sales@candelatech.com
support@candelatech.com
+1 (360) 380-1618 [PST, GMT -8]

Corrupting EAPOL-Key 3/4 Handshake Message RSNE WPA-Key Information Elements

Goal: Manually override RSN-related information elements of 3 of 4-way EAPOL authentication handshake messages sent by a LANforge system in AP Mode for testing purposes.

In this test scenario a LANforge system acts as a WiFi access point configured to use WPA2 authentication. The `rsne_override_eapol` field in LANforge Custom WiFi Parameters provides means to corrupt or customize certain information elements (IEs) in the third of four messages comprising EAPOL authentication "handshake". These IEs contain information about RSN encryption, including Pre-Shared Key (PSK) information required by 802.11 protocol for authentication success. Thus, such IEs may be overriden for the purpose of testing behavior under faulty authentication. Listed below is an example test case, of which documentation may be found in the hostap repository.

---

1. **Initial Setup for WPA2-Authentication Testing.**
   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 WPA2-PSK encrypted authentication.
   For more information see WPA2-Authentication Test Scenario

   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 `rsne_override_eapol` parameter is set in **User-Specified supplicant/hostapd configuration text**.
   Click **Apply** then **OK**.

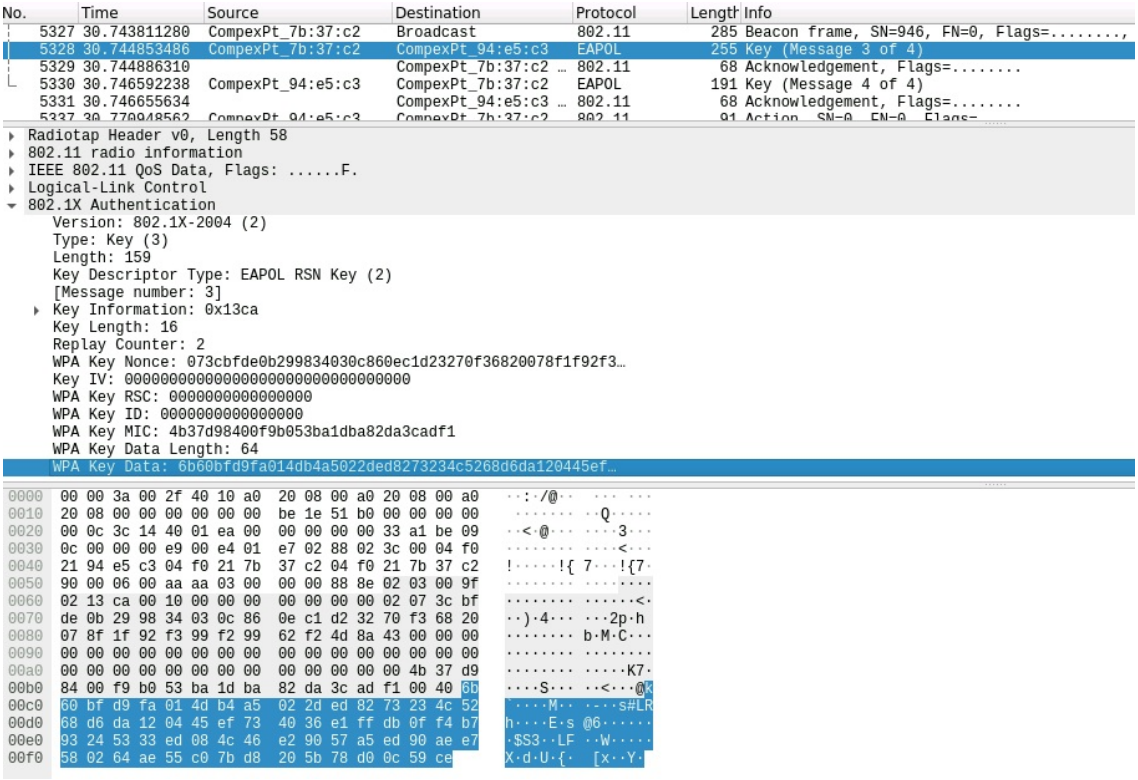
   B. Set the vAP down and back up to allow changes to take effect:
   In the **Port Manager** tab, select `vap0000`.
   Admin all selected interfaces **DOWN** (CTRL-PLUS).
   Admin all selected interfaces **UP** (CTRL-MINUS).

   C. Sniff packets to observe the authentication behavior:
   On the observation system in the **Port Manager** tab, select only `moni3a`:
   Click **Sniff Packets**.

   D. Reset the station to force re-authentication:
   In the **Port Manager** tab, select only `wlan1`.
   Click **Reset Port**.

E. 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.

F. Example results:



3. **RSNE Mismatch in EAPOL-Key Message 3/4:**

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:
`rsne_override_eapol=30140100000fac040100000fac040100000fac020c80`.
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 WPA-Key-Data field `EAPOL-Key Message 3 of 4` sent by `vap0000` is changed.
- The frame following `EAPOL-Key Message 3 of 4` sent by `vap0000` has type `DEAUTH`.

D. Example results: