IEEE P802.11
Wireless LANs

Proposal selected Pseudo Code in LB88

Date: 2006-10-13

Author(s):

Name	Company	Address	Phone	email
David Cypher	NIST	100 Bureau Drive, Stop 8920	301 975 4855	david.cypher@nist.gov

Abstract

This contribution proposes a suggested resolution to the selected pseudo code in Letter Ballot 88; particularly clauses 8.7.2.3A and 8.7.2.4A. There are two proposed pseudo code, one for each clause. The suggested changes were too numerous and too complicated (i.e., font, indenting, reorganize, corrections, etc.) to explain to include as individual text IEEE 802.11 WG LB88 comments. Instead two comments were placed one for each clause with the recommended change to see this contribution.

Notice: This document has been prepared to assist IEEE 802.11. 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 grants a free, irrevocable license to the IEEE to incorporate material contained in this contribution, and any modifications thereof, in the creation of an IEEE Standards publication; to copyright in the IEEE's name any IEEE Standards publication even though it may include portions of this contribution; and at the IEEE's sole discretion to permit others to reproduce in whole or in part the resulting IEEE Standards publication. The contributor also acknowledges and accepts that this contribution may be made public by IEEE 802.11.

Patent Policy and Procedures: The contributor is familiar with the IEEE 802 Patent Policy and Procedures <http://ieee802.org/guides/bylaws/sb-bylaws.pdf>, including the statement "IEEE standards may include the known use of patent(s), including patent applications, provided the IEEE receives assurance from the patent holder or applicant with respect to patents essential for compliance with both mandatory and optional portions of the standard." Early disclosure to the Working Group of patent information that might be relevant to the standard is essential to reduce the possibility for delays in the development process and increase the likelihood that the draft publication will be approved for publication. Please notify the Chair <stuart.kerry@philips.com> as early as possible, in written or electronic form, if patented technology (or technology under patent application) might be incorporated into a draft standard being developed within the IEEE 802.11 Working Group. **If you have questions, contact the IEEE Patent Committee Administrator at <patcom@ieee.org>**.

8.7.2.3A Per-MPDU Rx pseudo-code for an MMPDU

```
if dot11RSNAEnabled = TRUE and Bit 6 of RSNA Capability Field is set then
      if the Protected Frame subfield of the Frame Control Field is zero then
            if Protection for TA is off for Rx then
                  Receive the unencrypted MPDU without protections
            else
                  Discard the frame body without indication to LLC
            endif
      elseif Protection is true for TA then
            if ((MPDU has individual RA and Pairwise key exists for the
      MPDU’s TA) or (MPDU has a broadcast/multicast RA and network type is
      IBSS and IBSS GTK exists for MPDU’s RA)) then
                  if key is null then
                        discard the frame body
                  elseif entry has an AES-CCM key then
                        decrypt frame using AES-CCM key
                        if the integrity check fails then
                              discard the frame
                              increment dot11RSNAStatsCCMPDecryptErrors
                        endif
                  elseif entry has an AES-128-CMAC key then
                        check integrity of the frame using AES-128-CMAC key
                        if the ICV fails then
                              discard the frame
                              increment dot11RSNAStatsCMACICVErrors
                        endif
                  else
                        discard the frame body
                  endif
            elseif GTK for the Key ID does not exist then
                  discard the frame body
            elseif GTK for the Key ID is null then
                  discard the frame body
            elseif GTK for the Key ID is a CCM key then
                  decrypt frame using AES-CCM key
                  if the integrity check fails then
                        discard the frame
                        increment dot11RSNAStatsCCMPDecryptErrors
                  endif
            elseif the IGTK for the Key ID is an AES-128-CMAC key then
                  integrity check the frame using AES-128-CMAC decryption
                  if the ICV fails then
                        discard the frame
                        increment dot11RSNAStatsCMACICVErrors
                  endif
            endif
      else
            discard the frame body
      endif
endif
```

Formatted: Font: Bold

Formatted: Indent: Left: 1"

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

Deleted: discard the frame if the integrity check fails and increment dottRSNAStats-CCMPDecryptErrors¶

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

Deleted: discard the frame if the ICV fails and increment dot11CMACICVErrors¶

Formatted: Indent: Left: 1"

Formatted: Indent: Left: 1"

Formatted: Indent: Left: 1"

Formatted: Indent: Left: 1"

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Indent: Left: 1"

Formatted: Font: Bold

Deleted: discard the frame if the integrity check fails and increment dot11RSNAStatsCCMPDecryptErrors¶

Deleted: **discard the frame if the ICV fails and increment dotCMACICVErrors**

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold, Italic

8.7.2.4A Per-MDPU Rx pseudo-code

```
if dot11RSNAEnable = TRUE and Bit 6 of RSNA Capability Field is set then
      if the frame was not protected then
            Receive the MMPDU unprotected
      else //Have a protected MMPDU
            if Pairwise key is an AES-CCM key then
                  if its MPDUs had sequential PNs or it consists of only one MPDU then
                        Accept the MMPDU
                  else
                        discard the MMPDU as a replay attack
                        increment dot11RSNAStatsCCMPReplays
                  endif
            elseif Pairwise key is an AES-128-CMAC key then
                  if its MPDUs had sequential PNs or it consists of only one MPDU then
                        Accept the MMPDU
                  else
                        discard the MMPDU as a replay attack
                        increment dot11RSNAStatsCMACReplays
                  endif
            endif
      endif
endif
```

Formatted: Font: 10 pt, Bold

Deleted: Accept the MMPDU if its MPDUs had sequential PNs (or if it consisted of only one MPDU), otherwise discard the MMPDU as a replay attack and increment dot11RSNAStatsCCMPReplays

Formatted: Font: 10 pt, Bold

Formatted: Font: 10 pt, Bold

Formatted: Font: 10 pt, Bold

Formatted: Font: 10 pt, Bold

Formatted: Font: 10 pt, Bold

Formatted: Font: 10 pt, Bold

Formatted: Font: 10 pt, Bold

Formatted: Font: 10 pt, Bold

Formatted: Font: 10 pt, Bold

Formatted: Font: 10 pt, Bold

Formatted: Font: Bold

Formatted: Font: Bold

Deleted: Accept the MMPDU if its MPDUs had sequential PNs (or if it consists of only one MPDU), otherwise discard the MMPDU as a replay attack and increment dot11RSNAStatsCMACReplays

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

Formatted: Font: Bold

References:

IEEE 802.11 WG LB88: IEEE P802.11w/1.0, October 2006-10-13
IEEE P802.11-REVma-D7.0-redline.pdf