# Wifi-Protocol-1

20210638 최무송

Plan

- Contents of Wifi-protocol (week 1)

- WireShark + Security Vulnerability of Wifi-protocol (week 2)

- Security Vulnerability Attack practice with online platform (week 3)

IEEE 802.11 Wireless LAN (Wi-Fi)

- Technical Standard for Wireless LAN

- Started from 1997, currently revising
  - ex) Wifi 6E (802.11ax)

- Layer
  - Data Link Layer
  - Physical Layer

IEEE 802.11 Architecture

- Infrastructure mode
  - Access Point (Base station)
  - Basic Service Set (or cell)
    - cf. ESS

- Ad hoc mode

Internet

switch
or router

BSS 1

BSS 2
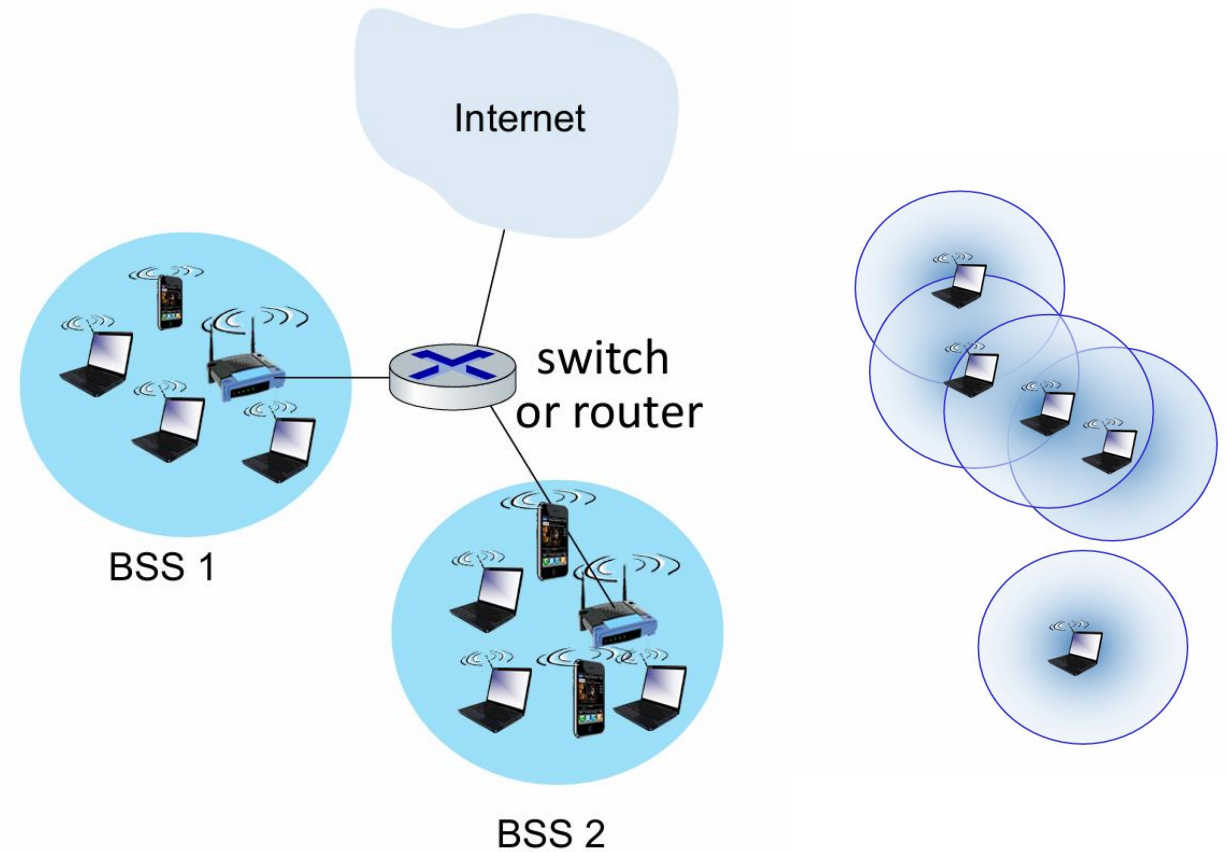
IEEE 802.11 Association

- Host scans channels & listening for Beacon Frames
  - Beacon frames: SSID(AP's name) + MAC address

- Select AP for authentication
  - EAPoL

- AP-Host association

- DHCP (host gets IP address)

내부 IP주소

192.168.0.1

서브넷 마스크

255.255.255.0

MAC 주소

B0:38:6C:1B:D3:C0

☐ 허브/AP모드 내부 게이트웨이 ⌄

사용중인 장치 정보   3개 사용중

192.168.0.4   28:DF:EB:09:5B:AA
무선연결 5GHz : 자동할당
DESKTOP-27HG6RG

Beacon frame

```
▼ IEEE 802.11 Beacon frame, Flags: ........
    Type/Subtype: Beacon frame (0x0008)
  ▼ Frame Control Field: 0x8000
      .... ..00 = Version: 0
      .... 00.. = Type: Management frame (0)
      1000 .... = Subtype: 8
    ▶ Flags: 0x00
    .000 0000 0000 0000 = Duration: 0 microseconds
  ▶ Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Transmitter address: Cisco_70:18:d0 (50:0f:80:70:18:d0)
  ▶ Source address: Cisco_70:18:d0 (50:0f:80:70:18:d0)
  ▶ BSS Id: Cisco_70:18:d0 (50:0f:80:70:18:d0)
    .... .... .... 0000 = Fragment number: 0
    1011 1101 1111 .... = Sequence number: 3039
    [WLAN Flags: ........]
```

IEEE 802.11 EAPoL

- EAP(Extensible Authentication Protocol) Encapsulation over LAN
- Authentication Framework
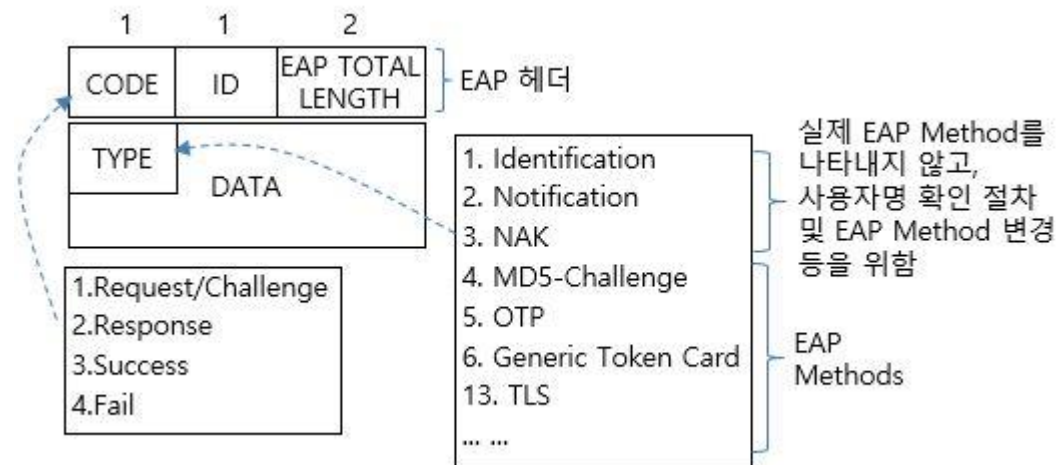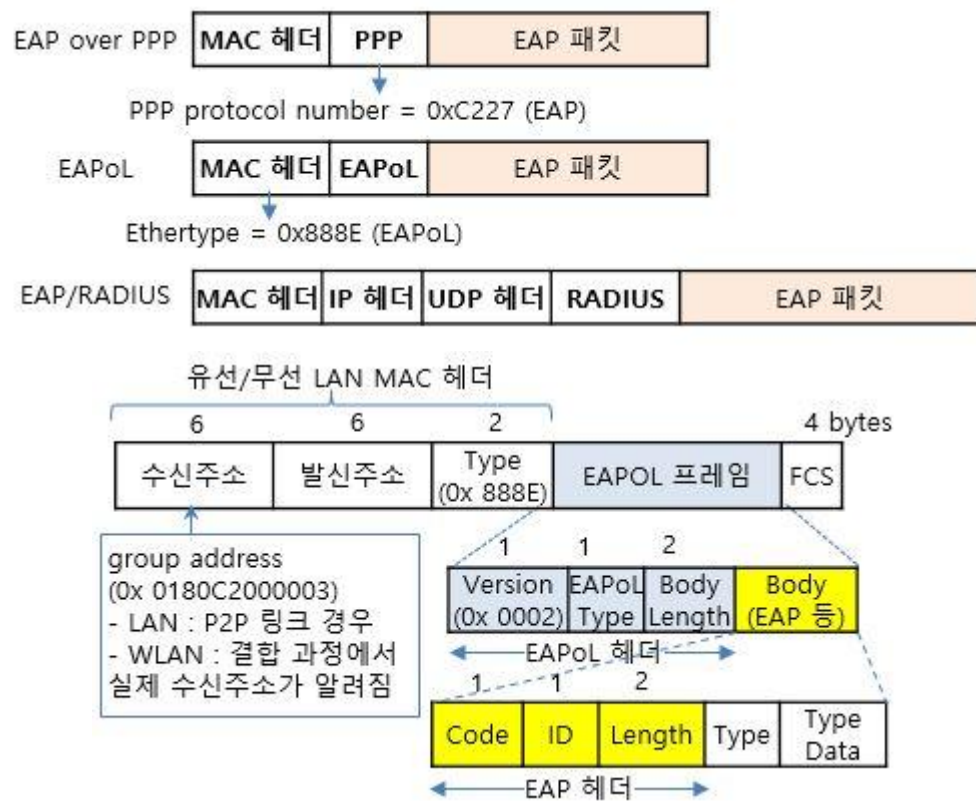
Encryption Method: WEP

- WEP: Wired Equivalent Privacy, Developed in 1999

- 4-step challenge and response
  - Client sends authentication request to AP
  - AP sends clear-text challenge to client
  - Client encrypts the text with WEP key and send it to AP
  - AP decrypts the response

- Weak security: Stream-Cipher with static key
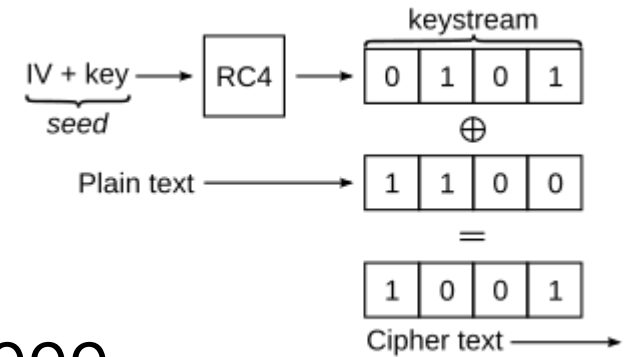
Encryption Method : WPA

- WPA: Wi-Fi Protected Access, also based on RC4

- WPA implements TKIP(Temporal Key Integrity Protocol)
  - key mixing function
  - Sequence counter
  - Message Integrity Check (replaces CRC)

- Weak security: Stream Cipher, MIC
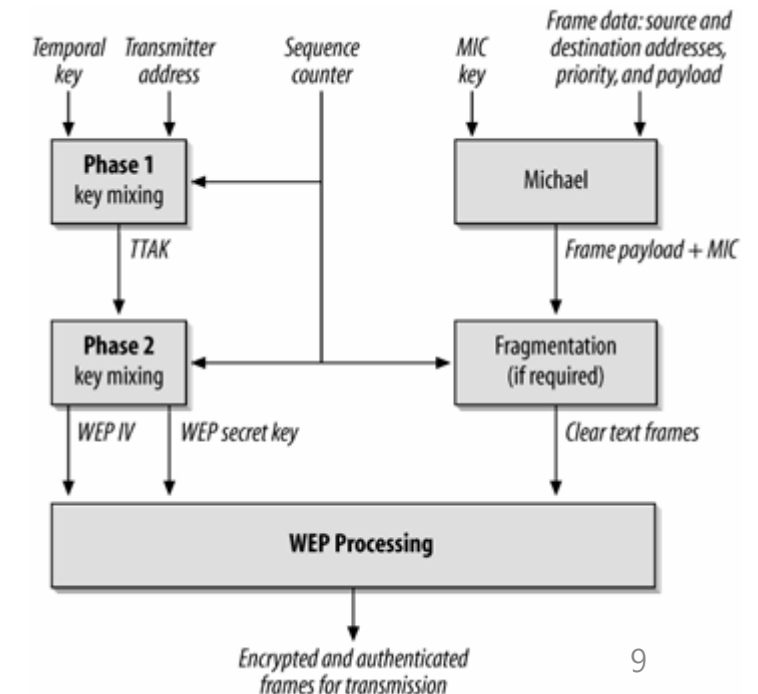
PSK (Pre-Shared Key)

- Used in WPA/WPA2

- Authentication + PTK generation

- 4-way Handshake
  - AP sends a random number (ANonce) to client
  - Client responds with its random number (SNonce)
  - AP calculates PTK and sends an encrypted message to client.
  - Client decrypts the message with PTK
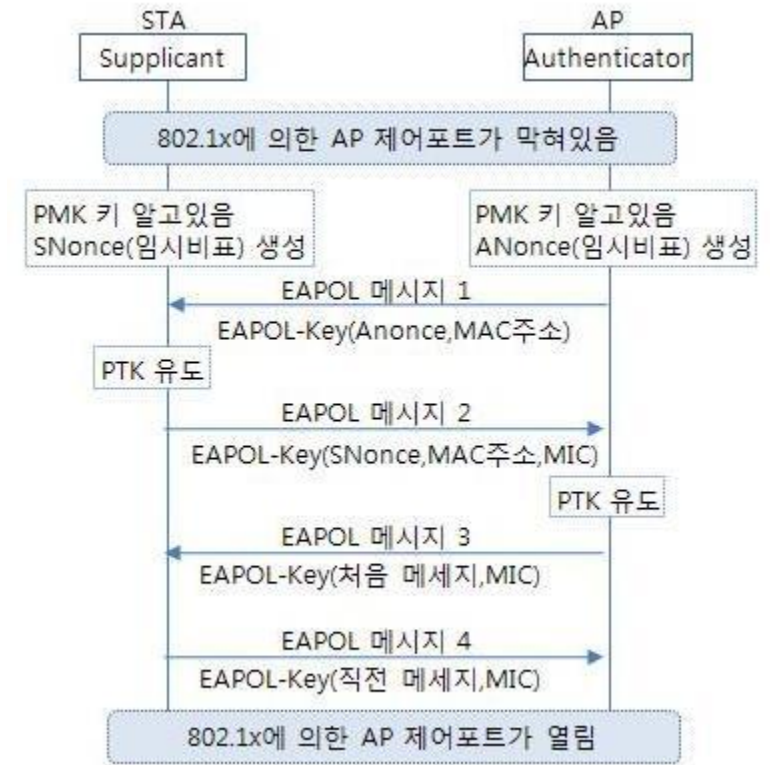
Encryption Method : WPA2

- WPA2 is enhanced version of WPA

- AES based Counter mode with CBC-MAC

- Weak security: MIC (4-way handshake)

- KRACK(Key Reinstallation Attack) (M3), PMKID offline dictionary attack(M1)

M1, M3

802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: Key (3)
    Length: 117
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 1]
    Key Information: 0x008a
        .... .010 = Key Descriptor Version: AES Cipher, HMAC-SHA1 MIC (2)
        .... 1... = Key Type: Pairwise Key
        ....00 .... = Key Index: 0
        .... .0.. .... = Install: Not set
        .... 1... .... = Key ACK: Set
        ....0 .... = Key MIC: Not set
        .... ..0. .... = Secure: Not set
        .... .0.. .... = Error: Not set
        .... 0... .... = Request: Not set
        ...0 .... = Encrypted Key Data: Not set
        ..0. .... = SMK Message: Not set
    Key Length: 16
    Replay Counter: 1
    WPA Key Nonce: 15adf473164f43a34f211ebc34495b588af5b915c0dd4478f5fbc89d2f7bd0fa
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 00000000000000000000000000000000
    WPA Key Data Length: 22
    WPA Key Data: dd14000fac04b9c9f71f0c96f62b6c11f545d2dff41b
        Tag: Vendor Specific: Ieee 802.11: RSN PMKID
            Tag Number: Vendor Specific (221)
            Tag length: 20
            OUI: 00:0f:ac (Ieee 802.11)
            Vendor Specific OUI Type: 4
            Data Type: PMKID KDE (4)
            PMKID: b9c9f71f0c96f62b6c11f545d2dff41b

802.1X Authentication
    Version: 802.1X-2004 (2)
    Type: Key (3)
    Length: 151
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 3]
    Key Information: 0x13ca
        .... .010 = Key Descriptor Version: AES Cipher, HMAC-SHA1 MIC (2)
        .... 1... = Key Type: Pairwise Key
        ....00 .... = Key Index: 0
        .... .1.. .... = Install: Set
        .... 1... .... = Key ACK: Set
        ....1 .... = Key MIC: Set
        .... ..1. .... = Secure: Set
        .... .0.. .... = Error: Not set
        .... 0... .... = Request: Not set
        ...1 .... = Encrypted Key Data: Set
        ..0. .... = SMK Message: Not set
    Key Length: 16
    Replay Counter: 2
    WPA Key Nonce: 15adf473164f43a34f211ebc34495b588af5b915c0dd4478f5fbc89d2f7bd0fa
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: e481fe9d4a2e0a53dd1119fb36104330
    WPA Key Data Length: 56
    WPA Key Data: b43c7737faedbf17306b5ea1d5059fd5379d0145fa6ddac1e08d460de93cd72c103a7f

Encryption Method : WPA3

- 192-bit encryption in WPA3-Enterprise mode

- SAE(Simultaneous Authentication of Equals) instead of PSK (Pre-Shared Key) exchange

- Safe and personalized encryption

- Evil Twin, Fragattack (WEP~WPA3)

SAE (Simultaneous Authentication of Equals)

• Password-authenticated key exchange (PAKE)

• Dragonfly handshake

• Forward secrecy guaranteed

• Dragonblood attack(Downgrade attack, Timing/Cache-based side-channel attack, DoS attack)