IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| SAE H2E capability indication | | | | |
| Date: 2020-06-12 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Jouni Malinen | Qualcomm, Inc. |  |  | jouni@qca.qualcomm.com |
|  |  |  |  |  |

Abstract

This document discusses how support for SAE H2E is indicated in P802.11-REVmd and proposed a small change to this to enable additional protection against downgrade attacks.

**Discussion**

IEEE P802.11-REVmd introduced a new option for deriving the SAE PWE using hash-to-element (H2E) mechanism (the "M137" change in the draft). Advertisement for the H2E capability was described only for the AP while leaving the non-AP STA capability implicit by the non-AP STA initiating SAE authentication using the special status code value in an SAE commit message. While this is sufficient for the H2E negotiation to work, this does not allow the AP to detect potential downgrade attacks from H2E to hunting-and-pecking and depends on the non-AP STA detecting that. Furthermore, this is somewhat inconsistent use of the RSNXE fields ("If a STA does not support any of capabilities.." while one of the capabilities is described only for AP).

It is straightforward to extend that capability indication to apply for both the AP and the non-AP STA so that both STAs can check against downgrade attacks. In particular, this allows the AP to detect a downgrade attack before sending GTK in EAPOL-Key msg 3/4 while the currently defined mechanism allows the non-AP STA to detect the attack only after that message has been transmitted. Changing the RSNXE capability bit to apply for "STA" is all that is needed for this since the generic rules regarding use of RSNXE take care of mandating the non-AP STA to include it in (Re)Association Request frame and a protected version in EAPOL-Key msg 3/4 for the cases where association exchange is not protected.

The mechanism proposed here has been implemented by multiple vendors and it has been tested between independent implementations.

**Proposed Changes**

**9.4.2.241 RSN Extension element (RSNXE)**

*Change Table 9-323 (D3.3 page 1466 line 17) as shown:*

The RSNXE field contains additional information required to establish an RSNA. The format of the RSNXE field is defined in Figure 9-780 (RSNXE format).

|  |  |  |  |
| --- | --- | --- | --- |
|  | Element ID | Length | Extended RSN Capabilities |
| Octets: | 1 | 1 | *n* |

**Figure 9-780—RSNXE format**

The Element ID and Length fields are defined in 9.4.2.1 (General).

The Extended RSN Capabilities field, except its first 4 bits, is a bit field indicating the extended RSN capabilities being advertised by the STA transmitting the element. The length of the Extended RSN Capabilities field is a variable *n*, in octets, as indicated by the first 4 bits in the field. The Extended RSN Capabilities field is shown in Table 9-323 (Extended RSN Capabilities field).

**Table 9-323—Extended RSN Capabilities field**

|  |  |  |
| --- | --- | --- |
| **Bit** | **Information** | **Notes** |
| 0–3 | Field length | The length of the Extended RSN Capabilities field, in octets, minus 1, i.e., *n* – 1. |
| 4 | Protected TWT Operations Support | The STA sets the Protected TWT Operations Support field to 1 when dot11ProtectedTWTOperationsImplemented is true, and sets it to 0 otherwise. See 10.47.1 (TWT overview). |
| 5 | SAE hash-to-element | The STA supports directly hashing to obtain the PWE instead of looping. See 12.4.4.2.3 (Hash-to-curve generation of the password element with ECC groups) and 12.4.4.3.3 (Direct Generation of the password element with FFC groups). |
| 6– (8×*n* – 1) | Reserved |  |

If a STA does not support any of capabilities defined in the RSNXE, then the STA is not required to transmit the RSNXE.