DEPARTAMENTO DE ELETRÓNICA, TELECOMUNICAÇÕES E INFORMÁTICA
MESTRADO INTEGRADO EM ENG. DE COMPUTADORES E TELEMÁTICA

ARQUITETURA DE REDES

Objectives

- Wi-Fi networks:
  - Joining a BSS and communication.
  - Authentication.
  - Open and WPA2 protected networks

1. With a Linux OS PC (PC1), configure it as a wireless monitoring node by adding a monitoring virtual wireless device (mon0) listening a specific channel and start a capture with Wireshark in that interface.
Analyze the capabilities of your wireless interface:

```
iw phy phy0 info
iw dev
```

To add a monitoring virtual wireless device (mon0) (as root or with sudo):

```
iw phy phy0 interface add mon0 type monitor
rfkill unblock 0
ip link set up dev mon0                    or "ifconfig mon0 up"
```

With "iw dev" identify the main wireless interface and delete it:

```
iw dev wlp1s0 del
```

Define the listening channel:

```
iw dev mon0 set channel <channel_number>
```

Note 1: Use iw dev and rfkill list commands to determine the wireless physical identifiers (if different from phy0 and 0, respectively)
Note 2: **If the channel assignment fails, disable/enable the Network-Manager service and applet and wireless interface, e.g.:**
Debian/Ubuntu:

```
service network-manager [stop|start]
killall nm-applet
ip link set [down|up] dev wlan0
```

Arch:

```
systemctl [stop|start] NetworkManager
killall nm-applet
ip link set [down|up] dev wlp1s0
```

Note3: To restore the initial configuration, reboot your PC.

2. Connect other wireless terminal (PC2) to a open wireless network with the correct parameters (SSID, Security – None), and test connectivity with the AP. At PC1, using a visualization filter to capture all wireless frames from (or to) PC2. Analyze the exchanged packets/frames and their content.
>>Explain how the association process is performed.

Filtering Wireless Layer 2 Information

Configure a Wireshark visualization filter to analyze the management packets:

```
wlan.fc.type_subtype==x
      x=0 association request
        10 diassociation
        2 reassociation request
        1 association response
        3 reassociation response
        4 probe request
        5 probe response
        8 beacon
        11 authentication
        12 deauthentication
        13 ACK
        27 RTS
        28 CTS
        40 Data
```

To analyze all the management packets but the beacons, configure the following Wireshark visualization filter (remove beacons and analyze packets from or to PC2):

```
not wlan.fc.type_subtype==8 && wlan.addr == mac_pc
```

3. Reconnect PC2 to the wireless network and test the connectivity with the AP through wireless. Exchange ICMP packets (ping) between PC2 and the AP or other wireless terminal.
>> Analyze the exchanged packets/frames during the association and authentication phase.
>> Explain how the data transmission is performed.

4. Now exchange very large ICMP packets (e.g. 1200 bytes, ping –s 1200) between PC2 and the AP. Analyze the exchanged packets/frames and their content. Explain how the transmission is now performed and analyze the differences between this and the previous experiences.
>> Explain the purpose of the RTS and CTS frames
Note: the AP must have a RTS/CTS threshold of 1000 bytes.
Note2: if PC2 is a Linux machine, the RTS/CTS threshold can be changed with: `iw phy phy0 set rts 1000`.

5. Connect now PC2 to a WPA2 secured wireless network with the correct parameters (SSID, Security – WPA2 Personal), and test connectivity with the AP. Analyze the exchanged packets/frames and their content.
>> Analyze the differences during the authentication process.
>> What 802.11 frames are used by the WPA2 Authentication?