Project: IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs)

Submission Title: IG SEC Closing Report for May 2014 Session
Date Submitted: 14 May, 2014
Source: Tero Kivinen, **Company:** INSIDE Secure
Address: Eerikinkatu 28, FI-00180 Helsinki, Finland
Voice:+358 20 500 7800, **FAX:** +358 20 500 7801, **E-Mail:** kivinen@iki.fi

Re: IG SEC Closing Report for May 2014 Session

Abstract: IG SEC Closing Report for May 2014 Session

Purpose:

IG SEC Closing Report

Tero Kivinen

Kona, HI

May 14, 2014

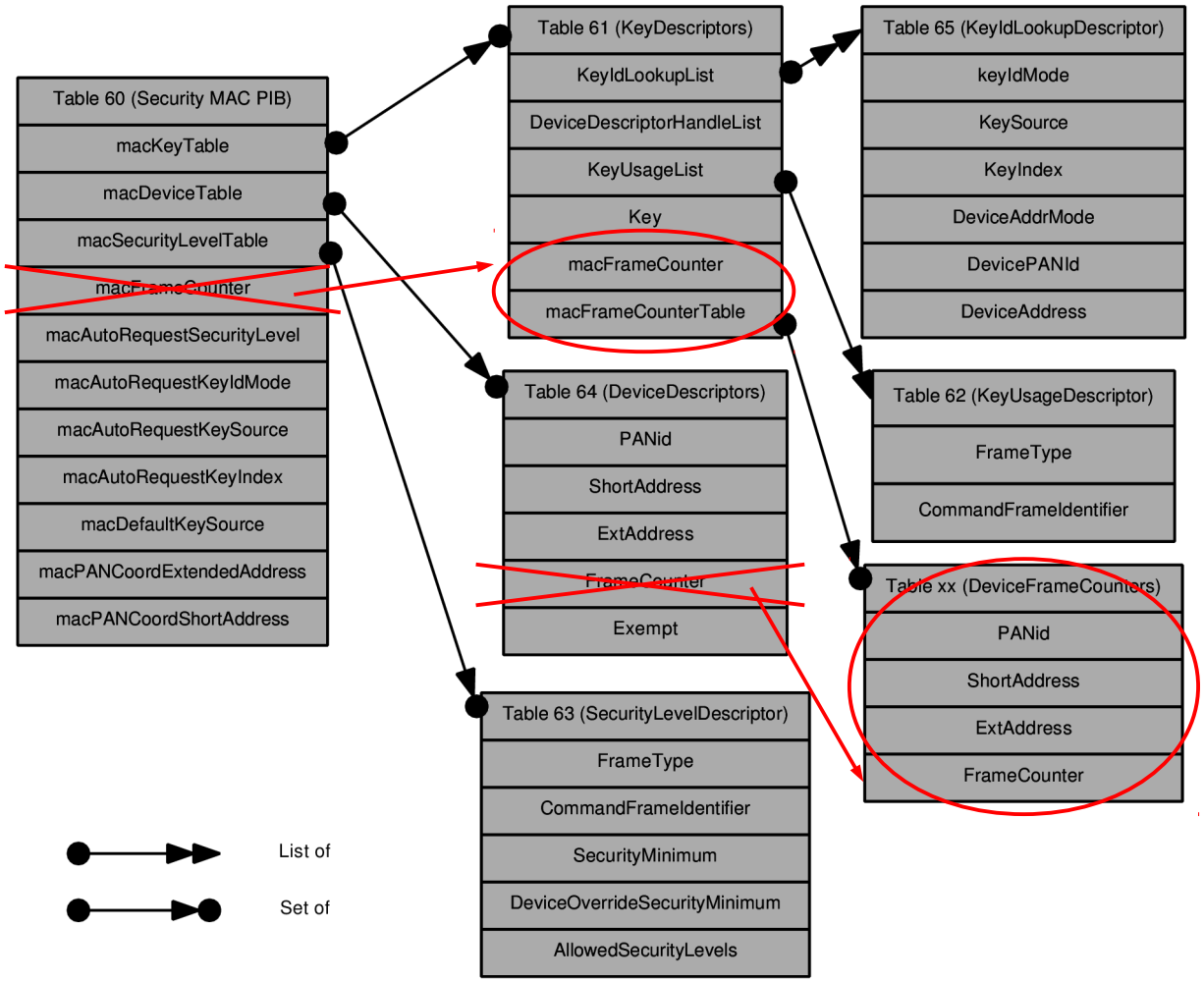
Meeting Goals

- IG SEC
  - Wednesday 14 May, AM1
    - Review of 802.15.4 Frame Counter security issue and discussion
  - Wednesday 14 May, PM2
    - Quantify the issue(s) and security issues and enhancements

Wednesday 14 May AM1

- FrameCounter presentation 15-14-0299-00
  - Agreed on the proposed solution
  - Need to check what changes that requires in the actual document
    - Before that we need to have the document, so we can see what needs to be changed.

Proposed Solution



Issue to Consider

- How does this affect inbound / outbound state machines
- How does this affect the frame counter in the TSCH (based on time)

Other things

- There is some weird text in the 802.15.4 specification:
  - Set of XXX, List of XXX
    - What is difference between them in PIB
  - Set of octets?

Wednesday 14 May PM2

- Enhanced ACK
- Going through the section 7 for sets / lists etc.

Problems in 802.15.4e

- Nonce Generation
  - Section 7.3.2 says that the Nonce might be generated using macShortAddress. The base 802.15.4 says you always use macExtendedAddress.
    - Using macShortAddress is NOT SAFE, as the short addresses might get reused (unless frame counter is using unique value like ASN), which would violate the principle that Nonce MUST be unique.
    - FIX: Remove all text saying using macShortAddress is possible when generating Nonce, short address can still be used in the actual packets sent out, I.e in the bytes on the wire.
    - Or, at least say it can be only used in TSCH mode

Problems in 802.15.4e

- Frame Counter Suppression
  - Section 7.4.1.3 has feature called Frame Counter Suppression, where the frame counter for the enhanced ack is taken from the frame we are ACKing.
    - This is NOT SAFE, as again the Nonce might get reused.
    - Fixes:
      - Remove whole Frame Counter Suppression feature
      - Or, make sure different nonce is generated always using some other methods (change nonce layout by adding bit for it (for example in security level part))
      - Or, say that Frame Counter Suppression can only be used in TSCH mode where the Frame Counter is global (or ASN), and otherwise use the normal macFrameCounter like sending normal packets, i.e. remove the last “or in the case of in enhanced acknowledgement, the frame counter of the frame being acknowledged” and add text about using normal macFrameCounter otherwise.

Teleconferences

- First teleconf:
  - 2014-05-27 17:00 UTC
    - Helsinki: 2014-05-27 20:00
    - New York: 2014-05-27 13:00
    - San Francisco: 2014-05-27 10:00