IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resolving the SAE comments from SB1 | | | | |
| Date: 2020-02-20 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HPE | 3333 Scott boulevard  Santa Clara, California,  The United States of America | +1 408 555 1212 |  |
|  |  |  |  |  |

Abstract

This submission proposes resolution to several SAE comments received in SB1.

**CID 4136**

Comment: In SAE, the plaintext password is used to calculate PWE. However, storing and passing plaintext password across protocol stacks may be vulnerable to malicious software.

Proposed Change: 1) Add a standard way for AP and client to agree on a method to map a plaintext SAE password to a random binary string, similar to the pass-phrase-to-PSK mapping in J.4.

2) Use the random binary representation of the password to calculate PWE.

Discussion: If the protocol stack has malicious software on it then passing anything, including a “random binary representation” of a password, will be vulnerable. Doing a passphrase to PSK mapping will not make any difference security-wise. One thing it will do, though, is make every single existing SAE implementation non-interoperable.

Resolution: Reject, the suggested change will not increase security of any system and will make older and newer SAE implementations not interoperable.

**CID 4190**

Comment: Should not use "element" for the security thing, should use "FFE", to avoid confusion with the frame component (see 9.4.2 Elements).

Proposed Change: As it says in the comment.

Discussion: “the security thing” is vague beyond reason. There are no line, page, or clause numbers associated with this CID and, not being a mind reader, I have no idea how to find “the security thing” to resolve this comment. The proposed change is nonsensical.

Resolution: Reject, no issue was identified and no valid change proposed.

**CID 4191**

Comment: Using the rejected groups list as the salt means the salt can be very short, so it's only a weak salt.

Proposed Change: Add a mechanism to allow devices to set up a non-weak initial (i.e. before any rejected groups get appended) salt

Discussion: There is no security vulnerability if a salt is known or short. If there are no rejected groups the salt is all zeros anyway which is a constant of all zeros, this is not a security vulnerability as the salt is used as a tweak in the KDF, not as a strengthener to a hashed password.

Resolution: Reject, there is no security vulnerability in the existing scheme.

**CID 4493**

Comment: "It is suggested that an Anti-Clogging Token field(#2534) not exceed 256 octets." -- euphemisms for "should" should not be used.

Proposed Change: Change to "An Anti-Clogging Token field(#2534) should not exceed 256 octets."

Discussion: This seems innocuous.

Resolution: Accept.

**CID 4654**

Comment: All references to "element"s (irrespective of case) that are about security objects should be FFE, to avoid confusion with 802.11 elements (9.4.2).

Proposed Change: As it says in the comment.

Discussion: This is essentially the same as CID 4190, but without the vague reference. Similarly, it provides no line, page, or clause numbers and fails to identify a problem. The proposed change is nonsensical. Suggesting that every use of a word be blindly changed is unreasonable as it would make changes that might not be desirable.

Resolution: Reject, it’s groundhog day in TGmd. See 4190.

**CID 4667**

Comment: At best, Table 12-2--Unique curve parameter is duplication of the algorithm given above. At worst, it's in contradiction.

Proposed Change: Delete Table 12-2 and the preceding para.

Discussion: There’s nothing wrong with providing help to implementers. Description of a formula and results of said formula for some inputs is not duplication and no error has been identified to justify referring to it as a contradiction.

Resolution: Reject, no problem has been identified and the cited table and paragraph provide useful information.

**CID 4668**

Comment: At best, Table 12-2--Unique curve parameter is duplication of the algorithm given above. At worst, it's in contradiction.

Proposed Change: Move Table 12-2 and the preceding para to above the "The SSWU method takes " para, combining and changing the moved para and the "The SSWU method takes " para to "The SSWU method takes a curve-specific parameter, z. Values for some defined groups based on their IANA-assigned values are listed in Table 12-2 (Unique curve parameter(M137)). For other groups, z is determined by finding the number that satisfies the following rules, given p, a, and b, from the curve's domain parameter set:"

Discussion: Making two identical comments with two different proposed changes invites chaos. The proposed change is not correct because z is determined by finding the number that satisfies the rules for all groups. They all use that formula, even the ones whose IANA-assigned values are listed in table 12-2.

Resolution: Reject, there is still no problem identified and the proposed change is not exactly correct.

**CID 4670**

Comment: "All operations in the SSWU algorithm shall be done in constant time. " is already stated, so CSEL and CEQ don't have to say it (indeed, this would suggest that maybe other operations such as multiplication do not have to be in constant time).

Proposed Change: Delete "operates in constant time and " (2x). Change "All operations in the SSWU algorithm shall be done in constant time. " to "All operations in the SSWU algorithm, including CSEL and CEQ, shall be done in constant time. "

Discussion: No problem has been identified. The operators that result in branching are explicitly called out due to them being so useful in doing side channel attacks. The entire algorithm must be done in constant time but calling out these special operators is useful information for implementers. Not only that but if explicitly calling out CSEL and CEQ “suggest that maybe other operations such as multiplication do not have to be in constant time” then calling them out explicitly in the proposed change would not really address the alleged issue.

Resolution: Reject, no problem has been identified and explicit mention of operations that result in code branching as needing special attention is important information for implementers.

**CID 4671**

Comment: "the SAE hash-to-PWE bit" - no such bit, and they're called subfields anyway. And set to what?

Proposed Change: Change to "to 1 the SAE hash-to-element subfield". In 12.4.4.2.2/3 change "indicate support for the SAE hash-to-element in its Extended RSN Capabilities field" to "set the SAE hash-to-element subfield in its Extended RSN Capabilities field to 1". In 12.4.4.2.3 change "setting the SAE hash-to-element bit in the Extended RSN Capabilities field" to "setting to 1 the SAE hash-to-element subfield in the Extended RSN Capabilities field"

Discussion: It’s called a “bit field”, a field composed of bits. Table 9-321, which describes this field of bits, has a column “Bit”. So there is a bit and it’s bit number 5 according to table 9-321. And the operations on bits are they they get set and cleared. There is no ambiguity about what they are set to as there can be only 1 possible value (and 1 guess at that what that 1 value is… hint hint).

Resolution: Reject, there is such a bit and bits get set.

**CID 4698**

Comment: What is a "SAE exchange" as opposed to "SAE authentication"? Ditto "FILS exchange".

Proposed Change: As it says in the comment.

Discussion: This is an offer to enter into a theological discussion, not identification of a problem. The proposed change is nonsensical

Resolution: Reject, no problem has been identified and no change has been suggested.

**CID 4740**

Comment: Some of the ResultCodes in the SAP have underscores (e.g. JOIN\_FAILURE\_TIMEOUT, NOT\_SUPPORTED) some not (e.g. AUTH FAILURE TIMEOUT, ANTI-CLOGGING

TOKEN REQUIRED). There is no justification for this inconsistency. Underscores make it easier to find result codes, so are preferable.

Proposed Change: Change "AUTH FAILURE TIMEOUT" to "AUTH FAILURE\_TIMEOUT" throughout the document.

Discussion: One sympathizes with search difficulties in a 4647 page document but it is not clear how the inclusion of one underscore to bind together two words in a three word term helps. Furthermore “change x to y throughout the document” is an unreasonable comment to make as the person resolving the comment has to go find all offending places in the document which the comment admits is a problem.

Resolution: Reject, unreasonable request.

**CID 4741**

Comment: Some of the ResultCodes in the SAP have underscores (e.g. JOIN\_FAILURE\_TIMEOUT, NOT\_SUPPORTED) some not (e.g. AUTH FAILURE TIMEOUT, ANTI-CLOGGING

TOKEN REQUIRED). There is no justification for this inconsistency. Underscores make it easier to find result codes, so are preferable, but if the group rejects this, then the alternative is to replace underscores with spaces in all ResultCodes.

Proposed Change: As it says in the comment.

Discussion: It’s groundhog day here in TGmd! While an unjustified inconsistency has been alleged, there is no change proposed.

Resolution: Reject, no change has been proposed.

**CID 4742**

Comment: Some of the ResultCodes in the SAP have underscores (e.g. JOIN\_FAILURE\_TIMEOUT, NOT\_SUPPORTED) some not (e.g. AUTH FAILURE TIMEOUT, ANTI-CLOGGING

TOKEN REQUIRED). There is no justification for this inconsistency. Underscores make it easier to find result codes, so are preferable.

Proposed Change: As it says in the comment.

Discussion: It’s groundhog day here in TGmd! While an unjustified inconsistency has been alleged, there is no change proposed.

Resolution: Reject, no change has been proposed.

**References:**