|  |
| --- |
| Proposed Resolution for Some Security CIDs |
| Date: 2013-09-17 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| René Struik | Struik Security Consultancy | Toronto ON | +1 (415) 690-7363+1 (647) 867-5658Skype: rstruik | rstruik.ext@gmail.com |

Abstract

This document discusses some security-related LB#198 comments related to D1.0 of the TGai specification.

**Summary sheet: Suggested resolution of a selection of comments from 13/1076r2:**

|  |  |  |
| --- | --- | --- |
| **CID#** | **Resolution** | **Brief rationale** |
| 2202 | Reject | Comment on nonce use, already discussed at length with D0.5 |
| 3002 | Reject | Comment on nonce use, already discussed at length with D0.5 |
| 3154 | Reject | Duplicate of #3002 |
| 3193 | Reject | Duplicate of #3193 |
| 3089 | Reject | Comment on nonce use, already discussed at length with D0.5. Commenter already gets extensibility he wants, fragmentation irrelevant |
| 2201 | Accept in Principle | Small textual changes to support GCM mode, currently in *draft* 802.11ac |
| 3003 | Accept in Principle | Virtually same as #2201 |
| 3155 | Accept in Principle | Duplicate of #3003 |
| 3194 | Accept in Principle | Duplicate of #3003 |
| 2986 | Accept | Add cross-reference to section on key usage in 802.11-2012 |
| 3245 | Accept in Principle | Eradicate all FILS re-association language |

**DETAILS: Suggested resolution of a selection of comments from 13/1076r2:**

**CID #2202:** (Dan Harkins) 11.11.2.7, p. 107, l. 32:

Do not use fixed nonces in AEAD schemes. Adopt the AEAD scheme from 11-13/0806r2.

Suggested resolution: Reject.
Motivation: The security of the CCM mode of operation requires that nonces are not reused with the same key. This is indeed the case with Draft D1.0 (as this was with Draft D0.5, when this comment was already discussed in great detail). This also fully conforms to the referenced NIST specification (see Section 5.3 of NIST SP 800-38C).
Further explanation for the commenter: Draft D1.0 only introduces one new use of the CCM mode of operation (in Clause 11.11.2.5) and this mode is invoked precisely once in each direction during key confirmation (Clause 11.11.2.4): once from STA to AP (Association Request) and once from AP to STA (Association Response). Since the two key confirmation messages use different nonces and the key KEK2 is only used during key confirmation and "freshly" generated at each invocation of the FILS protocol (in Clause 11.11.2.3), nonce reuse does not occur. Please note that the nonces used by either party are in fact counters, where STA uses as counters the even integers counting up from zero and where AP uses as counters the odd integers counting down. Since each side only uses the counter once, this comes down to using the counters 0 and 2104-1, respectively. As a final note, key confirmation messages remain unsecured frames in the sense of 802.11-2012, so are not impacted by 802.11-2012 frame fragmentation (as defined in Clause 9.2.7 hereof).

**CID #3002:** (Michael Montemurro) 11.11.2.7, p. 107, l. 32:

Fixed nonces, mistake.

Adopt AEAD scheme in 11-13/0806r2

Suggested resolution: Reject.
Motivation: see CID #2202.

**CID #3154:** (Richard Kennedy) 11.11.2.7, p. 107, l. 32:

Fixed nonces, mistake.

Adopt AEAD scheme in 11-13/0806r2

Suggested resolution: Reject.
Motivation: see CID #3154, of which this comment is a duplicate.

**CID #3193:** (Roger Durand) 11.11.2.7, p. 107, l. 32:

Fixed nonces, mistake.

Adopt AEAD scheme in 11-13/0806r2

Suggested resolution: Reject.
Motivation: see CID #3154, of which this comment is a duplicate.

**CID #3089:** (Paul Lambert) 11.11.2.5, p. 106, l. 47:

The usage of the CCM algorithm prevents any future extensions or fragmentation approaches in this part of IEEE 802.11. Adopt solution in .: IEEE 802.11-13/0806r2 or deine the usage of the nonce values as counters

Suggested resolution: Reject.
Motivation: see CID #2202. In particular, please note that key confirmation messages remain unsecured frames in the sense of 802.11-2012, so are not impacted by frame fragmentation and that the nonce values are already counters (where each counter is only used once).

**CID #2201:** (Dan Harkins) 11.11.2.5, p. 106, l. 47:

11ai follows 11ac, it should take into account changes that will be made to the standard by the time it passes sponsor ballot

No, AES-CCM is not the "only such scheme specified". Furthermore, just saying "AES-CCM" is ambiguous. If the first sentence is true then the second sentence should be removed. And when you remove it, get rid of "the following instantiation" too.

Suggested resolution: Modified resolution (accept in principle):

Motivation: While this draft is an amendment based on IEEE 802.11mc/D1.0, IEEE P802.11ad-2012., IEEE P802.11ac/D5.0, and IEEE P802.11af/D5.0, officially the draft is an amendment of 802.11-2012, which only specifies CCM mode. This being said, it is expected that the GCM mode that is in Draft 802.11ac/D5.0, will ultimately make it as part of the standard.

Suggested to change 11.11.2.5, 11.11.2.6, 11.11.2.7 as follows:

***Clause 11.11.2.5 AEAD scheme***

*Change line 48 as follows:*

Change “the only such scheme specified is” to “the only such scheme specified with 802.11-2012”.

*Add the following paragraph at the end of 11.11.2.5:*

The draft specification 802.11ac/D5.0 also specifies the AES-GCM mode of operation, which is the GCM scheme specified in NIST SP 800-38D with the following instantiation:

* The block cipher shall be AES-128 (see FIPS Pub 197);
* The authentication tag length (parameter t) shall be set to t=16;
* The length of the nonce (called IV) shall be set to 96 bits.

Either mode of operation can be used, as indicated by the cipher suite.

***Clause 11.11.2.6 Encrypt and authenticate operation for FILS association frames***

*Change l. 7-9 as follows:*

Remove the qualifier “13-octet”.

(Note: thus, with CCM mode, one will use 13-octet nonces; with GCM mode, one will use 12-octet nonces.)

***Clause 11.11.2.7 Decrypt and verify operation for FILS association frames***

*Change l. 31-33 as follows:*

Remove the qualifier “13-octet”.

(Note: thus, with CCM mode, one will use 13-octet nonces; with GCM mode, one will use 12-octet nonces.)

**CID #3003:** (Michael Montemurro) 11.11.2.5, p. 106, l. 47:

AES-CCM, only scheme specified.

This is false, use wording that is agnostic and expandable.

Suggested resolution: Modified resolution (accept in principle).

Motivation: see CID #2201.

**CID #3155:** (Richard Kennedy) 11.11.2.5, p. 106, l. 47:

AES-CCM, only scheme specified.

This is false, use wording that is agnostic and expandable.

Suggested resolution: Modified resolution (accept in principle).

Motivation: see CID #3003, of which this comment is a duplicate.

**CID #3194:** (Roger Durand) 11.11.2.5, p. 106, l. 47:

AES-CCM, only scheme specified.

This is false, use wording that is agnostic and expandable.

Suggested resolution: Modified resolution (accept in principle).

Motivation: see CID #3003, of which this comment is a duplicate.

**CID #2986:** (Michael Montemurro) 11.11.2.3, p. 103, l. 31:

Circular reference "...shall be used in exactly the same way as same-named keys of IEEE 802.11-2012 (but now derived as specified above)."

Point to the specific clauses in IEEE 802.11-2012 that this sentence references.

Suggested resolution: Accept.

*Change l. 32 as follows:*

Change “of IEEE 802.11-2012” to “of IEEE 802.11-2012 (see 4.10.4.2)”.

**CID #3245:** (Santosh Ghanshyam Pandey) 11.11.2.6, p. 106, l. 60:

It would be dangerous for at least the KEK2 key to be used more than one time, because of the fixed Nonce values used for AES-CCM. When this is used for an Association Request/Response a part of FILS Authentication (as shown in Figure 4-21a), this seems safe enough. But the FILS Secure Container is also present in Reassociation Request and Response frames (see Clauses 8.3.3.7 and 8.3.3.8), so presumably the process described in Clause 11.11.2.6 is used to protect those frames. It is not clear how the KEK2 is used safely in that case.

Clarify how Encrypt and authenticate works for Reassociation Request and Response frames, as well as Decrypt and verify in clause 11.11.2.7.

Suggested resolution: Modified resolution.

Motivation: Both keys KCK2 and KEK2 are strictly temporary and are only used during key confirmation, as part of the FILS authentication protocol (see 11.11.2.3, l. 26-29). Thus, Clause 11 of D1.0 does not apply to any other protocol, so nor with Reassociation.

In fact, isn’t the entire text surrounding FILS Reassociation in error and shouldn’t it be killed off altogether here? After all: the whole point of FILS authentication is that now the entire authenticated key establishment procedure takes only four protocol flows (rather than the umpteen with 802.11-2012, which at the time may have motivated use of Reassociation as a “short-cut” for going through Authentication and Association again), so if one needs to reassociate, one should simply execute another run of the (four-pass) FILS protocol.

Suggested changes to 8.3.3.6, 8.3.3.7, 8.4.2.186.1, 8.4.2.186.2, 8.4.2.186.3, 8.4.2.186.4, 10.3.2, 10.3.5.1, 10.44.4, 10.44.4.1, 10.44.4.2

{Remove FILS reassociation altogether}

*Remove Clause 8.3.3.7 entirely.*

*Remove Clause 8.3.3.8 entirely.*

*Change Clause 8.4.2.186.1 as follows:*

Remove all occurrences of “Reassociation Request” or “Reassociation Response”.

*Change Clause 8.4.2.186.2 as follows:*

Remove all occurrences of “Reassociation Request” or “Reassociation Response”.

*Change Clause 8.4.2.186.3 as follows:*

Remove all occurrences of “Reassociation Request” or “Reassociation Response”.

*Change Clause 8.4.2.186.4 as follows:*

Remove all occurrences of “Reassociation Request” or “Reassociation Response”.

*Change Clause 10.3.2 as follows:*

Remove “Reassociation” from the state diagram portions relevant to FILS (State 5 to State 4 transition and vice-versa) in Fig. 10-6.

*Change Clause 10.3.5.1 as follows:*

Remove the sentence on l. 58-59 entirely (i.e., remove “Successful reassociation sets a FILS STA's state to State 4 and enables it to exchange Class 3 frames”).

*Change Clause 10.44.4 as follows:*

Remove all occurrences of “Reassociation Request” or “Reassociation Response” (including the one in the title).

*Change Clause 10.44.4.1 as follows:*

Remove all occurrences of “Reassociation Request” or “Reassociation Response”.

*Change Clause 10.44.4.2 as follows:*

Remove all occurrences of “Reassociation Request” or “Reassociation Response”.