|  |
| --- |
| Proposed Resolution for Some Security CIDs |
| Date: 2013-07-16 |
| 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 comments related to D0.5 of the TGai specification:

* Suggested resolution of comments with CID #1255, #1334, #1006, #1256, #1371, #1396;
* Pseudo-resolution of comments with CID # 1377, 1388, 1387 (since withdrawn by commenter)
* Suggested correction of resolution to comment CID #1384 (since seemingly mislabeled)

**SUMMARY SHEET:**

**#1: Suggested resolution of comments referred to as “unresolved comments” in 13/495r15:**

|  |  |  |
| --- | --- | --- |
| **CID** | **Resolution** | **Brief rationale** |
| 1255 | Accept | Add acronym AEAD mode |
| 1334 | Reject | Comment based on technical misconception re nonce requirements |
| 1006 | Reject | Comment based on technical misconception re nonce requirements (see #1334) |
| 1256 | Accept | Editorial glitch (copy-paste error from §11.11.2.6 to §11.11.2.7): swap STA and AP |
| 1371 | Accept | Delete note on Denial-of-Service risk |
| 1396 | Accept | Fix cross-reference |

**#2: Withdrawn comments:**

|  |  |  |
| --- | --- | --- |
| **CID** | **Resolution** |  |
| 1377 | Withdrawn | Exchange certificates with authentication frames, rather than association frames  |
| 1388 | Withdrawn | TBD – Currently unclear to commenter how one arrives at rMSK key |
| 1387 | Withdrawn | TBD – Currently unclear to commenter how this works |

**#3: Mislabeled resolution of comments in “2013-07-Geneva-03” in 13/495r15:**

|  |  |  |
| --- | --- | --- |
| 1384 | Accept/Principle | Other solution to identified problem adopted in May 2013 (viz. 13/478r2) |

**DETAILS #1: Suggested resolution of comments referred to as “unresolved comments” in 13/495r15**

**CID #1255:** What does AEAD stand for?

Define "AEAD" in Section 3.

Suggested resolution: Accept in principle.

* *Change 11.11.2.5, l. 1* as follows: Replace “The authenticated encryption with associated data scheme to be used” by “The authenticated encryption with associated data **(AEAD)** scheme to be used” (i.e., add AEAD as acronym);
* *Add the following acronym to Clause 3.2*: AEAD – Authenticated Encryption with Associated Data.

**CID #1334:** CCM should NOT be used with static nonces.

Suggest using SAE algorithm - or change specification to use random nonces.

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 D0.5. This also fully conforms to the referenced NIST specification (see Section 5.3 of NIST SP 800-38C).
Further explanation for the commenter: Draft D0.5 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. 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 #1006:** Choose a different AEAD scheme. Using CCM with static nonces is non-standard, and fragile (i.e. not robust).

Suggest using a scheme that does not need a nonce, such as SIV mode or using a scheme that is not reliant on nonce uniqueness for its security, like AES-CBC plus HMAC-SHA. Pages are 85-89 and the lines are basically the entirety of 11.11.2.4 and 11.11.2.5 but the web form would not let me enter multiple pages, or subclauses :-(

Suggested resolution: Reject.

Motivation: See CID #1334.

**CID #1256:** The association request frame should be received and deciphered by AP, not STA.

Change the sentence in line 3 on page 89 to the following: “The AEAD scheme of 11.11.2.5 shall be used with the 802.11 Association Request frame (for deciphering by AP) or with the 802.11 Association Response frame (for deciphering by STA), with the following instantiation”.

Suggested resolution: Accept.

**CID #1371:** (T) Clause 4.10.3.7, p. 8, l. 24-28: While fragmentation of FILS messages may result in mild prospect of denial-of-service attacks, this effect is, in fact, marginal at best. See also the analysis on Slides 8-10 of 13/201r6). Moreover, even if one uses X509 certificates with a certificate chain of, say, length three, this would normally (with prudent pick of certificate fields) not lead to a field of size ~2kB, unless one picks enormous ordinary DLP groups. While it is okay to have some cautionary language into the specification, the current language seems to overblow the effect of supersized FILS flows. Suggested remedy: Either quantify the fragmentation attack risk compared to DoS attacks if frame would not require fragmentation, thereby justifying the statement, or retract this statement from the draft specification.

Suggested remedy: Either quantify the fragmentation attack risk compared to DoS attacks if frame would not require fragmentation, thereby justifying the statement, or retract this statement from the draft specification.

Suggested resolution: Accept in Principle.

* Delete the Note.

**CID #1396:** (T) Clause 11.11.2.4, p. 85, l. 23-24: The cross-references are incorrect. Suggested remedy: Replace these by 11.11.2.6 and 11.11.2.7, respectively.

Suggested resolution: Accept.

**DETAILS #2: Withdrawn comments**

**CID#1377**: (TR) Clause 8.3.3.5, p. 22, Table 8-22: Certificates should be exchanged during key establishment (exchange of Authentication frames) and \*not\* during key confirmation (exchange of Association frames), for two reasons: (a) exchanging large objects, such as certificates, during key establishment has a very limited impact on potential fragmentation attacks; (b) exchanging certificates early allows implementation of certification to happen in parallel to wait cycles while the other device is computing a key, rather than forcing a serialized implementation, thus potentially resulting in shortened time latency of the entire FILS protocol; (c) exchanging certificates during key establishment allows computational tricks, whereby key computation and signature verification is carried out at the same time, thereby potentially significantly reducing the computational cost of public-key operations. With the current flows, this is not possible. Suggested remedy: Exchange certificates during key establishment, rather than key confirmation. To do so, the corresponding data elements have to be specified with the Authentication frame, rather than with Association frames.

Suggested resolution: Withdrawn by commenter (see e-mail Tue July 16, 2013, 4:20pm EDT).

**CID #1388:** (T) Clause 11.11.2.2.1, p. 82, l. 60: One should add some text that explains how the AP computes the rMSK key from the EAP-Finish/Re-Auth packet: after all, this key is used by both STA and AP for mutual "authentication". Suggested remedy: Elaborate on this.

Suggested resolution: Withdrawn by commenter (see e-mail Tue July 16, 2013, 4:20pm EDT).

**CID #1387:** (T) Clause 11.11.2.2.1, p. 82, l. 24: The FILS Identity element does not seem to be used with the FILS protocol option in question, since it is not forwarded to the TTP, nor used in the key derivation function. Suggested remedy: Explain the rationale of the FILS Identity element.

Suggested resolution: Withdrawn by commenter (see e-mail Tue July 16, 2013, 4:20pm EDT).

**DETAILS #3: Mislabeled resolution of comments in “2013-07-Geneva-03” in 13/495r15:**

**CID #1384:** (TR) Clause 11.11.2.4, p. 86, l. 4-5: The mechanism by which key confirmation messages are encrypted-and-authenticated is highly inflexible, since one always encrypts all information element in the Association Request and Response payloads, rather than allowing some flexibility in terms of which information elements are to be encrypted and authenticated, resp. only authenticated. In the January 2013 session, Qualcomm and Aruba Networks people made the argument that the vendor-specific element might need to be visible in some deployment scenarios, e.g., for network monitoring and management purposes. Thus, in that case enciphering should happen as an OFF-ON-OFF pattern that is currently not provided. Suggested remedy: Implement the authenticated encryption scheme in a more flexible fashion, along the lines of 13/311r1.

Record in 13/495r15:

REJECTED (TGai General: 2013-07-16 09:30:58Z) - 13/311r1 was discussed by Tgai and did not get sufficient support as it contains several technical changes that go beyond purely addressing the issue raised in this comment. A straw poll indicated that the group requested a condensed specific text with detailed proposed changes for further discussion. Such detailed text is not available.

Shouldn’t this be something else? (if not, it seems we have spent a lot of time discussing this topic, without positive outcome)

Suggested resolution: Accept in Principle.

Motivation: Various solutions to the identified problem were discussed, where the solution documented in 13/478r2 was adopted during the May 2013 meeting.