

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_eapo1` 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 overridden 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_eapo1` 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:

No.	Time	Source	Destination	Protocol	Length	Info
5327	30.743811280	CompexPt_7b:37:c2	Broadcast	802.11	285	Beacon frame, SN=946, FN=0, Flags=.....
5328	30.744853486	CompexPt_7b:37:c2	CompexPt_94:e5:c3	EAPOL	255	Key (Message 3 of 4)
5329	30.744886310	CompexPt_7b:37:c2	CompexPt_7b:37:c2	802.11	68	Acknowledgement, Flags=.....
5330	30.746592238	CompexPt_94:e5:c3	CompexPt_7b:37:c2	EAPOL	191	Key (Message 4 of 4)
5331	30.746655634	CompexPt_94:e5:c3	CompexPt_94:e5:c3	802.11	68	Acknowledgement, Flags=.....
5337	30.770918562	CompexPt_94:e5:c3	CompexPt_7b:37:c2	802.11	91	Action, SN=0, FN=0, Flags=.....

```

▶ Radiotap Header v0, Length 58
▶ 802.11 radio information
▶ IEEE 802.11 QoS Data, Flags: .....F.
▶ Logical-Link Control
▼ 802.1X Authentication
  Version: 802.1X-2004 (2)
  Type: Key (3)
  Length: 159
  Key Descriptor Type: EAPOL RSN Key (2)
  [Message number: 3]
  ▶ Key Information: 0x13ca
    Key Length: 16
    Replay Counter: 2
    WPA Key Nonce: 073cbfde0b299834030c860ec1d23270f36820078f1f92f3...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 4b37d98400f9b053ba1dba82da3cadf1
    WPA Key Data Length: 64
    WPA Key Data: 6b60bfd9fa014db4a5022ded8273234c5268d6da120445ef...
0000 00 00 3a 00 2f 40 10 a0 20 08 00 a0 20 08 00 a0  ..:/0...
0010 20 08 00 00 00 00 00 00 be 1e 51 b0 00 00 00 00  ..:..0...
0020 00 0c 3c 14 40 01 ea 00 00 00 00 33 a1 be 09  ..<@...3...
0030 0c 00 00 00 e9 00 e4 01 e7 02 88 02 3c 00 04 f0  ..<...<...
0040 21 94 e5 c3 04 f0 21 7b 37 c2 04 f0 21 7b 37 c2  !...!{7...!{7...
0050 90 00 06 00 aa aa 03 00 00 00 88 8e 02 03 00 9f  ..:..:..<...
0060 02 13 ca 00 10 00 00 00 00 00 00 00 02 07 3c bf  ..:..:..<...
0070 de 0b 29 98 34 03 0c 86 0e c1 d2 32 70 f3 68 20  ..).4...2p.h...
0080 07 8f 1f 92 f3 99 f2 99 62 f2 4d 8a 43 00 00 00  ..:..:..b.M.C...
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..:..:..:..:..:..
00a0 00 00 00 00 00 00 00 00 00 00 00 00 00 4b 37 d9  ..:..:..:..:..K7...
00b0 84 00 f9 b0 53 ba 1d ba 82 da 3c ad f1 00 40 6b  ..:..S...<...@K...
00c0 60 bf d9 fa 01 4d b4 a5 02 2d ed 82 73 23 4c 52  ..:..M...s#LR...
00d0 68 d6 da 12 04 45 ef 73 40 36 e1 ff db 0f f4 b7  h...E.s@6...
00e0 93 24 53 33 ed 08 4c 46 e2 90 57 a5 ed 90 ae e7  .$$3...LF..W...
00f0 58 02 64 ae 55 c0 7b d8 20 5b 78 d0 0c 59 ce  X.d.U.f. [x.Y.f

```

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_eapo1=3014010000fac04010000fac04010000fac020c80.
```
 - 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:

No.	Time	Source	Destination	Protocol	Length	Info
2075...	1342.4271368...	CompexPt_94:e5:c3	CompexPt_7b:37:c2	EAPOL	231	Key (Message 2 of 4)
2075...	1342.4272044...	CompexPt_94:e5:c3	CompexPt_94:e5:c3	802.11	68	Acknowledgement, Flags=.....
2075...	1342.4299094...	CompexPt_7b:37:c2	CompexPt_94:e5:c3	EAPOL	247	Key (Message 3 of 4)
2075...	1342.4300088...	CompexPt_7b:37:c2	CompexPt_7b:37:c2	802.11	68	Acknowledgement, Flags=.....
2075...	1342.4417432...	CompexPt_94:e5:c3	CompexPt_7b:37:c2	802.11	84	Deauthentication, SN=266, FN=0, Flags=.....
2075...	1342.4417720...	CompexPt_94:e5:c3	CompexPt_94:e5:c3	802.11	68	Acknowledgement, Flags=.....
2076...	1342.5040532...	CompexPt_7b:37:c2	CompexPt_54:86:8a	802.11	279	Probe Response, SN=326, FN=0, Flags=.....

```

BSS Id: CompexPt_7b:37:c2 (04:f0:21:7b:37:c2)
STA address: CompexPt_94:e5:c3 (04:f0:21:94:e5:c3)
..... = Fragment number: 0
0000 0000 1001 .... = Sequence number: 9
  Qos Control: 0x0006
  Logical-Link Control
  802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: Key (3)
    Length: 151
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 3]
  Key Information: 0x13ca
    Key Length: 16
    Replay Counter: 2
    WPA Key Nonce: 69cb202fff701e663bb454cb2dd25216af7c1882c8ae39bb...
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 86b7cc8091558cbe6905cbf8103dc7ad
    WPA Key Data Length: 56
    WPA Key Data: 8a5910a7drc7dd6c7c3019e82fc0ead5e07389fa3b151b85...
0000 00 00 3a 00 2f 40 10 a0 20 08 00 a0 20 08 00 a0  ..:/@..
0010 20 08 00 00 00 00 00 00 4e d4 11 4c 00 00 00 00  ..L...
0020 00 0c 3c 14 40 01 e9 00 00 00 00 00 c9 d7 b4 09  ..<@...
0030 0c 00 00 00 e8 00 e6 01 e3 02 88 02 3c 00 04 f0  ..<...
0040 21 94 e5 c3 04 f0 21 7b 37 c2 04 f0 21 7b 37 c2  !.....!{ 7...!{7...
0050 90 00 06 00 aa aa 03 00 00 00 88 8e 02 03 00 97  ..<...
0060 02 13 ca 00 10 00 00 00 00 00 00 00 00 02 09 cb 20  ..<...i...
0070 2f ff 70 1e 66 3b b4 54 cb 2d d2 52 16 af 7c 18  /..p.F;..T..R..|..
0080 82 c8 ae 39 bb 6d c5 93 41 c9 16 74 92 00 00 00  ..9.m..A..t...
0090 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..<...
00a0 00 00 00 00 00 00 00 00 00 00 00 00 86 b7 cc  ..<...
00b0 89 15 58 cd be 69 05 cb f8 10 3d c7 ad 00 38 8a  ..X..i...=...8...
00c0 59 10 a7 bf c7 dd 6c 7c 30 19 e8 2f c0 ea d5 e0  Y.....| 0.../...
00d0 73 89 fa 3b 15 1b 85 12 fb 9d 89 73 d8 3d 23 ce  s.....s=#...
00e0 83 c6 b7 30 12 e4 4e e4 b4 29 20 4a b4 d8 1c da  ...0.N..) J...
00f0 86 c7 f1 1e 96 3a cf  ..<...

```