3. Raspberry Pi Operation in the Field

Intended Audience

Field tech support

Mandatory Items You Will Need

- One Raspberry Pi running Kali Linux
- Username and password for an account that can have root privileges on that Raspberry Pi (default at the time of this writing is `kali` / `D0rm@!` however note that console login is unreliable on Kali as logins with the correct username and password have been witnessed to bounce back to the login screen inexplicably with no known limit to the number of bounces. If this happens, use CTRL+ALT+F1 to get a terminal instead.)
- Raspberry Pi power supply
- Wi-Fi network SSID name and password that the lock is on

Optional Items You May Need

If you are using another computer to connect to the Raspberry Pi

- Ethernet cable

Handy items for direct connection with the Raspberry Pi

- USB* Mouse
- USB* Keyboard
- Monitor with monitor cable ending in micro-HDMI (e.g. the cable in the Miuzei kit is HDMI to micro-HDMI, etc.)
- Monitor power cable

If you cannot power cycle the lock

- USB* Wi-Fi antenna that can inject packets (e.g. Alfa AWUS036NHA https://www.alfa.com.tw/products/awus036nha?variant=36473966166088, etc.)

Notes

* = The Raspberry Pi's USB ports do not have much clearance, make sure the form factors of all the connectors do not obstruct another!

Connect to the Raspberry Pi

The Raspberry Pi supports connection via:

- SSH (requires the ethernet cable above, another computer on the same network, and the IP address of the Raspberry Pi)
- VNC (requires the ethernet cable above, another computer on the same network and the IP address of the Raspberry Pi)
- Direct connection (requires the "handy items for direction connection" indicated above) - Note that this is unreliable on Kali as logins with the correct username and password have been witnessed to bounce back to the login screen inexplicably with no known limit to the number of bounces. If this happens, use CTRL+ALT+F1 to get a terminal instead.

Procedures to connect are not detailed in this document as the myriad ways of doing so would make this document very confusing. The only thing that is common is that the Raspberry Pi power supply must be connected to the Raspberry Pi and the local electrical grid. What is needed at the end of any connection method is a command line terminal on the Wi-Fi sniffer.

Once Connected

Conventions:

- Console commands and text from the console will be in `monospace text`.
- Placeholder text will be inside chevrons (e.g. `<placeholder text>`, etc.). Change everything from the opening chevron to the closing chevron, including both chevrons, to match the current situation.
- In places with a lot of text where something specific is being sought, the sought item(s) is(are) highlighted in green. Text coloration has not been included for any console output as the myriad ways of connecting may result in different colour schemes being presented.

Put Wi-Fi Antenna into Monitor Mode and Begin Capturing

Before beginning, make sure all devices that should not be on the Wi-Fi network of the lock are disconnected. For example, if your laptop, smartphone, and/or tablet are connected to the Wi-Fi network of the lock, disconnect it from that network. Do your best to make sure only devices that were connected at the time the phenomenon being investigated occurred are connected when you start.

In this command-line terminal (referred to below with steps beginning with A), execute the following commands:

Step #	Command (Use Only One Line, No Newlines)	Resulting Text Should be Similar To	Actions

A1	`sudo airmon-ng check kill`	`Killing these processes:`
		
		`  PID Name`
		`  416 dhclient`
		`  617 wpa_supplicant`
			N/A

A2	`sudo airmon-ng start wlan0`	`PHY  Interface  Driver  Chipset`
		
		`phy0  wlan0  brcmfmac  Broadcom 43430`
		`  (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)`
		`command failed: Unknown error 524 (-524)`
		`  (mac80211 station mode vif disabled for [phy0]wlan0)`
			The error message is normal. Run the command `ifconfig` and verify that in the resulting text, there is a paragraph describing the interface wlan0mon similar to the text in green below:
			
			`eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500`
			`  inet 192.168.50.78  netmask 255.255.255.0  broadcast 192.168.50.255`
			`  inet6 fe80::da3a:ddff:fec3:9bcb  prefixlen 64  scopeid 0x20<link>`
			`  ether d8:3a:dd:c3:9b:cb  txqueuelen 1000  (Ethernet)`
			`  RX packets 1234  bytes 128159 (125.1 KiB)`
			`  RX errors 0  dropped 0  overruns 0  frame 0`
			`  TX packets 220  bytes 42510 (41.5 KiB)`
			`  TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0`
			
			`lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536`
			`  inet 127.0.0.1  netmask 255.0.0.0`
			`  inet6 ::1  prefixlen 128  scopeid 0x10<host>`
			`  loop  txqueuelen 1000  (Local Loopback)`
			`  RX packets 0  bytes 0 (0.0 B)`
			`  RX errors 0  dropped 0  overruns 0  frame 0`
			`  TX packets 0  bytes 0 (0.0 B)`
			`  TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0`
			
			`wlan0mon: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500`
			`  unspec 00-00-00-00-00-00-00-4C-00-00-00-00-00-00-00-00  txqueuelen 1000  (UNSPEC)`
			`  RX packets 392  bytes 69673 (68.0 KiB)`
			`  RX errors 0  dropped 392  overruns 0  frame 0`
			`  TX packets 0  bytes 0 (0.0 B)`
			`  TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0`

A3	`sudo airodump-ng --essid <SSID lock is on> wlan0mon`	`CH  1 ][ Elapsed: 1 min ][ 2024-09-10 17:27`
		
		`BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID`
		
		`EC:8C:A2:25:F6:58 -74 49 0 0 1 260 WPA2 CCMP PSK LyazonIntegration`
		
		`BSSID STATION PWR Rate Lost Frames Notes Probes`
		
		`(not associated) 1E:13:47:B6:32:2D -79 0 - 1 0 1`
		`(not associated) 20:33:BF:A9:DD:FC -71 0 - 6 0 1`
		`(not associated) 34:43:8C:F0:C1:BB -82 0 - 6 0 1`
		`(not associated) 48:29:52:FC:89:3A -27 0 - 1 0 5`
		`(not associated) 5A:A1:19:96:C9:99 -76 0 - 1 0 2`
		`(not associated) 6C:6A:8D:68:3E:28 -38 0 - 6 0 4`
		`(not associated) 7A:54:B8:54:69:F7 -67 0 - 5 0 1`
		`(not associated) 80:6F:D9:A5:BC:06 -65 0 - 1 0 2`
		`(not associated) 90:5B:AD:1D:D6:C5 -76 0 - 1 0 10`
		`(not associated) 0C:31:78:03:91:B4 -80 0 - 1 0 1`
		`(not associated) A4:16:66:41:F2:93 -82 0 - 1 0 1`
		`(not associated) B2:58:74:19:62:22 -77 0 - 1 0 1`
		`(not associated) CC:A2:66:7C:C2:31 -76 0 - 1 0 2`
		`(not associated) D0:DB:D1:EE:75:60 -55 0 - 6 0 3`
		`EC:8C:A2:25:F6:58 D4:3D:39:10:C1:48 -49 0e - 1 0 33`
			In the first table's ESSID column, record from that row:
			
			• `BSSID`
			• `CH` (channel number)
			
			For locks with firmware greater than 00.15.13, you can get your device's `STATION` (MAC) straight from Device Manager. Otherwise, it might be hard to pinpoint which one is the device exhibiting the behaviour that needs investigating.
			
			For locks with firmware less than or equal to 00.15.13, take that BSSID and locate one entry in the second table's BSSID column that matches the BSSID found above and record from that row (you may need to show a credential to the lock of interest on this Wi-Fi SSID to see this):
			
			• `STATION` (MAC)
			
			Note that for Lyazon devices, these should all begin with `D4:3D:39`.
			
			For example, for Wi-Fi SSID LyazonIntegration:
			
			• `BSSID = EC:8C:A2:25:F6:58`
			• `CH (Channel) = 1`
			• `STATION = D4:3D:39:10:C1:48`
			
			--- 	
			
			Space provided for you to record the above here:
			
			• `BSSID =`
			• `CH (Channel) =`
			• `STATION =`

A4	`sudo airodump-ng --essid <SSID lock is on> --channel <CH> wlan0mon --write ~/<YYYY-MM-DD_HH:MM_SiteName_SuiteNumber>`	`CH  1 ][ Elapsed: 6 s ][ 2024-08-15 15:21`
		
		`BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID`
		
		`EC:8C:A2:25:F6:58 -74 100 49 0 0 1 260 WPA2 CCMP PSK LyazonIntegration`
			Make a device join the Wi-Fi network of the lock. Some ways to accomplish this are:
			
			• Power cycle the lock (requires access to the suite as the lock's power supply is inside and a T10 screwdriver)
			• Connect a new lock to the Wi-Fi network (requires a spare lock, a smartdevice with a commissioning app, Wi-Fi SSID, and Wi-Fi password)
			• Force deauthorisation of a device and let it reconnect see the following optional section

Mandatory: Either Reboot the Lock or Force Deauthorisation

The data traffic between the lock and the Access Point is encrypted. In order to properly decrypt the capture, you **MUST** also capture the association process between the lock and the Access Point. Start the capture processing first, then use one of the options listed here to cause the re-association to happen. Also **remember to record the SSID name and password**. This information is also mandatory to decrypt the capture.

Options for causing the lock to re-associate with the Access Point include:

1. Power cycle the lock by pulling the batteries for at least 10 seconds then re-installing them.
2. Soft reboot the lock using *#9# from the keypad
3. Use the Raspberry Pi to force a deauthorization and re-association.

The "force deauthorization" option requires the optional USB Wi-Fi antenna above. Without interrupting the capturing terminal, open a second brand new terminal (referred to below with steps beginning with B) to the Wi-Fi sniffer and do the following operations:

Step #	Command (Use Only One Line, No Newlines)	Resulting Text Should be Similar To	Actions
B1	`sudo aireplay-ng --test wlan1`	`17:12:25  Trying broadcast probe requests...` `17:12:25  Injection is working!`	N/A
B2	`sudo ifconfig wlan1 down`	N/A	N/A
B3	`sudo iwconfig wlan1 mode monitor`	N/A	N/A
B4	`sudo iwconfig wlan1 channel <CH>`	N/A	N/A
B5	`sudo ifconfig wlan1 up`	N/A	N/A

B6	`sudo aireplay-ng --deauth 5 -a <BSSID> -c <STATION> wlan1`	`17:48:34  Waiting for beacon frame (BSSID: EC:8C:A2:25:F6:58) on channel 1`
		`17:48:35  Sending 64 directed DeAuth (code 7). STMAC: [D4:3D:39:10:C1:48] [ 2|46 ACKs]`
		`17:48:35  Sending 64 directed DeAuth (code 7). STMAC: [D4:3D:39:10:C1:48] [ 7|69 ACKs]`
		`17:48:36  Sending 64 directed DeAuth (code 7). STMAC: [D4:3D:39:10:C1:48] [59|61 ACKs]`
		`17:48:36  Sending 64 directed DeAuth (code 7). STMAC: [D4:3D:39:10:C1:48] [57| 3 ACKs]`
		`17:48:37  Sending 64 directed DeAuth (code 7). STMAC: [D4:3D:39:10:C1:48] [77|30 ACKs]`
			`exit`

(The last action in B6 is to send the exit the second terminal you opened on the Wi-Fi sniffer, thereby closing it.)

Capture Initial Verification

Capturing has begun and is running in the first terminal (referred to above and below with steps beginning with A). Return to it.

Step #	Action	Verification

A5	Inspect the first terminal. The text there should be similar to the following:
	
	`CH  1 ][ Elapsed: 36 s ][ 2024-09-10 17:48 ][ WPA handshake: EC:8C:A2:25:F6:58`
	
	`EC:8C:A2:25:F6:58  -74  49  0  0  1  260  WPA2 CCMP  PSK  LyazonIntegration`
	
	`BSSID  STATION  PWR  Rate  Lost  Frames  Notes  Probes`
	
	`(not associated)  1E:13:47:B6:32:2D  -79  0  -1  0  1`
	`(not associated)  20:33:BF:A9:DD:FC  -71  0  -6  0  1`
	`(not associated)  34:43:8C:F0:C1:BB  -82  0  -6  0  1`
	`(not associated)  48:29:52:FC:89:3A  -27  0  -1  0  5`
	`(not associated)  5A:A1:19:96:C9:99  -76  0  -1  0  2`
	`(not associated)  6C:6A:8D:68:3E:28  -38  0  -6  0  4`
	`(not associated)  7A:54:B8:54:69:F7  -67  0  -5  0  1`
	`(not associated)  80:6F:D9:A5:BC:06  -65  0  -1  0  2`
	`(not associated)  90:5B:AD:1D:D6:C5  -76  0  -1  0  10`
	`(not associated)  0C:31:78:03:91:B4  -80  0  -1  0  1`
	`(not associated)  A4:16:66:41:F2:93  -82  0  -1  0  1`
	`(not associated)  B2:58:74:19:62:22  -77  0  -1  0  1`
	`(not associated)  CC:A2:66:7C:C2:31  -76  0  -1  0  2`
	`(not associated)  D0:DB:D1:EE:75:60  -55  0  -6  0  3`
	`EC:8C:A2:25:F6:58  D4:3D:39:10:C1:48  -49  0e-1  0  33  EAPOL  LyazonIntegration`
		If you see on any row in the second table below all of the following in the same row:
		
		- In the `Notes` column, `EAPOL`
		- In the `BSSID` column, the BSSID recorded above
		
		everything needed to have a complete capture is done. If this is not there, repeat the action of step A4 (make a device join the Wi-Fi network of the lock) until it does.

A6	If there are specific conditions that the phenomenon being investigated happen in, do them a few times now (e.g. it happens when a bad code credential is entered, it happens after half an hour, etc.). If there are no specific conditions, just let the capture keep running.	No specific verifications on this end of things, do any phenomenon-specific verifications that were indicated.

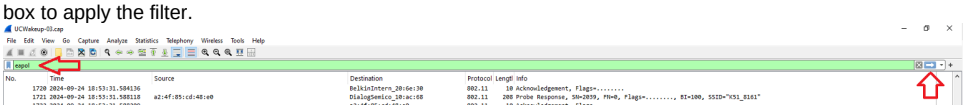
A7	When it is time to stop the capture, activate the terminal that the capture is happening in and press: q	CH 1][Elapsed: 36 s][2024-09-10 17:48][Are you sure you want to quit? Press Q again to quit. EC:8C:A2:25:F6: 58 -74 49 0 0 1 260 WPA2 CCMP PSK LyazonIntegration BSSID STATION PWR Rate Lost Frames Notes Probes (not associated) 1E:13:47:B6:32: 2D -79 0 - 1 0 1 (not associated) 20:33:BF:A9:DD: FC -71 0 - 6 0 1 (not associated) 34:43:8C:F0:C1: BB -82 0 - 6 0 1 (not associated) 48:29:52:FC:89: 3A -27 0 - 1 0 5 (not associated) 5A:A1:19:96:C9: 99 -76 0 - 1 0 2 (not associated) 6C:6A:8D:68:3E: 28 -38 0 - 6 0 4 (not associated) 7A:54:B8:54:69: F7 -67 0 - 5 0 1 (not associated) 80:6F:D9:A5:BC: 06 -65 0 - 1 0 2 (not associated) 90:5B:AD:1D:D6: C5 -76 0 - 1 0 10 (not associated) 0C:31:78:03:91: B4 -80 0 - 1 0 1 (not associated) A4:16:66:41:F2: 93 -82 0 - 1 0 1 (not associated) B2:58:74:19:62: 22 -77 0 - 1 0 1 (not associated) CC:A2:66:7C:C2: 31 -76 0 - 1 0 2 (not associated) D0:DB:D1:EE:75: 60 -55 0 - 6 0 3 EC:8C:A2:25:F6:58 D4:3D:39:10:C1: 48 -49 0e- 1 0 33 EAPOL LyazonIntegration
A8	Confirm stopping the capture by pressing: q	N/A

Optional: After Capture Validation

Because capturing the association process between the lock and the access point is so critical, you might want to validate that the association process was properly captured and none of the packets were dropped. There are four (4) packets in the association process, and all four packets must be captured.

Use WireShark either on the Raspberry Pi or extract the capture to your PC.

1. Open the capture file in WireShark
2. Apply an eapol display filter by entering "eapol" (without the quotes) in the "Apply a display filter..." box and press the arrow in the right side of that box to apply the filter.



3. Verify that all four EAPOL packets are present in the capture and that the exchange is between the lock and the Access Point.