**IEEE P802.15**

**Wireless Personal Area Networks**

|  |  |  |
| --- | --- | --- |
| Project | IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs) | |
| Title | IG SEC Minutes of the May 2014 Meeting | |
| Date Submitted | 15 May, 2014 | |
| Source | Tero Kivinen INSIDE Secure Eerikinkatu 28  FI-00180 Helsinki  Finland | Voice: +358 20 500 7800 Fax: +358 20 500 7801 E-mail: kivinen@iki.fi |
| Re: | IG SEC Minutes of the May 2014 meeting in Kona, HI | |
| Abstract | IG SEC Minutes of the May 2014 meeting in Kona, HI | |
| Purpose | Official Minutes | |
| Notice | This document has been prepared to assist the IEEE P802.15. It is offered as a basis for discussion and is not binding on the contributing individual(s) or organization(s). The material in this document is subject to change in form and content after further study. The contributor(s) reserve(s) the right to add, amend or withdraw material contained herein. | |
| Release | The contributor acknowledges and accepts that this contribution becomes the property of IEEE and may be made publicly available by P802.15. | |

# Wednesday May 14th 2014, AM1 session

Chair Tero Kivinen (INSIDE Secure) called the meeting to order at 08:07.

Chair presented the opening slides 15-14-0311-00 and called the group's attention to the IEEE patent policy and made a call for notification of essential patents. There were no responses in the meeting.

Tero Kivinen presented the 15-14-0299-00 presentation about the frame counter issues. There was some discussion about the impact on the old devices and what it means when using TSCH where the frame counter is based on the time. The group agreed on proposed solution, and decided that the next steps would be to go through the 802.15.4 draft document and see what changes the proposed solution requires in the document. Doing that will require to be able to see the actual draft document first, which will be available only after the Kona meeting. This proposed solution will also cause some changes to the inbound and outbound state machines.

While doing that it was asked what is the difference of List of XXX and Set of XXX in the MAC PIB. The 802.15.4 specification do not have any definition of those words, and whether there is any differences with them. One difference might be whether it is ordered list or just set of items (without order and perhaps even without duplicates). The use of “Set of 16 octets” when describing the key is not supportive to that. This is something that will be taken to the maintenance group or the editor to clear up.

The meeting was recessed at 09:30.

# Wednesday May 14th 2014, PM2 session

The Chair called the meeting to order at 16:02.

Tero Kivinen started by presenting the parts of closing reports 15-14-0315-00 which contained the two problems in security of the 802.15.4e. The first issue is that section 7.3.2 of the 802.15.4e describes that the Nonce might be generated also using the macShortAddress. This is not safe unless the uniqueness of the nonce is guaranteed otherwise. When using the TSCH mode the frame counter is globally unique incrementing Absolute Slot Number (ASN) which will make the nonce unique even when macShortAddress is used to generate the nonce, but when TSCH is not used then macShortAddress cannot be used. It was not clear if there is any benefits for deviating the normal 802.15.4 nonce generation in 802.15.4e in this aspect. The 802.15.4 always specifies that macExtendedAddress is used to generate the nonce. There was long discussion about the issue, and it was agreed that macShortAddress could be used when using TSCH, but the text describing the how to generate nonce for the 5-octet frame counter, does not limit its use only for the TSCH. Also the text does not describe how the short address should be padded and positioned when placed in the 8-octet field. Also there was typo TCSH in the section.

The group discussed two possible ways to fix this issue:

- Remove the text saying that macShortAddress can be used when generating nonce.

- Reformat the text so it is clear that macShortAddress can only be used in the TSCH mode.

The next problem noticed in the 802.15.4e was the Frame Counter Suppression feature. This is related to the enhanced acknowledgments. The 802.15.4e says that when sending back enhanced acknowledgment, it copies the security fields of the inbound frame, and uses the same frame counter that was used for inbound packet when sending enhanced acknowledgment, and sets the frame counter suppression bit to 1 to specify that frame counter is omitted from the actual enhanced acknowledgment frame sent.

This is not safe, as this will cause the sender of the enhanced acknowledgment to reuse his frame counter for multiple packets. Firstly it will use it when sending his own packet with the same frame counter out, and lately every time any of peers it is talking to sends packet to him which have that same frame counter and who request enhanced acknowledgment.

The frame counter suppression section 7.4.1.3 lists several ways it can be used: global unique counter, using ASN for TSCH, or using the frame counter of the inbound frame to be ACKed. Global unique counter which is shared by all the peers might be bit hard to implement, as the recipient of the enhanced acknowledgment frame needs to know which value the sender used for that.. Using ASN in TSCH mode for the frame counter and suppressing it from the packet do work, as ASN is globally known by both peers. The last part saying that using the frame counter of the inbound frame is not secure, and it should be removed.

The group discussed three possible ways to fix this issue:

- Remove the whole Frame Counter Suppression feature

- Make sure the different nonce is always generated even when same frame counter is used, for example by modifying the Nonce generation so one extra bit is set in the security level part that will be different for the enhanced acknowledgment compared to the normal data packet.

- Specify that the Frame Counter Suppression feature can only be used in the TSCH mode, i.e. where the frame counter is global unique counter ASN, and in all other case it cannot be used, and enhanced acknowledgment frames must be sent out using normal frame counter rules.

It was agreed that both of these issues are sent to the SC-maintenance group as comments, so they can be taken in to account in the 802.15.4 draft as soon as possible (Action point to Chair).

The final agenda item for the meeting as to agree on the first teleconference. The first teleconference will be 2014-05-27 17:00 UTC (20:00 in Helsinki, 13:00 in New York, and 10:00 in San Francisco).

The meeting was adjourned at 17:20.