May 06, 2019

OPTIMIZED PAIRWISE MASTER KEY IDENTIFIER BASED ROAMING FOR WI-FI PROTECTED ACCESS 3 SIMULTANEOUS AUTHENTICATION OF EQUALS WITH WIRELESS LOCAL AREA NETWORK CONTROLLER OR ACCESS POINT

Swapnil Shah

Umesha G M

Sayan Das

Bibek Sahu

OPTIMIZED PAIRWISE MASTER KEY IDENTIFIER BASED ROAMING FOR WI-FI PROTECTED ACCESS 3 SIMULTANEOUS AUTHENTICATION OF EQUALS WITH WIRELESS LOCAL AREA NETWORK CONTROLLER OR ACCESS POINT

AUTHORS:
Swapnil Shah
Umesha G M
Sayan Das
Bibek Sahu

ABSTRACT

Techniques are described herein for Wi-Fi® Protected Access 3 (WPA3) Simultaneous Authentication of Equals (SAE) client authentication and roaming. The validity of a session may be checked before attempting network association with a target Access Point (AP). This solution may avoid a delay in network connectivity when the previous session is invalid, thereby improving network connectivity for SAE based authentication when clients roam across APs.

DETAILED DESCRIPTION

The Wi-Fi® Protected Access 3 (WPA3) standard was defined to improve personal and enterprise security. WPA3 provides a method to improve personal security by adopting Simultaneous Authentication of Equals (SAE) based authentication to derive a Pairwise Master Key (PMK) using a shared secret password between the Access Point (AP) and wireless endpoints (clients).

The Wireless Local Area Network (LAN) Controller (WLC) or AP and client can authenticate each other by exchanging SAE commit and confirm frames as mandated by the WPA3 SAE protocol. At the end of SAE authentication, the client and WLC/AP may derive the PMK, which is further used in an Extensible Authentication Protocol (EAP) over LAN (EAPOL) four-way handshake to derive the session encryption keys to encrypt the session traffic between the AP and the wireless client.

The WPA3 SAE protocol allows the client to perform fast roaming between APs using the previously-derived PMK Identifier (PMKID) instead of deriving a new PMKID with each AP. In such fast roaming cases, the SAE client sets the PMKID in the Robust

Security Network (RSN) Information Element (IE) from the previous association while roaming to the new AP.

When a client roams, it includes the previously-derived PMKID from its previous association in a re-association request to the new AP. Upon receipt of the re-association request, the WLC/AP may send a re-association response with status code "0" if the PMK/PMKID of the previous association is present at the WLC/AP. Otherwise, the WLC/AP sends a re-association response with status code "53" followed by de-authentication frames and the client starts a new session by re-initiating SAE authentication with the new AP.

If the client receives a re-association response with the status code "SUCCESS," the PMKID is valid and the previously-cached PMK is used in the EAPOL four-way handshake with the new AP to derive the session keys.

If the client receives an association response with status code "53" from the new AP, the AP does not have the corresponding PMK of the PMKID received in the re-association request. In this case, the client needs to restart the SAE commit/confirm frames to derive a new PMK. Rejecting the client after initiating the association due to PMKID mismatch results in slower roaming and delay in connecting to the network.

Figure 1 below illustrates an example sequence diagram depicting SAE authentication and client association using SAE Authentication Key Management (AKM).

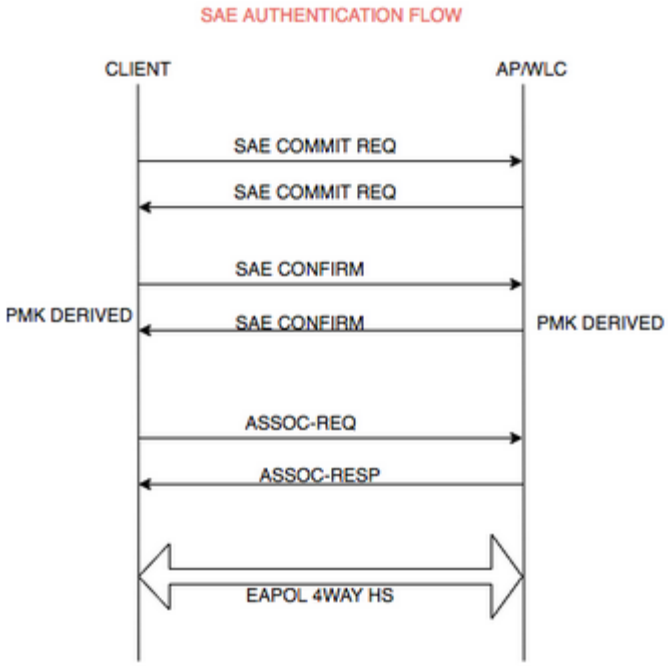

Figure 1

There is at least one major difference in PMKID roaming for SAE and other AKM. Regarding the re-association request for 802.11i AKM (i.e., a standard roaming method using PMKID, as per the 802.11i standard), if the PMKID is not valid, the client is forced to undergo the full authentication process to derive a new security association PMK without sending any de-authentication frames.

However, in the case of WPA3 SAE, the AP is expected to send the de-authentication frame to the client if the PMKID received in the re-association request does not match the PMKID present at the WLC/AP. In the SAE based roaming scenario, if the PMKID is invalid, client receives a de-authentication trigger and has to start SAE authentication again. The de-authentication trigger after detecting the invalid PMKID in the re-association request can delay client connection to the network.

Figure 2 below illustrates an example sequence diagram depicting roaming using a PMKID.

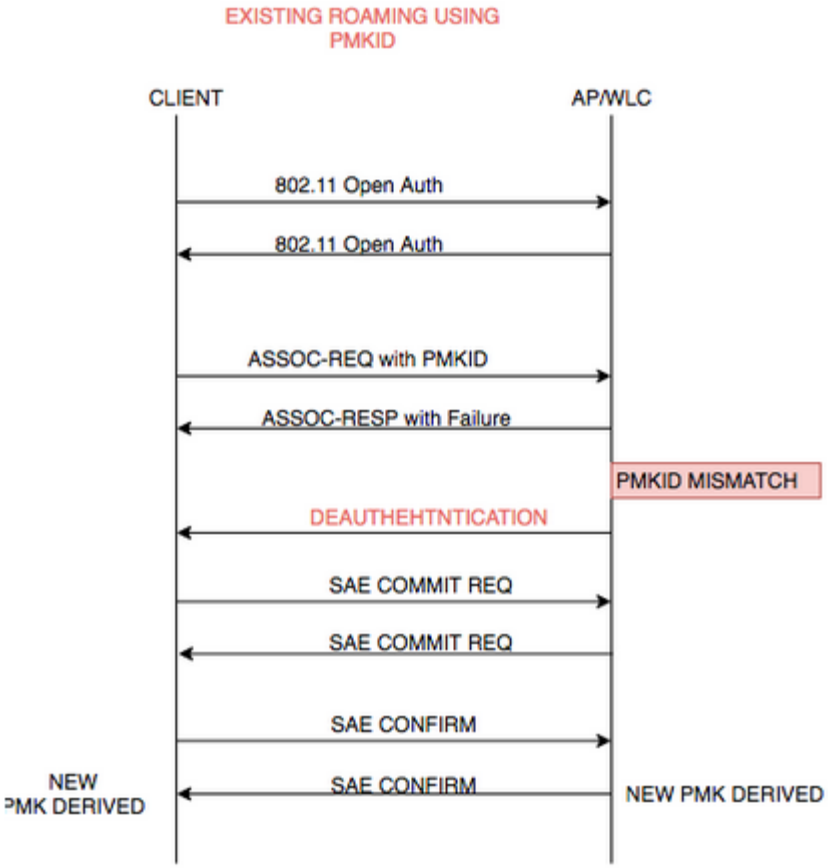

Figure 2

Techniques are described herein to improve WPA3 SAE client connectivity by early detection of the validity of the security association with the new AP even before attempting network association. This helps wireless clients roam faster, thereby improving the network connectivity experience.

As described herein, roaming delay and latency for SAE clients are optimized when there is no common PMKID between APs and wireless clients. There are several methods to allow the client to check the validity of the PMKID before attempting network association in order to avoid de-authentication as well as seamless roaming.

The first method involves including the PMKID in an open authentication frame. A tag may include the PMKID in an 802.11 open authentication sequence one frame. The WLC/AP may verify the PMKID in the 802.11 open authentication frame and reply with a new status code to indicate whether PMKID validation was successful. If the client receives the PMKID validation success status code in the open authentication response, it may decide to perform re-association and complete the roaming with the new AP without de-

authentication. This saves four frames in the case of PMKID mismatch, namely the association request, the association response, disassociation, and de-authentication. This first method helps to improve network connectivity while the client is roaming across APs.

Figure 3 below illustrates an example sequence diagram that depicts the case when the PMKID received in the open authentication frame matches the PMKID stored in the WLC/AP cache.

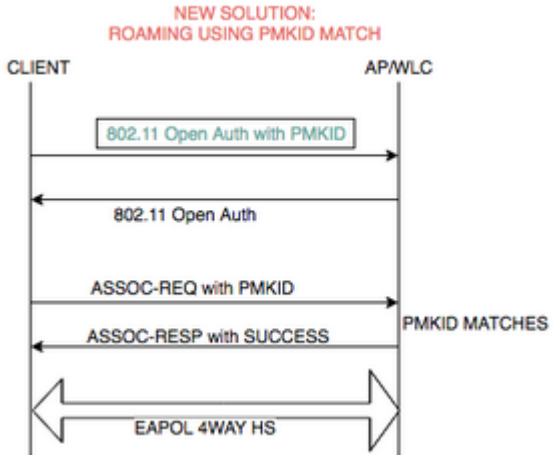

Figure 3

Figure 4 below illustrates an example sequence diagram that depicts the case when the PMKID does not match the PMKID stored in the WLC/AP cache.

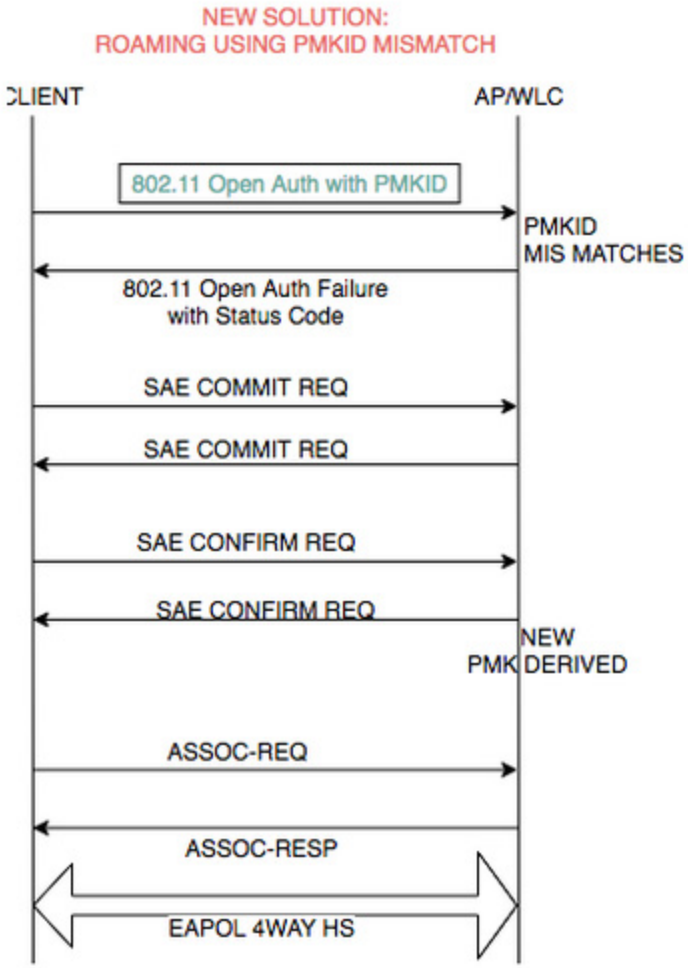

Figure 4

The second method uses the PMKID in an SAE commit message/frame. Here, the client is associated to a wireless network using SAE authentication. When the client decides to roam to a new AP, the wireless client sends the SAE commit message with the PMKID therein. The PMKID may be encoded in a vendor specific tag along with its scalar and finite field element. Upon receiving the SAE commit message from the client, if the vendor specific element containing the PMKID is present, the WLC/AP may check for PMKID validity. If the PMKID found to be valid, the WLC/AP includes the PMKID tag in the SAE commit message to indicate that the client may use the PMKID. If the PMKID is found to be invalid, the WLC/AP may continue the SAE authentication sequence by sending the SAE commit frame to derive a new PMK. The second method thus enables the client to start with an SAE authentication frame instead of an open authentication frame.

In case of a PMKID mismatch, four frames will be saved, namely the association request, the association response, disassociation, and de-authentication.

The third method uses a Generic Advertisement Service (GAS) public action frame to validate the PMKID. The GAS frame may be used to check the validity of the PMKID before attempting PMKID-based roaming. The client may send the GAS frame with the PMKID therein to the WLC/AP before attempting roaming. The WLC/AP validates the PMKID received in the GAS frame and sends the response with a success/failure status. If the status is "SUCCESS," the client may initiate the roaming to that AP. Otherwise, the client initiates SAE authentication to derive a new PMK as the PMKID is no longer valid on the AP. Accordingly, in case of PMKID mismatch, four frames will be saved. However, in the interest of checking the validity of PMKID, two additional frames (namely, GAS request and response) may be used. Thus, the third method effectively saves two frames.

The fourth method uses the PMKID in a probe request/response. The PMKID is added in the probe request in a similar manner as the first method (i.e., including the PMKID in the open authentication frame). Before roaming, the client may check the validity of the PMKID by including it in a probe request. The WLC/AP may, in turn, send a probe response with a new status code to indicate the PMKID validity. If the status code is set as "SUCCESS," the client may proceed with sending the association request with the PMKID as the roam will be successful. If the status code is "failure," the client may directly initiate an SAE handshake and save three frames. In case of PMKID mismatch, four frames will be saved. However, in the interest of checking the validity of PMKID, two additional frames (namely, probe request and response) may be used. Thus, the third method effectively saves two frames.

The fifth method involves querying for PMKID using Access Network Query Protocol (ANQP) messaging (e.g., a Passpoint ANQP query). Before roaming, the client may initiate an ANQP query with the new PMKID subtype in a vendor information ID to obtain the current PMKID stored at the WLC/AP. The WLC may send the ANQP response along with current valid PMKID for this client. The client may initiate the re-association request if the PMKID received in the ANQP response matches the PMKID held by the client. If the received PMKID does not match, the client may start SAE authentication to derive a new PMK. Accordingly, in case of PMKID mismatch, four frames will be saved.

However, in the interest of checking the validity of the PMKID, two additional frames (namely, ANQP query and response) may be used. Thus, the third method effectively saves two frames.

This solution improves the roaming experience for many use cases. In one use case, wireless network deployment uses multiple vendors, such as public Wi-Fi (e.g., a stadium). If the client has an option to roam to one of two APs belonging to different vendors, the client may decide whether to initiate SAE handshake or send an association request with the PMKID.

A second use case involves single vendor deployment. If the client has an option to roam to one of two APs belonging to two different WLCs which are not in the same mobility group, the client may precisely decide to roam to a given AP using the techniques described herein.

A third use case involves a flex group. For example, a WLC may support multiple flex groups and the PMK may be shared proactively by the WLC within the flex group. If the client has an option to roam to one of two APs belonging to two different flex groups, the client may decide to roam to the AP that has the PMK.

A fourth use case involves session expiry. Here, the WLC may wait for one second upon session expiry before sending disassociation and deauthentication messages. If the client roams within this wait period of one second, the WLC may respond to the client by sending an association response with status code “53.” The client may check the validity of the PMKID and preclude four frames (i.e., association request, association response, disassociation, and de-authentication). Thus, the solution described herein may save up to four frames.

In summary, techniques are described herein for WPA3 SAE client authentication and roaming. The validity of a session may be checked before attempting network association with a target AP. This solution may avoid a delay in network concavity when the previous session is invalid, thereby improving network connectivity for SAE based authentication when clients roam across APs.