IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Assortment of SA ballot comments | | | | |
| Date: 2023-10-30 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Jouni Malinen | Qualcomm Technologies, Inc. |  |  | jouni@qca.qualcomm.com |
|  |  |  |  |  |

Abstract

This document proposes comment resolutions to the following REVme/D4.0 initial SA ballot comments:

CID 6419, 6483

# CID 6419

Clause Number: 2

Comment:

It is not clear whether the section 5.3 fix in https://theory.stanford.edu/~jcm/papers/fp09-he.pdf actually been included in the spec (the intro suggests there was agreement it should/would be)

Proposed Change:

Add "Analysis of the 802.11i 4-Way Handshake" to Clause 2

Proposed Resolution:

REVISED - Incorporate changes under the “Proposed changes for CID 6419” section of <this doc>.

### Discussion

The comment is apparently referring to this part in the paper’s introduction:

We provided these basic attacks and repairs to the 802.11 TGi; the third repair in Section 5.3 was adopted. Although the 802.11i documentation was left unchanged so that the ratification would not be delayed, the repair will be added once the documentation is updated [Walker, email communication, June 30, 2004].

Section 5.3 of the paper (“Nonce Re-use”) describes this repair as follows:

The third repair is to eliminate the intermediate states on the supplicant side. Specifically, the supplicant can re-use the values of SNonce until a legitimate handshake is completed and a shared PTK is achieved between the supplicant and the authenticator. In other words, the supplicant does not update its nonce responding to each received *Message 1* until *Message 3* is received and verified.

IEEE P802.11-REVme/D4.0 shows RSNA Supplicant key management state machine to assign “SNonce = Random” in the AUTHENTICATION state which is entered when “an SSID is to be authenticated”. In other words, this is not when receiving any 4-way handshake message 1, but at the start of the exchange. That would seem to imply that the SNonce value is to be re-used over multiple message 1 retries. However, 12.7.6.2 (4-way handshake message 1) could be interpreted to indicate that a new SNonce would be generated for each received message 1.

There does not seem to be any clear justification for adding a reference to the paper into Clause 2 as suggested in the comment. However, it would seem reasonable to make the standard clearer in when the SNonce value is updated.

### Proposed changes for CID 6419

**12.7.6.2 4-way handshake message 1**

*Modify 12.7.6. 2 as shown (REVme-D4.1 P3036 L9):*

Processing for PTK generation is as follows:

The Authenticator sends message 1 to the Supplicant at the end of a successful IEEE 802.1X authentication, after (re)association completes for a STA that has authenticated with SAE or for which PSK authentication is negotiated, when a cached PMKSA is used, or after a STA requests a new key. On reception of message 1, the Supplicant determines whether the Key Replay Counter field value has been used before with the current PMKSA. If the Key Replay Counter field value is less than or equal to the current local value, the Supplicant discards the message. Otherwise, the Supplicant:

a) Generates a new nonce SNonce if no SNonce has been yet generated for this 4-way handshake. The same SNonce is reused within the 4-way handshake until a valid message 3 has been received.

b) Derives PTK, the derived PTK including the Key derivation key (KDK) if WUR frame protection is being negotiated.

c) Constructs message 2.

# CID 6483

Clause Number: 12

Comment:

The same SNonce should be reused until a valid M3 has been received, to avoid DoS attacks (see https://theory.stanford.edu/~jcm/papers/fp09-he.pdf )

Proposed Change:

Make this recommendation (as a "should")

Proposed Resolution:

REVISED - Incorporate changes under the “Proposed changes for CID 6419” section of <this doc>.

### Discussion

Practically same comment as CID 6419 except with a different proposed change. 12.7.6.2 does not use shall/should language, so descriptive language seems more appropriate in that context. The Supplicant state machines already imply this behavior, so there does not seem to be justification for having to make this any more complex than that. The resolution text for CID 6419 can be used to address this comment as well.

# CID 6085

Clause Number: 12.4.7.3 Page: 2834 Line: 6

Comment:

Use of a plaintext SAE password identifier can reveal personal identifier of a STA (or user) when per-device or per-user passwords are used even if the STA is using MAC address randomization. This is undesired and can reduce likelihood of deployment of SAE password identifiers which can result in deployment issues for future IEEE 802.11 deployments like EHT/MLO where PSK cannot be used, but multiple passwords might be needed.

Proposed Change:

Incorporate changes from the latest revision of https://mentor.ieee.org/802.11/dcn/23/11-23-1236-01-000m-hpke-protected-sae-password-identifiers-for-privacy.docx

Proposed Resolution:

### Discussion

Abcd

### Proposed changes for CID 6085

**12.7.6.2 4-way handshake message 1**

*Modify 12.7.6. 2 as shown (REVme-D4.1 P3036 L9):*

Abcd

# CID 6086

Clause Number:

Comment:

There are various use cases where multiple ESSs (i.e., different SSIDs) are used to connect to the same IEEE 802 LAN. This could be needed, e.g., when setting up a separate ESS with older RSN parameters to allow misbehaving deployed STAs to get connected. It would be helpful to the user experience if the protocol would be extended to allow the AP to provide information to non-AP STAs about which SSIDs are connected to the same LAN, so that the STA UI could guide the user in selecting the most appropriate SSID (e.g., pick the ESS where SAE is enabled in a case where a separate ESS is set with only PSK AKMs for legacy support).

Proposed Change:

Introduce a new information element that an AP can advertise to point to a preferred ESS which connects to the same LAN.

Proposed Resolution:

### Discussion

Abcd

### Proposed changes for CID 6086

**12.7.6.2 4-way handshake message 1**

*Modify 12.7.6. 2 as shown (REVme-D4.1 P3036 L9):*

Abcd

# CID 6088

Clause Number: 12.2.2 Page: 2793 Line: 49

Comment:

There is now quite a few references to OWE and its behavior in the IEEE 802.11 standard. However, this is not sufficient to implement OWE without having to go through the combination of the IEEE 802.11 standard and IETF RFC 8110. This is unnecessarily complex and results in issues in maintaining OWE in the future. As an example of this, there is a known difference between RFC 8110 and deployed OWE implementations: https://www.rfc-editor.org/errata/eid6182. It would be good to get a single place that defines the actually implemented OWE and the best place for this would seem to be the IEEE 802.11 standard.

Proposed Change:

Merge in the key derivation and other protocol details from IETF RFC 8110 into IEEE 802.11 and updates these based on this errata: https://www.rfc-editor.org/errata/eid6182.

Proposed Resolution:

### Discussion

Abcd

### Proposed changes for CID 6088

**12.7.6.2 4-way handshake message 1**

*Modify 12.7.6. 2 as shown (REVme-D4.1 P3036 L9):*

Abcd

# CID 6000

Clause Number:

Comment:

Proposed Change:

Proposed Resolution:

### Discussion

Abcd

### Proposed changes for CID 6000

**12.7.6.2 4-way handshake message 1**

*Modify 12.7.6. 2 as shown (REVme-D4.1 P3036 L9):*

Abcd