Network Security Laboratory – Lecture 3

WIFI CRACKING (WEP + WPA)

Dott. Andrea Baffa
email: abaffa94@servizimicrosoft.unical.it

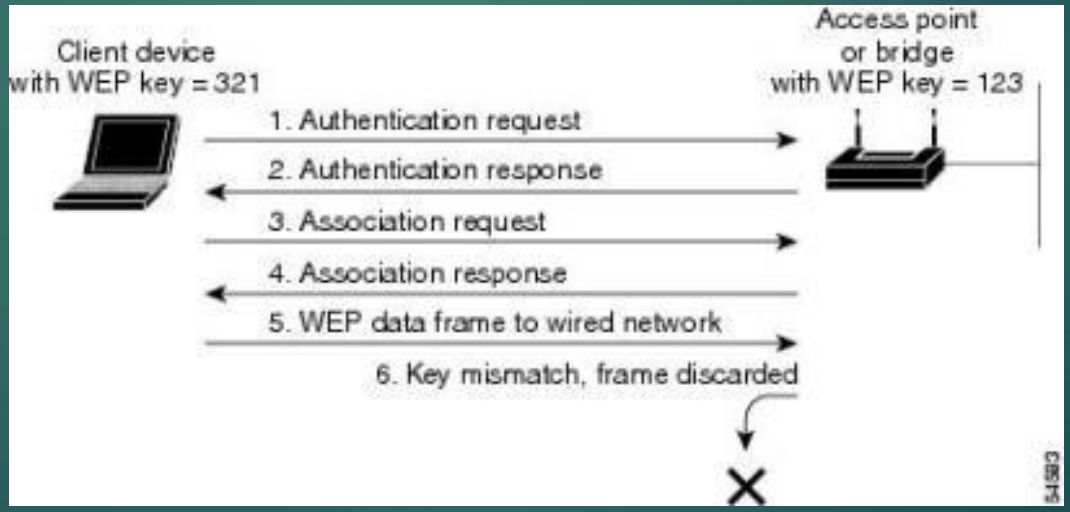
Wireless LAN (WLAN)

- is a wireless computer network that links two or more devices using wireless communication to form a local area network (LAN)
- Based on IEEE 802.11 protocol
- we can classify them according to the security protocols used. There are three types:
  - Open WLAN (without any kind of protection)
  - WEP
  - WPA

Wired Equivalent Privacy (WEP)

- Use a RC4 key, formed by the union of the KEY and the Initialization Vector (IV)

- WEP Negoziation:



Why WEP is weak

- WEP is considered vulnerable for many reason:
- Length of IV, just 24 bit
- Possibility of reuse of the IV
- All connections are encrypted with the same Pre Shared Key (PSK)

WEP Cracking

- Exploiting weakness of WEP
- sniffing enough data to have duplicates IV
- Use Aircrack-ng to discover WEP Key exploiting captured data

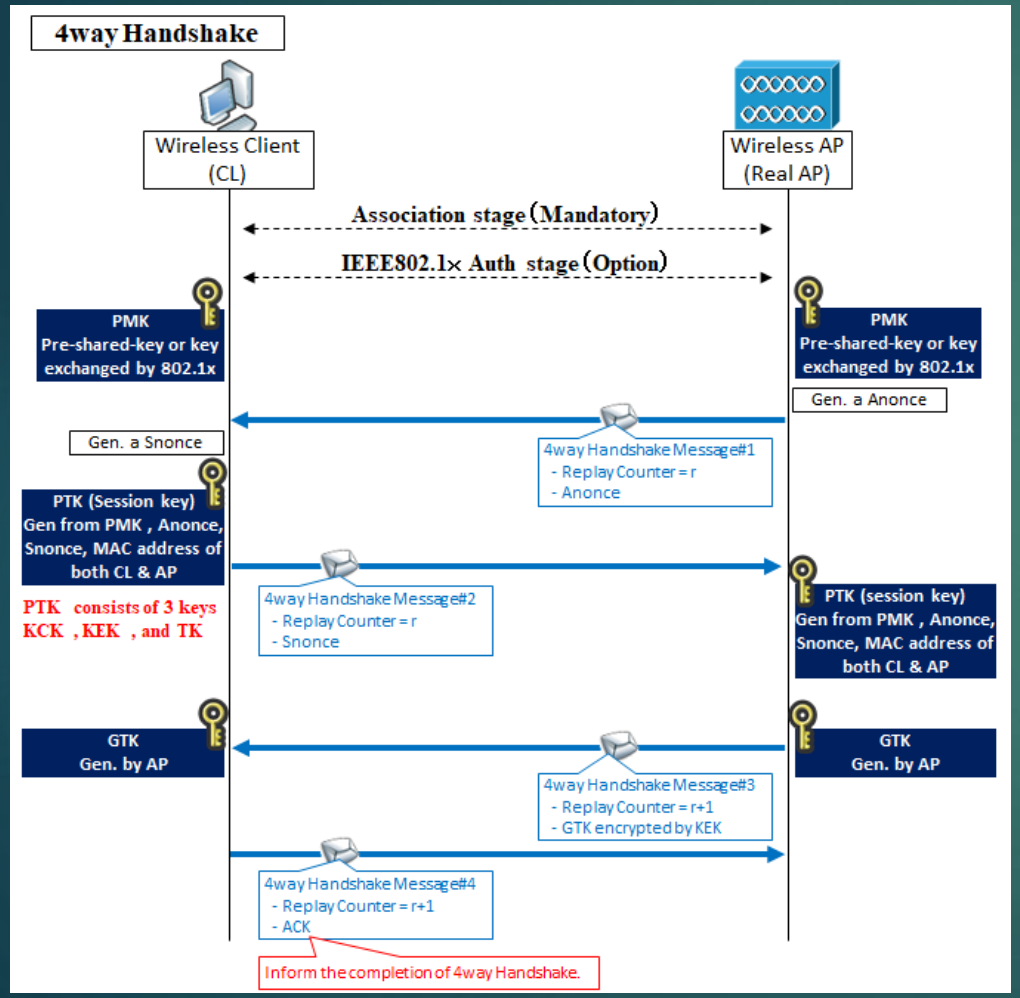
WEP Cracking - exercise

- Let's see a video for WEP attack
- Go on course website and download WEP Capture
- Using Aircrack-ng try to discover the key yourself, following the guide
- What is the password?
- And how the attack works?

WiFi Protected Access (WPA)

- WPA can be classified as WPA Personal or WPA Enterprise
- Our focus will be on WPA Personal, also known as WPA-PSK
- Based on a Pre Shared Key

WPA Personal Handshake



- This kind of handshake is based on mutual authentication.
  - Each host must provide the right PTK, derived on the PMK (the password of the network)
- The PTK is used to encrypt data
- Each connection has different PTK, so an hosts cannot decrypt conversation between another hosts and the AP, improving security of WPA

WPA Attacks

- We have some way to attack a WiFi protected with WPA
- Of course we can try a **bruteforce**, or **dictionary attack**, on the PMK
- But we also can try an attack on PSK with the **rainbow table attack**
  - PSK is a key of 256 bit derived from PMK, ESSID and some others parameters

WPA Cracking

- In order to perform some attack we must, at first, sniff the handshake
- Let's see a video for capturing the WPA Handshake
- Once we have the handshake we can perform some attacks in order to find the key

WPA Cracking - exercise

- On course Website there is a capture of the handshake, called wpa_capture
- Download and try to discover the password, using the guide available
- For rainbow table attack, you could either generate your own rainbow table or using the ones available on course website
- The goal of this exercise is to discover the password

Questions?

The lesson is over.

Thank you!