

Overriding SAE-Commit Message of WPA3-Authentication Sequence

Goal: Corrupt specific IEs of SAE-Commit messages to provoke WPA3-EAPOL authentication failure. The `sae_commit_override` field in LANforge **Custom WiFi Parameters** provides means to corrupt or customize certain information elements (IEs) of **SAE-Commit** messages of WPA3 authentication sequence using SAE-encrypted management frames (802.11w). **Scalar** and **Finite-Field** elements may be overridden with arbitrary hex strings, provoking authentication failure. Below are documented example test cases and their expected behavior.

1. Initial Setup for WPA3-Authentication Testing with Simultaneous Authentication of Equals (SAE).

The setup requires AP and station NIC drivers capable of enabling SAE encryption (this example uses MediaTek radios with ath10k(988x) driver), enabling encrypted management frames (802.11w), enabling WPA3 and disabling WPA2-PSK authentication in both station and AP.

- A. Set up a virtual AP for testing.
In this test, it is named `vap0000` on parent device `wiphy0`.
For more information see [Create VAP in Bridge Mode](#)
- B. On a separate radio, create a station to authenticate with `vap0000`:
In the **Port Manager** tab, select `wiphy1` and click **Create**; select **WiFi STA**, then click **Apply**.
In this test, the station is named `wlan1` on parent device `wiphy1`.
For more information see [Generating Traffic for WLAN Testing](#)
- C. Configure `vap0000` and `wlan1` to use **WPA3-SAE** encrypted authentication.
Ensure that `802.11w` is enabled, since it is required for WPA3.
For more information see [Setting up WPA3](#)
- D. Configure `vap0000` and `wlan1` with **SSID** `test-wpa2-psk` and **Keyphrase** `qwertyuiop`.
- E. Create a Monitor Port on its own radio to sniff wireless packets.
In this test, the monitor port is named `moni3a`.
For more information see [Using Wireshark to Sniff WiFi Monitors](#)

2. Control (No Change):

- A. Configure **Custom WiFi** in `vap0000`:
Select `vap0000` and click **Modify**.
Navigate to the **Custom WiFi** tab.
Ensure that no `sae_commit_override` parameter is set in **User-Specified supplicant/hostapd configuration text**.
Click **Apply** then **OK**.
- B. Set the vAP down and back up to allow changes to take effect:
In the **Port Manager** tab, select `vap0000`.
Admin all selected interfaces **DOWN** (CTRL-PLUS).
Admin all selected interfaces **UP** (CTRL-MINUS).
- C. Sniff packets to observe the authentication behavior:
On the observation system in the **Port Manager** tab, select only `moni3a`:
Click **Sniff Packets**.
- D. Observe the results, which should be similar to the following:
 - Packets are not malformed.
 - The station `wlan1` succeeds in authenticating with `vap0000`.
 - RSN Information Element is found in **EAPOL-Key Message 3 of 4** sent by `vap0000` with WPA-Key-Data field.

E. Example results and expected behavior:

A. **SAE-Commit** Message: Control Test

B. **SAE-Confirm** Message: Control Test

C. Behavior in LANforge **Wifi Messages**: Control Test (1)

D. Behavior in LANforge **Wifi Messages**: Control Test (2)

3. SAE Commit Override:

A. Configure **Custom WiFi** in `vap0000`:

Select `vap0000` and click **Modify**.

Navigate to the **Custom WiFi** tab.

In the **User-Specified supplicant/hostapd configuration text** field, write (with no line breaks):

```
sae_commit_override=13ffbad00d215867a7c5ff37d87bb9bdb7cb116e520f71e8d7a794ca2606d537ddc6c099c40e7a25372b80a8fd443cd7dd222c8ea21b8ef372d4b3e316c26a73fd999cc79ad483eb826e7b3893ea332da68fa13224bcdeb4fb18b0584dd100a2c514.
```

Note the recognizable `'bad00d2'` in this hex.

Click **Apply** then **OK**.

B. Reset ports and sniff packets:

Repeat steps B through D of [Step 2](#).

C. Observe the results, which should be similar to the following:

- The station `wlan1` fails to authenticate with `vap0000`.
- The station `wlan1` cycles between scanning and association attempts.
- LANforge Wifi-Messages shows **CTRL-EVENT-SSID-TEMP-DISABLED** for `reason=CONN_FAILED`.
- No longer **Confirm** message is visible in the authentication sequence, rather **Deauthentication**.

D. Example results and expected behavior:

A. **SAE-Confirm** Message: Override Test

B. Behavior in LANforge **Wifi Messages**: Override Test