May 20, 2019

PROACTIVE IDENTITY PRE-SHARED KEY CACHE FOR WIRELESS CLIENTS AT WIRELESS LOCAL AREA NETWORK CONTROLLER OR ACCESS POINT

Umesha G M

Swapnil Shah

Vikram Shishodia

PROACTIVE IDENTITY PRE-SHARED KEY CACHE FOR WIRELESS CLIENTS AT WIRELESS LOCAL AREA NETWORK CONTROLLER OR ACCESS POINT

AUTHORS:
Umesha G M
Swapnil Shah
Vikram Shishodia

ABSTRACT

Techniques are described herein for downloading an Identity Pre-Shared Key (iPSK) passphrase to an Access Point (AP) before Simultaneous Authentication of Equals (SAE) is initiated. iPSK may be an individual PSK per client Media Access Control (MAC) address. This may help support Wi-Fi® Protected Access 3 (WPA3) SAE clients.

DETAILED DESCRIPTION

In today's Wireless Local Area Network (WLAN) deployments, personal WLAN security is widely deployed by customers at home, hotspots, metro stations, etc. The main challenge is providing network security for personal security WLANs. Most network deployments use a common password security key(s) per WLAN network or group of users.

Some solutions available today involve reducing network threats by using multiple/individual passwords. The passwords may be per device based key mapping (e.g., Identity Pre-Shared Key (iPSK) per client Media Access Control (MAC) address). There may also be multiple PSKs per WLAN.

The iPSK solution may not work for Wi-Fi Protected Access 3 (WPA3) Simultaneous Authentication of Equals (SAE) clients because the iPSK password is available at the beginning of the SAE handshakes. Hence, the proactive iPSK key caching is required to ensure the iPSK password is available before the client starts the SAE authentication. Through proactive iPSK key caching at the Access Point (AP) or Wireless LAN Controller (WLC), the iPSK password fletching latency may be avoided if the key is cached proactively even before the client attempts association / SAE authentication.

This use case is very important because there are deployments which have individual passwords being mapped per device for personal security WLANs. This also needs to be solved for WPA3 using SAE-based authentication as well.

The challenge for WPA3 SAE based authentication is that iPSK passwords are not available when the client attempts SAE authentication. Otherwise, SAE authentication cannot be accomplished to derive the session key.

Figure 1 below is an example sequence diagram depicting SAE-based authentication using a common shared WLAN password (PSK).

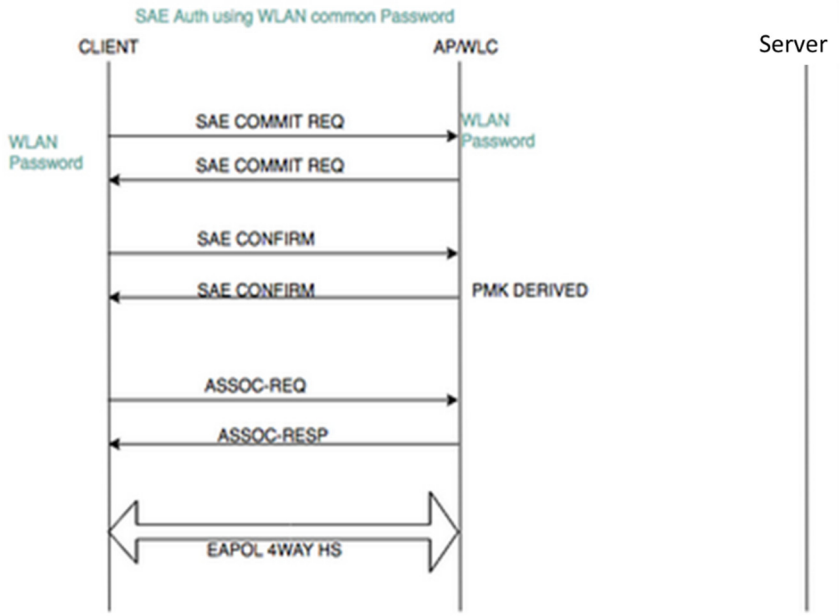

Figure 1

Individual passwords (iPSKs) may be available immediately when the SAE handshake is started. The individual passwords (iPSK) are fletched from an Authentication, Authorization, and Accounting (AAA) server when the association request is received. Once the iPSK password is received, it is used in an Extensible Authentication Protocol over LAN (EAPOL) four-way handshake. By contrast, for WPA3 SAE authentication the iPSK password is available at the WLC/AP even before association. Accordingly, a solution is provided herein to proactively cache the password at the WLC/AP so the WPA3 SAE client may also authenticate using iPSK passwords.

The WLC/AP may obtain the individual password (iPSK) from the external server even before SAE authentication is initiated by the clients. There are a number of different methods for fetching wireless endpoint passwords from a remote AAA server which maintains the per-device passwords (iPSKs).

The following steps to obtain the iPSK passwords are made available for the WPA3 SAE client prior to SAE authentication. First, all iPSK passwords are pre-downloaded from a server (or identity service) to the WLC/AP. The WLC/AP may retrieve and copy all the individual wireless endpoint MAC entries from the server as appropriate. Whenever there is an addition or deletion, Change of Authorization (CoA) may be used to indicate the change in the password entry file and the AP may retrieve the new iPSK password file. The password file may be stored in the WLC/eWLC.

There are also several trigger points to push the iPSK of the client to the AP. One trigger point is pushing the iPSK of the client to the AP when the client sends an active probe request to the AP. Another trigger point is pushing the iPSK of the client to the AP when the client performs a network query by sending public action Access Network Query Protocol (ANQP) messages. Still another trigger point is the AP retrieving the iPSK of the client when the AP receives the first SAE message from the wireless client.

There are several steps involved in retrieving the password of a client that is expected to be a WPA3 SAE client. First, the individual password (PSK per client MAC address) file is pre-downloaded from an Authentication and Command Authorization (ACA) server or identity service to the AP. The AAA server may maintain the password per device which may be used while authenticating the personal security WLANs. The password may be used for any WPA/WPA2/WPA3 securities. The WLC may download the file using Remote Authentication Dial-In User Service (RADIUS) messaging. The RADIUS response may contain vendor Attribute Value Pair (AVP) payloads having the iPSK passwords. All the iPSK passwords are sent to the WLC, which maintains a copy of the iPSK passwords per MAC address in the iPSK database. If there is a modification or addition to the existing password list on the AAA server it may initiate a RADIUS CoA message to indicate to the WLC to re-download the iPSK passwords.

Figure 2 below is an example sequence diagram depicting this method.

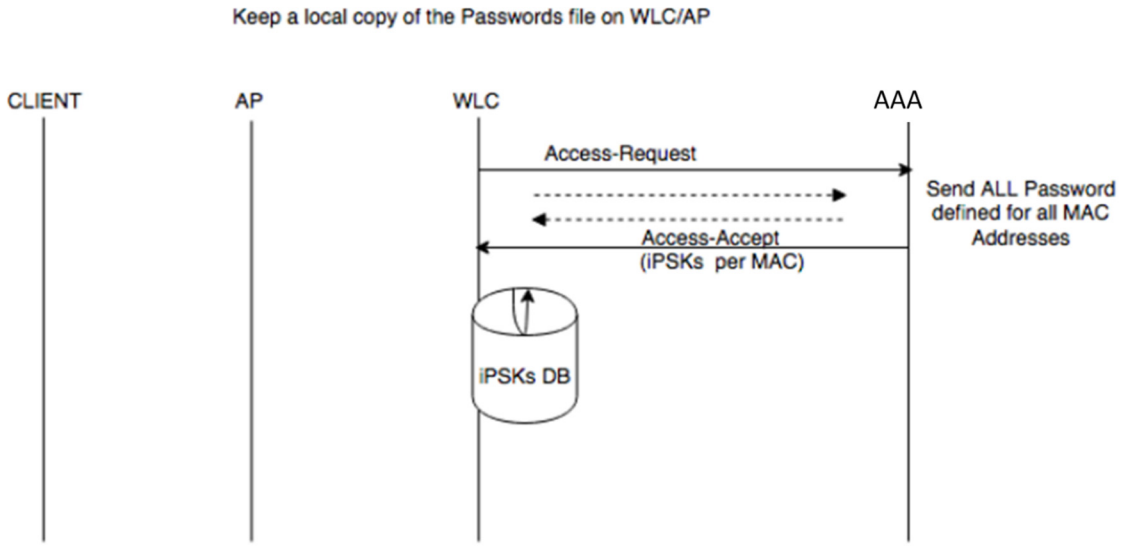

Figure 2

The flow sequence to fletch/push the iPSK password between the WLC and the AP are now described. First, the iPSK of the client is pushed to the AP when the client sends an active probe request to the AP. The actively probing wireless clients generally send the probe request messages to the AP before attempting the authentication/association. When the AP receives the probe message from client, the AP sends a message to fletch the iPSK password from the WLC.

Figure 3 below is an example sequence diagram depicting the sequence of message flows.

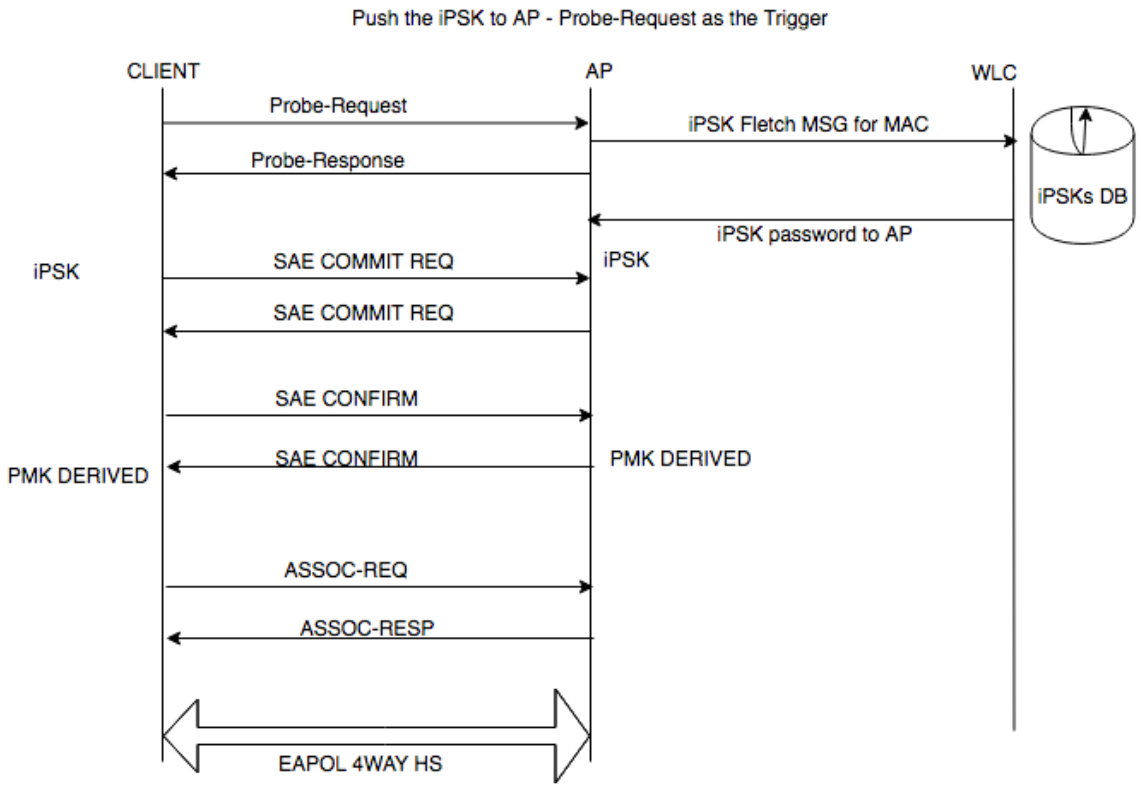

Figure 3

Second, the iPSK password is pushed to the AP when the ANQP query is received at the WLC. The Passpoint 2.0 framework provides an ANQP query/response based mechanism even prior to authentication/association to the WLAN. The wireless client queries the wireless network using the Passpoint 2.0 ANQP query messaging to discover network capabilities and information even before attempting wireless authentication/association. Passpoint2.0 and WPA3 SAE authentication capabilities may be enabled together on the WLAN.

Figure 4 below is an example sequence diagram depicting operations to push the client-specific iPSK password from the WLC to the AP.

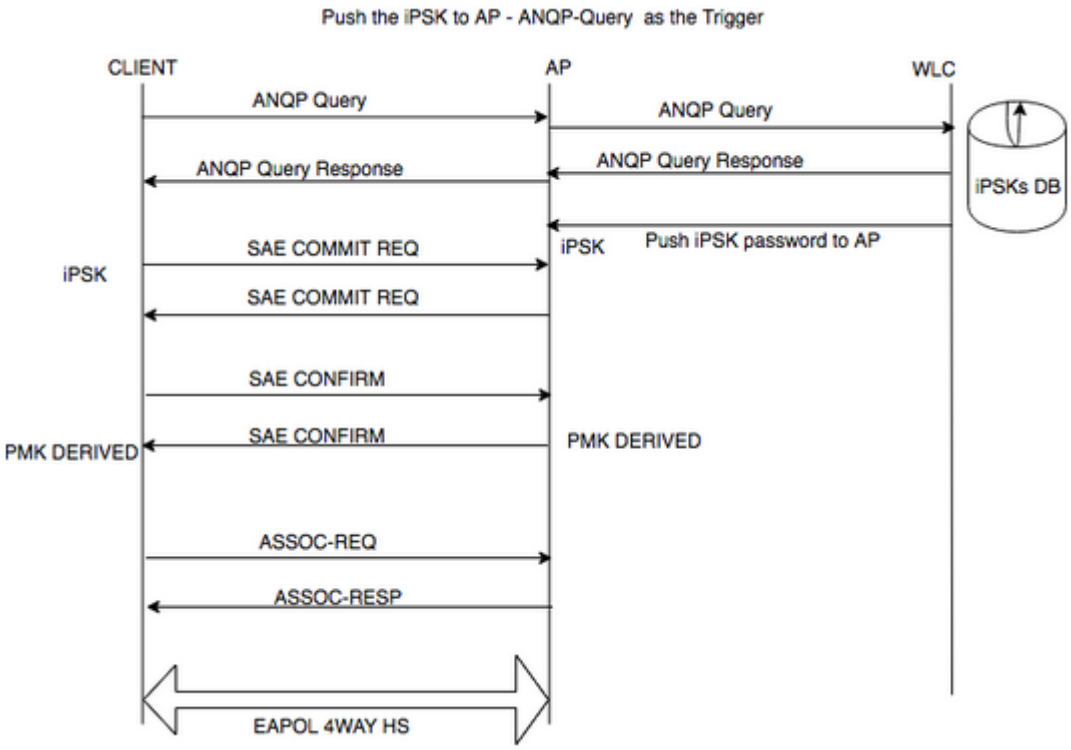

Figure 4

Third, the iPSK client password may be retrieved when the SAE commit request is initiated by the wireless client. If the iPSK password is not available at the AP, a message may be initiated to the WLC to retrieve the iPSK password from the WLC when the SAE authentication message (commit message) is started.

Figure 5 below is an example sequence diagram depicting this sequence of message flows.

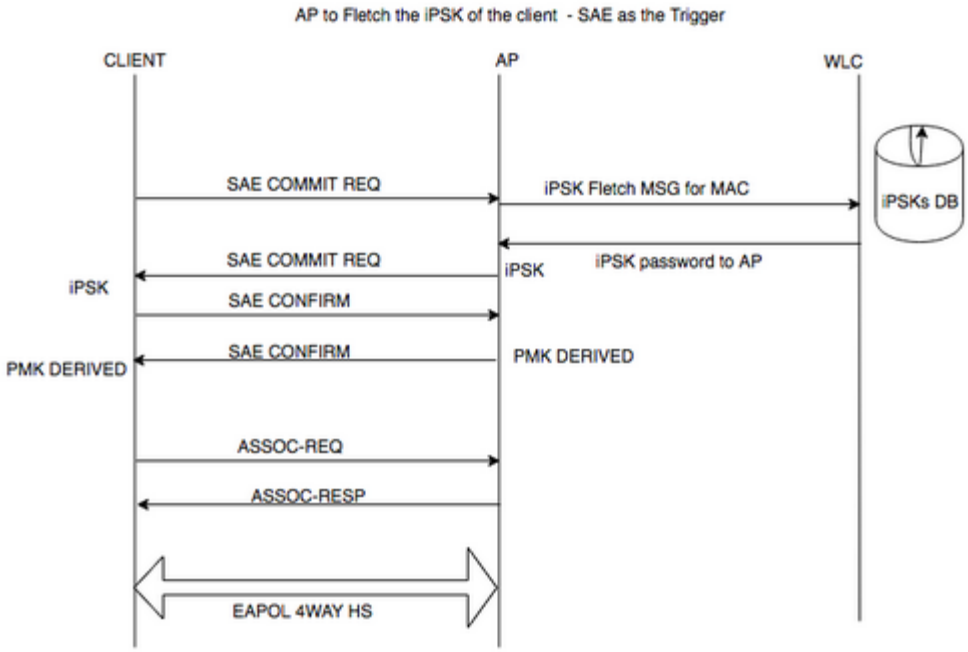

Figure 5

In summary, techniques are described herein for downloading an iPSK passphrase to an AP before SAE is initiated. This may help support WPA3 SAE clients.