Network Security Laboratory Session 6

WIFI CRACKING (WEP + WPA)

Wireless LAN (WLAN)

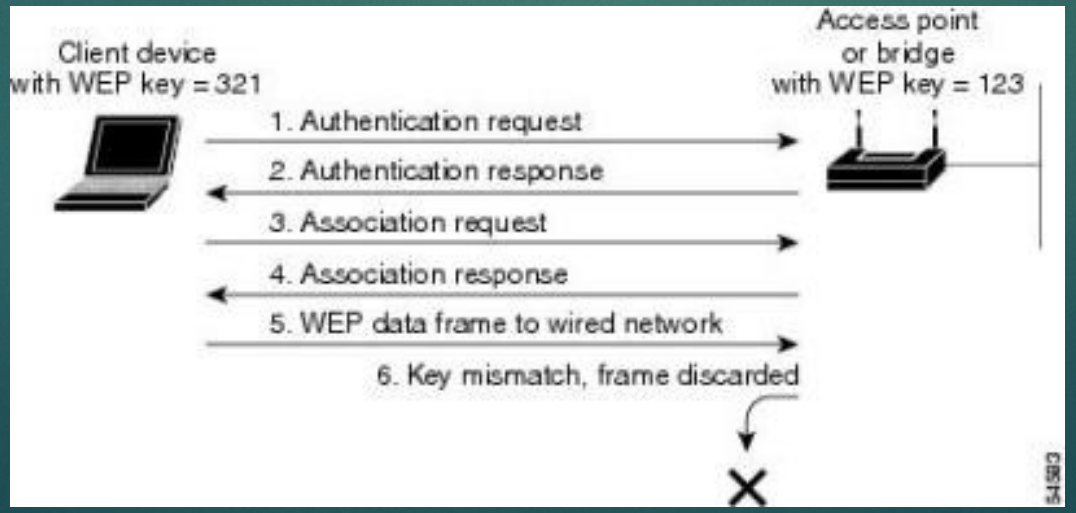
- A ***WLAN*** is a **W**ireless **L**ocal **A**rea **N**etwork that links two or more devices using wireless communication
- It is based on IEEE 802.11 protocol
- WLAN can be classified depending on the security protocols they use
- Three macro categories:
  - Open WLAN (no protection)
  - WEP (today is obsolete)
  - WPA (version 2 and 3)
    - WPA3 → More secure but …

Wired Equivalent Privacy (WEP)

WEP weaknesses:

- **Stream cipher**. Encryption algorithms applied to data streams, called stream ciphers, can be vulnerable to attack when a key is reused. The protocol's relatively small key space makes it impossible to avoid reusing keys
- **RC4 weaknesses.** The **RC4** algorithm itself has come under scrutiny for cryptographic weakness and is no longer considered safe to use. It makes use of an **Initialization Vector (IV)** combined with a **key** in order to crypt data.
  N.B.: the **IV** would be agreed on in advance by both the sender and the recipient. In addition, the IV can be transmitted independently or included as part of the session setup prior to message exchange
- **Shared key.** The default configuration for these systems uses a single shared key for all users. You can't authenticate individual users when all users share the same key

- WEP Negoziation:



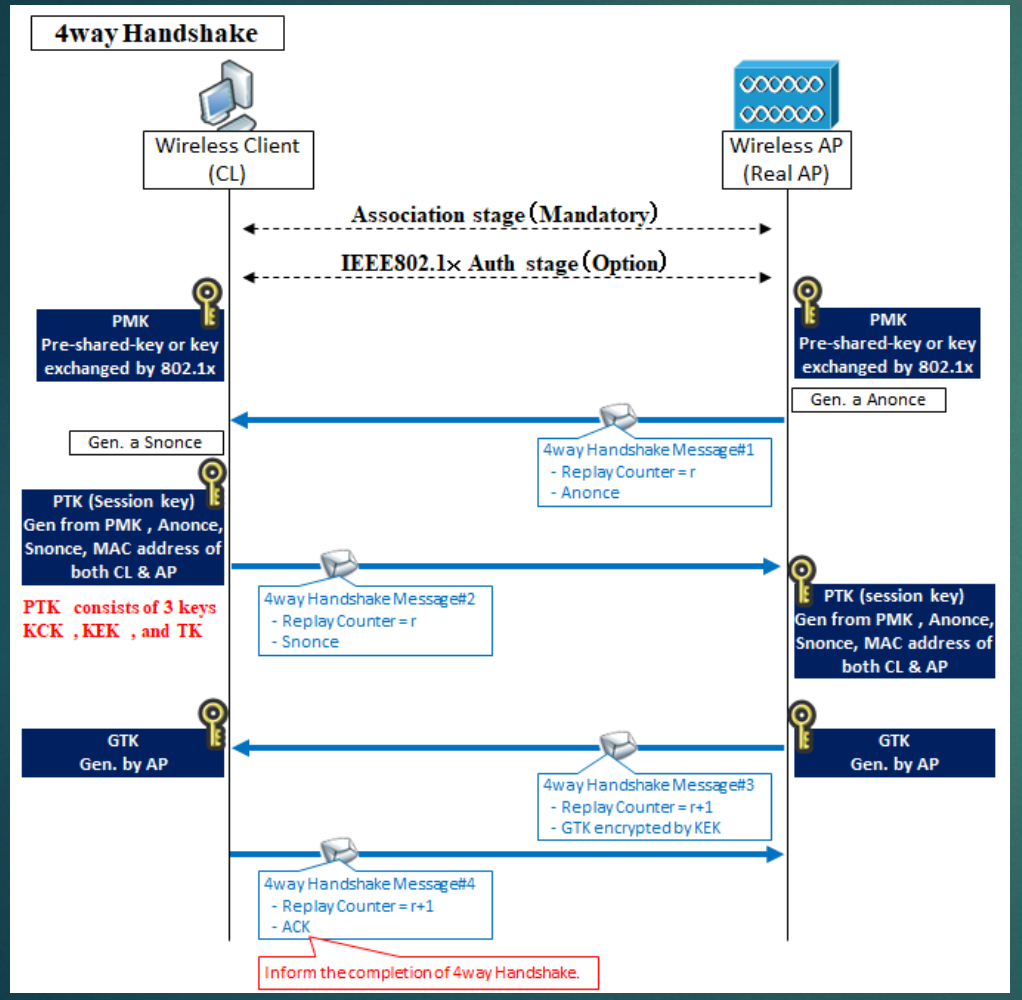
Why WEP is weak

- WEP is considered vulnerable for many other reasons:
- **IV length**: 24 bit
- The same IV can be reused more times
- All connections are encrypted with the same **P**re **S**hared **K**ey (**PSK**)

WiFi Protected Access (WPA)

- Several sub-catergories of WPA
  - WPA Personal
  - WPA Enterprise
- WPA Personal: most commonly used at home (also known as WPA-PSK)
- It is 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

1. Each connection uses different PTK
2. A third host **C** can't decrypt messages exchanged between the host **CL** (see image) and the **AP**
3. **Result:** WPA security improved

WPA Attacks

- We have several ways to discover WPA passwords
  - Bruteforce attacks
  - Dictionary based attacks

All these attacks are addressed to the PMK, but….

THEY REQUIRE TIME!

- Other types of attacks exploits the PSK
  - PSK is a key of 256 bit derived from PMK, ESSID and some others parameters
  - **Possible attack:** rainbow table attack