do a joint effort and develop a threat model for IEEE 802 protocols. They presented a draft threat model for IEEE 802 protocols based on the latest IETF privacy documents.

Alissa commented on privacy “attacker” and security “attacker.” A privacy attacker is not necessarily the same entity as a security attacker. The attacks may be different, so there may need to be some distinction or clarification between the two entities. JC encouraged the members of the SG to look at the presentation and/or references and provide feedback.

Rene: Seems like the scope is too broad. Perhaps the group should focus on the tangible issues that have been found (e.g. surveillance) and not waste time in other less effective solutions.

Alissa and Juan Carlos explained that the threat model was supposed to be generic, and that the actual issues/risk in 802 protocols, as well as the proposed solutions, are still to follow up after the model is developed.

* **Presentation – Overview of Privacy in 802.16 – Philip Barber (BMT)**

<https://mentor.ieee.org/privecsg/dcn/14/privecsg-14-0012-00-0000-overview-of-privacy-in-802-16.pptx>

Phil presented the privacy features that have been introduced in 802.16m-2011. He explained that Privacy was achieved through near total replacement of the use of MAC Address (MAC-48/EUI-48) as the AMS identifier in AMS-ABS communications in both data plane and management/control plane. It was replaced with a transitory, 12-bit Station Identifier (STID) on AMS STID assigned from a managed number pool by the ABS. Replaced with ABSID (24-bit 802.16 Operator ID + 24-bit operator programmable number) on ABS.

Station Identifier (STID) assigned on a per-session basis. Station ID would persist. Always a network managed number space. On ABS: operator ID.

uniquely identify the AMS in AMS-ABS communications only within that space.

privacy process: IEEE 802.16 preserved the MAC-48/EUI-48 provided during the handshake. During handshake, given a STID, encrypted.

In summary, IEEE 802.16.1 defined the use of transitory, randomly assigned temporary addresses, the suppression of identifiers embedded in the data stream, and ciphering and integrity protection provide a combination of methods to improve privacy protection. Overall it is the combination of management/control plane and data plane techniques that provide the method of IEEE 802.16.1 privacy protection.

A WORD presentation with more detail will also be uploaded to the mentor document site.

Piers – sometimes the MAC address ciphered. PSK? AMS nonce passed during the initial handshake.

Yes, if intercept nonce, then would be able to decode

Lily – handshake can happen in diff layer?

no, purely at layer 2. Management control message at layer 2 contains nonce. message not protected.

Lily – if that is not protected, how secure it the key?

Phil – protected only to the extent that the malicious user had to have listened. Even if could get nonce, then would get the MAC address, but not the relationship between the STID and the MAC address. During the initial exchanges, get temporary ID assigned. Only at the conclusion of the authentication process would install station ID.

Dan H – why didn’t use a random MAC address? then post-authentication, link?

Phil – Not sure of details. There was some discussion. This is what the group decided to do.

Are there IEEE 802.16.1implementations? His understanding is that there are.

**Next steps**

Juan Carlos reminded the group of the 2 scheduled Privacy EC SG sessions at the upcoming 802 Plenary meeting, on Tuesday 4 and Thursday 6 November, both from 7:30 PM to 9:30 PM.

The plan will be to report the Executive Committee during the closing plenary about the progress in the SG, and request an extension to the SG for one more cycle (until March 2015) to work on a PAR.

**AOB**

* None

**Adjournment**

* Meeting adjourned at 11:35am EDT