IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| What does it mean to be “well-encoded”? | | | | |
| Date: 2016-01-20 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Dan Harkins | HP Enterprise | 1322 Crossman avenue, Sunnyvale, California, United States of America | +1 408 227 4500 | dharkins at aruba networks dot com |
|  |  |  |  |  |

Abstract

This submission addresses CID 10672

CID:

|  |  |  |  |
| --- | --- | --- | --- |
| Section | Comment | Proposed Change | Resolution |
| 11.11.2.3.5 | "a well-encoded ephemeral public key" -- what defines whether an ephemeral public key is well-encoded? | Delete "well-encoded" | Revised: the proposed change does not answer the question posed in the comment. Encorporate the changes to the Draft from this document |

Discussion:

**Caveat emptor**: *let the buyer beware!*

Validation checks of public keys let the recipient verify that the component(s) of the key conform to the key generation requirements of the group from which they are generated. If an invalid key is used, it may void the security guarantees of the protocol using public keys.

***Instruct the editor to modify section 11.6.12.4.2 as indicated:***

**11.6.12.4.2 Exchange of PKEX Key Commit messages**

Upon receipt of a PKEX Key Commit message the STA will check whether the finite cyclic group is acceptable. If not, the STA shall silently discard the message. If the group is acceptable the STA checks whether it has a public key in that group to exchange. If it does not, and does not wish to create such a public key it shall silently discard the message.

Next, the STA determines whether it has sent a PKEX Key Commit message to the STA that transmitted the received message (the peer STA) or to the group address. If not, for example if the recipient is an AP STA, the STA shall generate PWE, if necessary, as defined above, generate a PKEX Key Commit message, and transmit it to the peer STA. Otherwise, and in any case, the PKEX Key Commit message is processed:

1. The peer's nonce is retrieved from the Challenge Text field of the Challenge Text element in the received frame;
2. The encrypted public key is obtained by converting the octet string(s) to an element according to 11.3.7.2.5 (Octet string to element conversion). If conversion fails, the PKEX Commit message is silently discarded;
3. The encrypted public key, C, is decrypted using PWE to produce the STA’s public key, P, according to the decryption function definition in 11.6.12.1 (General): P = elem-op(C, -PWE);
4. The decrypted public key P is then validated in a group-specific fashion as described in 5.6.2.3 of NIST SP 800-56A R2. If validation fails, PKEX terminates unsuccessfully.
5. A shared element, S, is generated using scalar-op() from 11.3.4 (Finite Cyclic groups) with the private analog to the STAs public key, priv, and the peer STA's decrypted public key, P, and a secret value, s, is derived from S using function F() from 11.3.4 (Finite cyclic groups):

S = scalar-op(priv, P)

s = F(S)

***Instruct the editor to modify section 11.11.2.3.3 as indicated:***

**11.11.2.3.3 AP processing of Authentication frame**

Upon reception of the Authentication frame, the AP shall do the following procedure:

1. If Authentication frame includes a Finite Cyclic Group field, then the AP shall first determine whether the indicated finite cyclic group in the received FILS Authentication frame is supported.
2. If the indicated finite cyclic group in the received FILS Authentication frame is not supported, the AP shall respond with an Authentication frame with the Authentication algorithm number set to 4 (FILS authentication) (see 8.4.1.1 (Authentication Algorithm Number field)) and the Status Code field set to 77 (Authentication is rejected because the offered finite cyclic group is not supported) and shall terminate the exchange.
3. If PFS is being used, the STA’s public key shall be converted from an octet string to an element according to the conversion in 11.3.7.2.5 (Octet string to element conversion). Then the AP shall validate the STA’s public key in a group-specific fashion as described in 5.6.2.3 of NIST SP800-56A R2. If validation fails the AP shall terminate the exchange.
4. The AP shall check whether PMKSA caching is being attempted by the presence of the PMKID List element.

***Instruct the editor to modify section 11.11.2.3.4 as indicated:***

**11.11.2.3.4 AP construction of Authentication frame**

If the AP is not connected to, or does not recognize the Authentication Server identified by the STA using the realm in the key Name-NAI field of the EAP-Initiate/Re-auth packet, then the AP shall send Authentication frame with Status Code field set to 113, “Authentication rejected due to unknown Authentication Server” to the non-AP STA.

Otherwise, the AP shall generate its own nonce and construct an Authentication frame for the STA. This frame shall contain the FILS wrapped data that encapsulates EAP-Finish/Re-auth packet received from the Authentication Server. In addition, if PFS is used, the Element field of the Authentication frame sent by the AP contains the AP’s ephemeral public key. In this frame, the AP shall set the Authentication sequence number to 2.

If PFS is being used for the exchange, the AP shall perform the group's scalar-op (see 11.3.4.1 (General)) with the STA's ephemeral public key and its own ephemeral private key to produce an ephemeral Diffie-Hellman shared secret, DHss.

***Instruct the editor to modify section 11.11.2.3.5 as indicated:***

**11.11.2.3.5 Non-AP STA processing of Authentication frame**

The STA processes the received Authentication frame as follows:

1. If the received Authentication frame does not include the Authentication Algorithm Number equal to 4 (FILS authentication) (see 8.4.1.1 (Authentication Algorithm Number field)), or if PMKSA caching was attempted and the received Authentication frame includes a PMKID that does not match a PMKID in the Authentication frame sent by the STA; or if the received Authentication frame doesn’t include either a PMKID or an EAP-Finish/Re-auth packet, the STA shall abandon FILS authentication.
2. If the received Authentication frame includes the Status Code field equal to 15 (Authentication rejected because of challenge failure) or 53 (invalid PMKID), then the STA shall abandon the FILS authentication.
3. The STA verifies that the AP transmitted PFS parameters are consistent with the desire of the STA (indicated by whether or not the STA transmitted an ephemeral public key):

1 If the STA transmitted an ephemeral public key, and the received Authentication frame does not include an ephemeral public key, then the STA shall abandon the FILS authentication.

2 If the STA did not transmit an ephemeral public key desired PFS, and the received Authentication frame includes an ephemeral public key, then the STA shall abandon the FILS authentication.

1. If applicable, the STA processes the EAP-Finish/Re-auth packet as per IETF RFC 6696:

1 If the ‘R’ flag = 0, indicating success, then the STA shall derive rMSK.

2 If the ‘R’ flag = 1, indicating failure, then the STA shall abandon the FILS authentication.

1. If PFS is being used for the exchange, the AP’s public key shall be converted from an octet string to an element according to the conversion in 11.3.7.2.5 (Octet string to element conversion). Then the STA shall validatethe AP’s public key in a group-specific fashion as described in 5.6.2.3 of NIST SP 800-56A R2. If validationfails, the STA shall terminate the FILS authentication protocol. Otherwise, the STA shall perform the group's scalar-op (see 11.3.4.1 (General)) with the AP’s ephemeral public key and its own ephemeral private key to produce an ephemeral Diffie-Hellman shared secret, DHss.
2. The STA shall perform key derivation per 11.11.2.5 (Key establishment with FILS authentication) and key confirmation per 11.11.2.6 (Key confirmation with FILS authentication).

**References:**