IEEE P802.11
Wireless LANs

|  |
| --- |
| S1G MAC Resolution to CID5016 |
| Date: 2020-09-17 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| David Goodall | Morse Micro |  |  | dave@morsemicro.com |
|  |  |  |  |  |

Abstract

This submission shows

* 1 CID: 5016

Revisions:

* Rev 0: Initial version of the document.
* Rev 1: Updated PV1 test vectors (with intermediate values).

# CID 5016

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **CID** | **Clause** | **Page.Line** | **Comment** | **Proposed Change** |
| 5016 | J.6.4 | 4528.64 | The nonce values for the CCMP-128 PV1 test vectors 1, 2 and 3 appear to be incorrect. Section 12.5.3.3.4 Construct CCM nonce indicates that bits 0..3 of the Nonce Flags subfield shall be set to the priority value of the MPDU. For all PV1 test vectors the priority value is 3 (PTID/Subtype=3) so each example CCMP nonce should start with 0x23 as the first octet. | Correct the nonce values for the three PV1 test vectors and regenerate the resulting encrypted vectors. |

## Background

The text relating to nonce construction is:

* Construct CCM nonce(#2720)

The Nonce field occupies 13 octets, and its structure is shown in Figure 12-21 (Nonce field(#1406)(11ah)). The structure of the Nonce Flags subfield of the Nonce field is shown in Figure 12-22 (Nonce Flags subfield(11ah)).

|  |  |  |  |
| --- | --- | --- | --- |
|  | Nonce Flags | STA MAC Address Identified By A2 | PN |
| Octets: | 1 | 6 | 6 |
| * Nonce field(#1406)(11ah)
 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | B0         B3 | B4 | B5 | B6         B7 |
|  | Priority | Management | PV1 | Zeros |
| Bits: | 4 | 1 | 1 | 2 |
| * Nonce Flags subfield(11ah)
 |

(#4614)The Priority subfield shall be set to the priority value of the MPDU.

(#4614)The Management subfield shall be set to 1 if the MPDU is a Management frame and management frame protection is negotiated; otherwise, it shall be set to 0.

(#4614)The PV1 subfield shall be set to 1 for a PV1 frame; otherwise, it shall be set to 0.

(#4614)The Zeros subfield shall be set to 0.

(#4614)The STA MAC Address Identified By A2 subfield shall contain the Address 2 field from the MAC header for PV0 MPDUs and the MAC address identified by the A2 field in the MAC header for PV1 MPDUs (see 9.8.3.2 (Address fields)).

(#4614)The PN subfield shall contain the packet number, with PN0 in the last octet of the subfield.

## Discussion

Review of the PV1 related test vectors in J.6.4 (CCMP test vectors) indicates that the above has been followed except for the setting of the Priority subfield to the priority value of the MPDU. Therefore, the PV1 test vectors need to be regenerated with a corrected CCM nonce.

The regenerated test vectors have been supplied by Jouni Malinen (Qualcomm).

The test vector changes are consistent with the recent changes in <https://mentor.ieee.org/802.11/dcn/20/11-20-0877-02-000m-cr-pv1-security.docx>

# Proposed Resolution: CID 5016

**Revised.**

Instructions to Editor:

At D4.0 P4528L20, replace the current PV1 test vectors with the following:

***------------- Begin Text Changes ---------------***

BSSID: a2:ae:a5:b8:fc:ba

DA: 02:d2:e1:28:a5:7c

SA: 52:30:f1:84:44:08

Association ID: 7

Base PN: 123 (0x0000007b)

SC = 0x3380 (FragNum=0 SeqNum=824)

TID = 3

Key ID: 0

TK - hexdump(len=16): c9 7c 1f 67 ce 37 11 85 51 4a 8a 19 f2 bd d5 2f

PN = SC||BPN

PN (PN0..PN5) - hexdump(len=8): 80 33 7b 00 00 00 00 00

PV1 test vector #1:

Header compression used and A3 was previously stored at the receiver

FC=0x0061 (PV=1 Type=0 PTID/Subtype=3 From\_DS=0 More\_Fragments=0 Power\_Management=0 More\_Data=0 Protected\_Frame=0 End\_of\_SP=0 Relayed\_Frame=0 Ack\_Policy=0)

A1=a2:ae:a5:b8:fc:ba

A2=07 00 (SID: AID=7 A3\_Present=0 A4\_Present=0 A-MSDU=0); corresponds to 52:30:f1:84:44:08 in uncompressed header

Sequence Control: 80 33 (FN=0 SN=824)

A3 not present; corresponds to 02:d2:e1:28:a5:7c in uncompressed header

A4 not present

Plaintext Frame Header - hexdump(len=12): 61 00 a2 ae a5 b8 fc ba 07 00 80 33

Plaintext Frame Body - hexdump(len=20): f8 ba 1a 55 d0 2f 85 ae 96 7b b6 2f b6 cd a8 eb 7e 78 a0 50

CCMP AAD - hexdump(len=22): 61 10 a2 ae a5 b8 fc ba 52 30 f1 84 44 08 00 00 02 d2 e1 28 a5 7c

CCMP nonce - hexdump(len=13): 23 52 30 f1 84 44 08 00 00 00 7b 33 80

CCM B\_0 - hexdump(len=16): 59 23 52 30 f1 84 44 08 00 00 00 7b 33 80 00 14

CCM T - hexdump(len=8): 54 a0 f5 a5 58 c3 8b 98

CCM U - hexdump(len=8): f8 ca bc a8 6d ff 2c f8

CCMP encrypted - hexdump(len=20): 4c 53 53 ce ea fa 0d 5a 04 52 49 66 04 86 e1 68 41 59 e9 42

Encrypted Frame Header - hexdump(len=12): 61 10 a2 ae a5 b8 fc ba 07 00 80 33

Encrypted Frame Frame Body - hexdump(len=28): 4c 53 53 ce ea fa 0d 5a 04 52 49 66 04 86 e1 68 41 59 e9 42 f8 ca bc a8 6d ff 2c f8

Encrypted Frame FCS - hexdump(len=4): 9e 3d 21 65

PV1 test vector #2:

Header compression used and A3 was not previously stored at the receiver

FC=0x0061 (PV=1 Type=0 PTID/Subtype=3 From\_DS=0 More\_Fragments=0 Power\_Management=0 More\_Data=0 Protected\_Frame=0 End\_of\_SP=0 Relayed\_Frame=0 Ack\_Policy=0)

A1=a2:ae:a5:b8:fc:ba

A2=07 20 (SID: AID=7 A3\_Present=1 A4\_Present=0 A-MSDU=0); corresponds to 52:30:f1:84:44:08 in uncompressed header

Sequence Control: 80 33 (FN=0 SN=824)

A3=02:d2:e1:28:a5:7c

A4 not present

Plaintext Frame Header - hexdump(len=18): 61 00 a2 ae a5 b8 fc ba 07 20 80 33 02 d2 e1 28 a5 7c

Plaintext Frame Body - hexdump(len=20): f8 ba 1a 55 d0 2f 85 ae 96 7b b6 2f b6 cd a8 eb 7e 78 a0 50

CCMP AAD - hexdump(len=22): 61 10 a2 ae a5 b8 fc ba 52 30 f1 84 44 08 00 00 02 d2 e1 28 a5 7c

CCMP nonce - hexdump(len=13): 23 52 30 f1 84 44 08 00 00 00 7b 33 80

CCM B\_0 - hexdump(len=16): 59 23 52 30 f1 84 44 08 00 00 00 7b 33 80 00 14

CCM T - hexdump(len=8): 54 a0 f5 a5 58 c3 8b 98

CCM U - hexdump(len=8): f8 ca bc a8 6d ff 2c f8

CCMP encrypted - hexdump(len=20): 4c 53 53 ce ea fa 0d 5a 04 52 49 66 04 86 e1 68 41 59 e9 42

Encrypted Frame Header - hexdump(len=18): 61 10 a2 ae a5 b8 fc ba 07 20 80 33 02 d2 e1 28 a5 7c

Encrypted Frame Frame Body - hexdump(len=28): 4c 53 53 ce ea fa 0d 5a 04 52 49 66 04 86 e1 68 41 59 e9 42 f8 ca bc a8 6d ff 2c f8

Encrypted Frame FCS - hexdump(len=4): aa 07 71 93

PV1 test vector #3:

Type 3 frame from SA to DA(=BSSID) (i.e., no separate DA in this example)

FC=0x006d (PV=1 Type=3 PTID/Subtype=3 From\_DS=0 More\_Fragments=0 Power\_Management=0 More\_Data=0 Protected\_Frame=0 End\_of\_SP=0 Relayed\_Frame=0 Ack\_Policy=0)

A1=a2:ae:a5:b8:fc:ba

A2=52:30:f1:84:44:08

Sequence Control: 80 33 (FN=0 SN=824)

A3 not present; corresponds to 02:d2:e1:28:a5:7c in uncompressed header

A4 not present

Plaintext Frame Header - hexdump(len=16): 6d 00 a2 ae a5 b8 fc ba 52 30 f1 84 44 08 80 33

Plaintext Frame Body - hexdump(len=20): f8 ba 1a 55 d0 2f 85 ae 96 7b b6 2f b6 cd a8 eb 7e 78 a0 50

CCMP AAD - hexdump(len=22): 6d 10 a2 ae a5 b8 fc ba 52 30 f1 84 44 08 00 00 02 d2 e1 28 a5 7c

CCMP nonce - hexdump(len=13): 23 52 30 f1 84 44 08 00 00 00 7b 33 80

CCM B\_0 - hexdump(len=16): 59 23 52 30 f1 84 44 08 00 00 00 7b 33 80 00 14

CCM T - hexdump(len=8): 76 b9 1f 36 2a 0c e0 e8

CCM U - hexdump(len=8): da d3 56 3b 1f 30 47 88

CCMP encrypted - hexdump(len=20): 4c 53 53 ce ea fa 0d 5a 04 52 49 66 04 86 e1 68 41 59 e9 42

Encrypted Frame Header - hexdump(len=16): 6d 10 a2 ae a5 b8 fc ba 52 30 f1 84 44 08 80 33

Encrypted Frame Frame Body - hexdump(len=28): 4c 53 53 ce ea fa 0d 5a 04 52 49 66 04 86 e1 68 41 59 e9 42 da d3 56 3b 1f 30 47 88

Encrypted Frame FCS - hexdump(len=4): ff a5 82 36

***------------- End Text Changes ------------------***

**References:**