

# Wifi-Protocol-2

20210638 최무송

# Plan

- Week 1: Wifi Protocol + 취약점 알아보기
- **Week 2:** 복습 + Wireshark
- Week 3: 실제 환경에서의 테스트

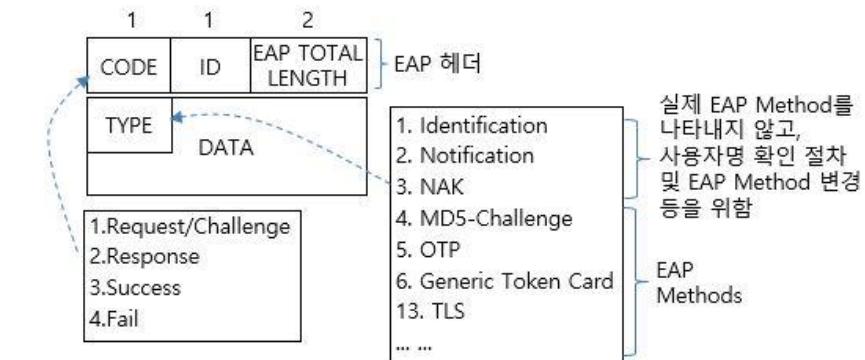
# Review

- EAP/EAPOL
- PSK, PMK, PTK?
- 4-way handhsake
- Dragonblood attack (Timing + DoS)

# EAP / EAPOL

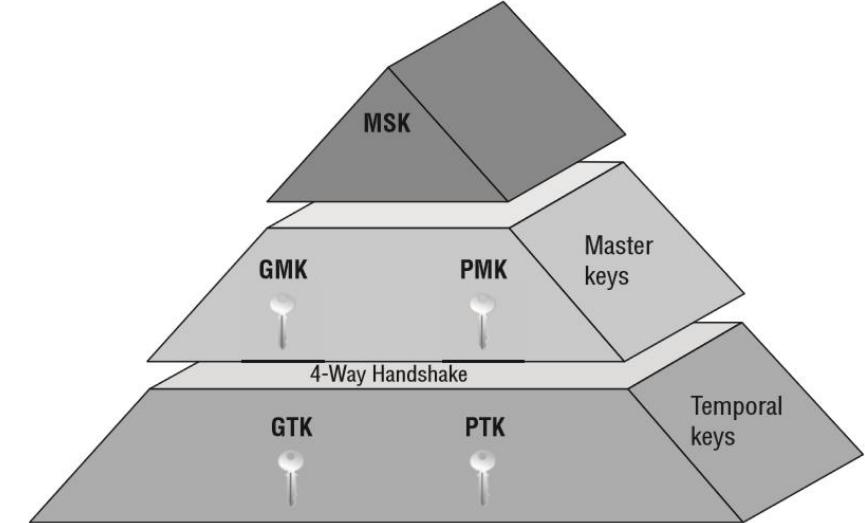


- 802.1x: 포트 기반 접근 제어
  - Supplicant, Authenticator, Authentication Server 간의 프레임워크
  - 인증 이후에 제어된 포트를 이용하도록 하는 형태
  - 무선 랜 환경에서 인증에 사용 되는 것이 EAP이다
- EAP: 인증 프로토콜을 위한 프레임워크
  - EAPOL: EAP Encapsulation over LAN
  - RADIUS 패킷: Authenticator - 인증 서버



# 4-way handshake: key level

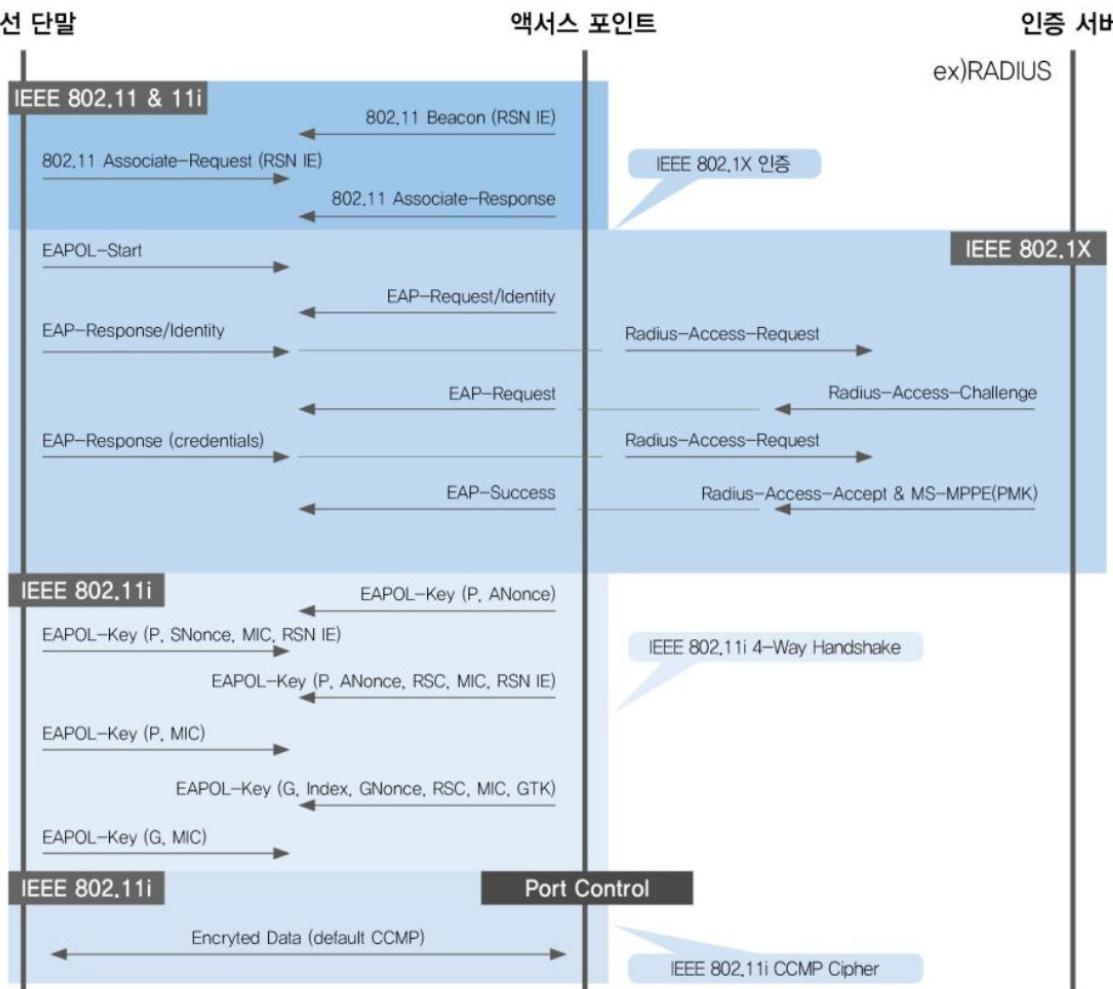
- MSK/MK (Master Session Key)
  - 802.1X/EAP 혹은 PSK authentication로 생성
- PMK (Pairwise Master Key)/GMK (Group Master Key)
  - MSK 이용
- PTK (Pairwise Transient Key)/GTK (Group Temporal Key)
  - AP와 STA 간 통신(unicast/multicast or broadcast)에서 암호화에 사용되는 동적 암호 키



# 4-way handshake: overall

- Authentication, Association → 4-way handshake → Encrypted data flow with PTK/GTK
  - 802.11 인증 및 연결: beacon frame, management frame
  - 802.1X 인증: EAP 이용 (data frame)
- PMK 유도 방식
  - WPA-개인: PSK(사전 공유키) 모드 (PSK=MSK로 사용됨)
  - WPA-엔터프라이즈: 802.1x 인증 모드 (Radius 서버가 생성한 MSK의 일부)
- PTK = PRF (PMK + Anonce + SNonce + Mac (AA)+ Mac (SA))
  - Anonce/Snonce: Authenticator/Supplicant의 난수
- MIC: Message Integrity Check

## 무선 단말



## Supplicant



Master keys: PMK and GMK  
Temporal keys: PTK and GTK



- a) PMK is known  
b) Generate SNonce

Derive PTK



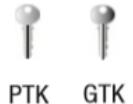
Message 1: EAPOL-Key (ANonce, Unicast)

Message 2: EAPOL-Key (SNonce, Unicast, MIC)

Encrypted GTK  
Message 3: EAPOL-Key (Install PTK, Unicast, MIC, Encrypted GTK)

Message 4: EAPOL-Key (Unicast, MIC)

Install PTK and GTK



IEEE 802.1X controlled port unblocked

## Authenticator



PMK      GMK

- a) PMK is known  
b) Generate ANonce



Derive PTK  
If needed generate GTK



PTK

GTK



Install PTK



PTK

7

```
for (counter = 1; counter < 40; counter++)  
    x = hash(pw, addr1, addr2, counter)  
    if x >= p: continue  
    if square_root_exists(x) and not P:  
        return (x,  $\sqrt{x^3 + ax + b}$ )
```

# Dragonblood Attack

- Dragonfly handshake
  - convert password into group element (point on elliptic curve)
  - Iteration is affected by pw and mac address
- Timing (side-channel) attack
  - By spoofing mac addresses, we can filter out password with iteration (average time)
  - Offline dictionary attack possible
- DoS attack
  - Hash-to-curve algorithm iterates 40 times to prevent side-channel attack

# Wireshark

- Wireshark 공식 홈페이지의 샘플을 이용
  - wpa2linkuppassphraseiswireshark.pcap
- 앞서 설명한 과정 직접 살펴보기
  - Connection to Wifi (Beacon frame, probe, authentication, association)
  - 4-way handshake (EAPoL)
  - CCMP Cipher (WPA-2)
    - DHCP
  - Disassociation

# Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Cisco_70:18:d0	Broadcast	802.11	298	Beacon frame, SN=3039, FN=0, Flags=....., BI=102, SSID="ikeriri-5g"
2	37.245000	Sony_50:73:db	Broadcast	802.11	130	Probe Request, SN=379, FN=0, Flags=....., SSID=Wildcard (Broadcast)
3	37.247000	Cisco_70:18:d0	Sony_50:73:db	802.11	292	Probe Response, SN=1748, FN=0, Flags=....R..., BI=102, SSID="ikeriri-5g"
4	50.744000	Sony_50:73:db	Cisco_70:18:d0	802.11	54	Authentication, SN=482, FN=0, Flags=.....
5	50.744000	Cisco_70:18:d0	Sony_50:73:db	802.11	54	Authentication, SN=3802, FN=0, Flags=.....
6	50.744000	Sony_50:73:db	Cisco_70:18:d0	802.11	243	Association Request, SN=483, FN=0, Flags=....., SSID="ikeriri-5g"
7	50.746000	Cisco_70:18:d0	Sony_50:73:db	802.11	173	Association Response, SN=3803, FN=0, Flags=.....
8	50.746000	Cisco_70:18:d0	Sony_50:73:db	EAPOL	179	Key (Message 1 of 4)
9	50.789000	Sony_50:73:db	Cisco_70:18:d0	EAPOL	179	Key (Message 2 of 4)
10	50.798000	Cisco_70:18:d0	Sony_50:73:db	EAPOL	213	Key (Message 3 of 4)
11	50.798000	Sony_50:73:db	Cisco_70:18:d0	EAPOL	157	Key (Message 4 of 4)
12	50.799000	Cisco_9c:6a:e4	Sony_50:73:db	802.11	132	QoS Data, SN=0, FN=0, Flags=.p....F.
13	50.990000	Sony_50:73:db	Broadcast	802.11	408	QoS Data, SN=0, FN=0, Flags=.p....T
14	50.990000	Modacom_94:ea:bc	Sony_50:73:db	802.11	662	QoS Data, SN=1, FN=0, Flags=.p....F.
15	51.126000	Sony_50:73:db	Broadcast	802.11	102	QoS Data, SN=1, FN=0, Flags=.p....T
16	92.162000	Sony_50:73:db	Cisco_70:18:d0	802.11	50	Disassociate, SN=966, FN=0, Flags=.....

# Wireshark(Beacon frame)

```
▶ Frame 1: Packet, 298 bytes on wire (2384 bits), 298 bytes captured (2384 bits)
▶ Radiotap Header v0, Length 24
▶ 802.11 radio information
└ 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
        .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ..0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = +HTC/Order flag: Not strictly ordered
        .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 wireless management
        ▶ Fixed parameters (12 bytes)
        ▶ Tagged parameters (238 bytes)
            ▶ Tag: SSID parameter set: "ikeriri-5g"
            ▶ Tag: Supported Rates 6(B), 9(B), 12(B), 18(B), 24(B), 36(B), 48(B), 54(B), [Mbit/sec]
            ▶ Tag: Traffic Indication Map (TIM): DTIM 0 of 2 bitmap
            ▶ Tag: HT Capabilities
            ▶ Tag: RSN Information
                Tag Number: RSN Information (48)
                Tag length: 20
                RSN Version: 1
            ▶ Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
                Pairwise Cipher Suite Count: 1
            ▶ Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
                Auth Key Management (AKM) Suite Count: 1
            ▶ Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK
            ▶ RSN Capabilities: 0x003c
```

# Wireshark(Probe Request)

```
▶ Frame 2: Packet, 130 bytes on wire (1040 bits), 130 bytes captured (1040 bits)
▶ Radiotap Header v0, Length 24
▶ 802.11 radio information
└ IEEE 802.11 Probe Request, Flags: .....
    Type/Subtype: Probe Request (0x0004)
    ▶ Frame Control Field: 0x4000
        .... ..00 = Version: 0
        .... 00.. = Type: Management frame (0)
        0100 .... = Subtype: 4
        ▶ 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: Sony_50:73:db (40:40:a7:50:73:db)
    ▶ Source address: Sony_50:73:db (40:40:a7:50:73:db)
    ▶ BSS Id: Broadcast (ff:ff:ff:ff:ff:ff)
        .... .... .... 0000 = Fragment number: 0
        0001 0111 1011 .... = Sequence number: 379
        [WLAN Flags: ....]
    ▶ IEEE 802.11 Wireless Management
        ▶ Tagged parameters (82 bytes)
            ▶ Tag: SSID parameter set: Wildcard SSID
                Tag Number: SSID parameter set (0)
                Tag length: 0
                SSID: <MISSING>
```

# Wireshark(Probe Response)

```
▶ Frame 3: Packet, 292 bytes on wire (2336 bits), 292 bytes captured (2336 bits)
▶ Radiotap Header v0, Length 24
▶ 802.11 radio information
└ IEEE 802.11 Probe Response, Flags: ....R...
    Type/Subtype: Probe Response (0x0005)
    ▶ Frame Control Field: 0x5008
        .... ..00 = Version: 0
        .... 00.. = Type: Management frame (0)
        0101 .... = Subtype: 5
    ▶ Flags: 0x08
        .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
        .... .0.. = More Fragments: This is the last fragment
        ▶ .... 1... = Retry: Frame is being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0.. .... = Protected flag: Data is not protected
            0... .... = +HTC/Order flag: Not strictly ordered
            .000 0000 0011 1100 = Duration: 60 microseconds
    ▶ Receiver address: Sony_50:73:db (40:40:a7:50:73:db)
    ▶ Destination address: Sony_50:73:db (40:40:a7:50:73:db)
    ▶ 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
        0110 1101 0100 .... = Sequence number: 1748
    [WLAN Flags: ....R...]
```

# Wireshark(Authentication)

```
▶ Frame 4: Packet, 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
▶ Radiotap Header v0, Length 24
▶ 802.11 radio information
└ IEEE 802.11 Authentication, Flags: .....
    Type/Subtype: Authentication (0x000b)
    ▶ Frame Control Field: 0xb000
        .... ..00 = Version: 0
        .... 00.. = Type: Management frame (0)
        1011 .... = Subtype: 11
    ▶ Flags: 0x00
        .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = +HTC/Order flag: Not strictly ordered
        .000 0000 0011 1100 = Duration: 60 microseconds
    ▶ Receiver address: Cisco_70:18:d0 (50:0f:80:70:18:d0)
    ▶ Destination address: Cisco_70:18:d0 (50:0f:80:70:18:d0)
    ▶ Transmitter address: Sony_50:73:db (40:40:a7:50:73:db)
    ▶ Source address: Sony_50:73:db (40:40:a7:50:73:db)
    ▶ BSS Id: Cisco_70:18:d0 (50:0f:80:70:18:d0)
        .... .... .... 0000 = Fragment number: 0
        0001 1110 0010 .... = Sequence number: 482
    [WLAN Flags: ....]
```

# Wireshark(Authentication)

```
▶ Frame 5: Packet, 54 bytes on wire (432 bits), 54 bytes captured (432 bits)
▶ Radiotap Header v0, Length 24
▶ 802.11 radio information
▼ IEEE 802.11 Authentication, Flags: .....
    Type/Subtype: Authentication (0x000b)
    ▶ Frame Control Field: 0xb000
        .... ..00 = Version: 0
        .... 00.. = Type: Management frame (0)
        1011 .... = Subtype: 11
    ▶ Flags: 0x00
        .000 0000 0011 1100 = Duration: 60 microseconds
    ▶ Receiver address: Sony_50:73:db (40:40:a7:50:73:db)
    ▶ Destination address: Sony_50:73:db (40:40:a7:50:73:db)
    ▶ 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
        1110 1101 1010 .... = Sequence number: 3802
        [WLAN Flags: ....]
    ▶ IEEE 802.11 Wireless Management
        ▶ Fixed parameters (6 bytes)
            Authentication Algorithm: Open System (0)
            Authentication SEQ: 0x0002
            Status code: Successful (0x0000)
```

# Wireshark(Association Request)

```
▶ Frame 6: Packet, 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits)
▶ Radiotap Header v0, Length 24
▶ 802.11 radio information
└ IEEE 802.11 Association Request, Flags: .....
    Type/Subtype: Association Request (0x0000)
    ▶ Frame Control Field: 0x0000
        .... ..00 = Version: 0
        .... 00.. = Type: Management frame (0)
        0000 .... = Subtype: 0
    ▶ Flags: 0x00
        .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = +HTC/Order flag: Not strictly ordered
        .000 0000 0011 1100 = Duration: 60 microseconds
    ▶ Receiver address: Cisco_70:18:d0 (50:0f:80:70:18:d0)
    ▶ Destination address: Cisco_70:18:d0 (50:0f:80:70:18:d0)
    ▶ Transmitter address: Sony_50:73:db (40:40:a7:50:73:db)
    ▶ Source address: Sony_50:73:db (40:40:a7:50:73:db)
    ▶ BSS Id: Cisco_70:18:d0 (50:0f:80:70:18:d0)
        .... .... 0000 = Fragment number: 0
        0001 1110 0011 .... = Sequence number: 483
    [WLAN Flags: ....]
IEEE 802.11 Management
```

# Wireshark(Association Request)

```
▼ IEEE 802.11 Wireless Management
  ▶ Fixed parameters (4 bytes)
  ▶ Tagged parameters (191 bytes)
    ▶ Tag: SSID parameter set: "ikeriri-5g"
    ▶ Tag: Supported Rates 6(B), 9(B), 12(B), 18(B), 24(B), 36(B), 48(B), 54(B), [Mbit/sec]
    ▶ Tag: Power Capability Min: 13, Max: 23
    ▶ Tag: Supported Channels
    ▶ Tag: RSN Information
      ▶ Tag Number: RSN Information (48)
        ▶ Tag length: 20
        ▶ RSN Version: 1
        ▶ Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
          ▶ Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
          ▶ Group Cipher Suite type: AES (CCM) (4)
          ▶ Pairwise Cipher Suite Count: 1
        ▶ Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
          ▶ Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
            ▶ Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
            ▶ Pairwise Cipher Suite type: AES (CCM) (4)
          ▶ Auth Key Management (AKM) Suite Count: 1
        ▶ Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK
          ▶ Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) PSK
            ▶ Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
            ▶ Auth Key Management (AKM) type: PSK (2)
      ▶ RSN Capabilities: 0x003c
```

# Wireshark(Association Response)

```
▶ Frame 7: Packet, 173 bytes on wire (1384 bits), 173 bytes captured (1384 bits)
▶ Radiotap Header v0, Length 24
▶ 802.11 radio information
▼ IEEE 802.11 Association Response, Flags: .....
    Type/Subtype: Association Response (0x0001)
    ▶ Frame Control Field: 0x1000
        .... .00 = Version: 0
        .... 00.. = Type: Management frame (0)
        0001 .... = Subtype: 1
        ▶ Flags: 0x00
            .000 0000 0011 1100 = Duration: 60 microseconds
        ▶ Receiver address: Sony_50:73:db (40:40:a7:50:73:db)
        ▶ Destination address: Sony_50:73:db (40:40:a7:50:73:db)
        ▶ 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
            1110 1101 1011 .... = Sequence number: 3803
            [WLAN Flags: ....]
    ▼ IEEE 802.11 Wireless Management
        ▶ Fixed parameters (6 bytes)
            ▶ Capabilities Information: 0x8531
                Status code: Successful (0x0000)
                ...00 0000 0000 0110 = Association ID: 0x0006
        ▶ Tagged parameters (119 bytes)
```

# Wireshark(4-way handshake, M1)

```
▶ Frame 8: Packet, 179 bytes on wire (1432 bits), 179 bytes captured (1432 bits)
▶ Radiotap Header v0, Length 24
▶ 802.11 radio information
▶ IEEE 802.11 QoS Data, Flags: .....F.
    Type/Subtype: QoS Data (0x0028)
    ▶ Frame Control Field: 0x8802
        .... .00 = Version: 0
        .... 10.. = Type: Data frame (2)
        1000 .... = Subtype: 8
        ▶ Flags: 0x02
            .... ..10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x2)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0... .... = Protected flag: Data is not protected
            0.... .... = +HTC/Order flag: Not strictly ordered
            .000 0000 0011 1100 = Duration: 60 microseconds
    ▶ Receiver address: Sony_50:73:db (40:40:a7:50:73:db)
    ▶ Transmitter address: Cisco_70:18:d0 (50:0f:80:70:18:d0)
    ▶ Destination address: Sony_50:73:db (40:40:a7:50:73:db)
    ▶ Source address: Cisco_70:18:d0 (50:0f:80:70:18:d0)
    ▶ BSS Id: Cisco_70:18:d0 (50:0f:80:70:18:d0)
    ▶ STA address: Sony_50:73:db (40:40:a7:50:73:db)
        .... .... 0000 = Fragment number: 0
        0000 0000 0000 .... = Sequence number: 0
        [WLAN Flags: .....F.]
    ▶ Qos Control: 0x0007
    ▶ Logical-Link Control
    ▶ 802.1X Authentication
```

```
▼ 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: 15adf473164f43a34f211ebc34495b588af5b915c0dd4478f5fbcb89d2f7bd0fa
  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
```

# Wireshark(4-way handshake, M2)

```
▶ Frame 9: Packet, 179 bytes on wire (1432 bits), 179 bytes captured (1432 bits)
▶ Radiotap Header v0, Length 24
▶ 802.11 radio information
└ IEEE 802.11 QoS Data, Flags: ....T
    Type/Subtype: QoS Data (0x0028)
    ▶ Frame Control Field: 0x8801
        .... .00 = Version: 0
        .... 10.. = Type: Data frame (2)
        1000 .... = Subtype: 8
    ▶ Flags: 0x01
        .... .01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
        .... .0.. = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = Protected flag: Data is not protected
        0... .... = +HTC/Order flag: Not strictly ordered
        .000 0000 0011 1100 = Duration: 60 microseconds
    ▶ Receiver address: Cisco_70:18:d0 (50:0f:80:70:18:d0)
    ▶ Transmitter address: Sony_50:73:db (40:40:a7:50:73:db)
    ▶ Destination address: Cisco_70:18:d0 (50:0f:80:70:18:d0)
    ▶ Source address: Sony_50:73:db (40:40:a7:50:73:db)
    ▶ BSS Id: Cisco_70:18:d0 (50:0f:80:70:18:d0)
    ▶ STA address: Sony_50:73:db (40:40:a7:50:73:db)
        .... .... 0000 = Fragment number: 0
        0000 0000 .... = Sequence number: 0
        [WLAN Flags: ....T]
    ▶ Qos Control: 0x0006
    ▶ Logical-Link Control
    ▶ 802.1X Authentication
```

```
└ 802.1X Authentication
    Version: 802.1X-2001 (1)
    Type: Key (3)
    Length: 117
    Key Descriptor Type: EAPOL RSN Key (2)
    [Message number: 2]
    ▶ Key Information: 0x010a
        .... .... .... .010 = Key Descriptor Version: AES Cipher, HMAC-SHA1 MIC (2)
        .... .... .... 1... = Key Type: Pairwise Key
        .... .... .... .00 .. = Key Index: 0
        .... .... .... 0... = Install: Not set
        .... .... .... 0.... = Key ACK: Not set
        .... .... .... 1.... = Key MIC: 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: 0
    Replay Counter: 1
    WPA KeyNonce: 1b9717293f9d9d6979d94b36dbc9d83418bbce09f72edc1e1ae4fd79821ffda4
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: 2f8e7921e572af75a7c898e625ffb43
    WPA Key Data Length: 22
    ▶ WPA Key Data: 30140100000fac040100000fac040100000fac023c00
        ▶ Tag: RSN Information
```

# Wireshark(4-way handshake, M3)

```
▶ Frame 10: Packet, 213 bytes on wire (1704 bits), 213 bytes captured (1704 bits)
▶ Radiotap Header v0, Length 24
▶ 802.11 radio information
▼ IEEE 802.11 QoS Data, Flags: .....F.
  Type/Subtype: QoS Data (0x0028)
  ▶ Frame Control Field: 0x8802
    .... ..00 = Version: 0
    .... 10.. = Type: Data frame (2)
    1000 .... = Subtype: 8
  ▶ Flags: 0x02
    .... .10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x2)
    .... .0.. = More Fragments: This is the last fragment
    .... 0... = Retry: Frame is not being retransmitted
    ...0 .... = PWR MGT: STA will stay up
    ..0. .... = More Data: No data buffered
    .0... .... = Protected flag: Data is not protected
    0.... .... = +HTC/Order flag: Not strictly ordered
    .000 0000 0011 1100 = Duration: 60 microseconds
  ▶ Receiver address: Sony_50:73:db (40:40:a7:50:73:db)
  ▶ Transmitter address: Cisco_70:18:d0 (50:0f:80:70:18:d0)
  ▶ Destination address: Sony_50:73:db (40:40:a7:50:73:db)
  ▶ Source address: Cisco_70:18:d0 (50:0f:80:70:18:d0)
  ▶ BSS Id: Cisco_70:18:d0 (50:0f:80:70:18:d0)
  ▶ STA address: Sony_50:73:db (40:40:a7:50:73:db)
    .... .... ..000 = Fragment number: 0
    0000 0000 0001 .... = Sequence number: 1
    [WLAN Flags: .....F.]
  ▶ Qos Control: 0x0007
  ▶ Logical-Link Control
  ▶ 802.1X Authentication

  ▶ 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 KeyNonce: 15adf473164f43a34f211ebc34495b588af5b915c0dd4478f5fbc89d2f7bd0fa
    Key IV: 00000000000000000000000000000000
    WPA Key RSC: 0000000000000000
    WPA Key ID: 0000000000000000
    WPA Key MIC: e481fe9d4a2e0a53dd1119fb36104330
    WPA Key Data Length: 56
    WPA Key Data: b43c7737faedb17306b5ea1d5059fd5379d0145fa6ddac1e08d460de93cd72c103a7fb2c21445d2b740139c80ac569ae1e865a198c79a21
```

# Wireshark(4-way handshake, M3)

```
▼ WPA Key Data: b43c7737faedb17306b5ea1d5059fd5379d0145fa6ddac1e08d460de93cd72c103a7fb2c21445d2b740139c80ac569ae1e865a198c79a21
  ▼ Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag length: 20
    RSN Version: 1
  ▼ Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
    Group Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
    Group Cipher Suite type: AES (CCM) (4)
    Pairwise Cipher Suite Count: 1
  ▼ Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
    ▼ Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
      Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
      Pairwise Cipher Suite type: AES (CCM) (4)
      Auth Key Management (AKM) Suite Count: 1
    ▼ Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK
      ▼ Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) PSK
        Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
        Auth Key Management (AKM) type: PSK (2)
    ▶ RSN Capabilities: 0x003c
  ▼ Tag: Vendor Specific: Ieee 802.11: RSN GTK
    Tag Number: Vendor Specific (221)
    Tag length: 22
    OUI: 00:0f:ac (Ieee 802.11)
    Vendor Specific OUI Type: 1
    Data Type: GTK KDE (1)
    .... .01 = Key ID: 0x1
    .... .0.. = Tx: Temporal key used only for reception
    0000 0... = Reserved: 0x00
    Reserved: 0x00
    GTK: eab4e5b93588db11d1ecfda6eac5606b
  WPA Key Data Padding: dd00
  [KCK: d9eb99b06ea78764cf358998050f017f]
  [KEK: 22ffffbcadfb9d96816884599c16d65dd]
```

# Wireshark(4-way handshake, M4)

```
> Frame 11: Packet, 157 bytes on wire (1256 bits), 157 bytes captured (1256 bits)
> Radiotap Header v0, Length 24
> 802.11 radio information
-> IEEE 802.11 QoS Data, Flags: ....T
    Type/Subtype: QoS Data (0x0028)
-> Frame Control Field: 0x8801
    .... ..00 = Version: 0
    .... 10.. = Type: Data frame (2)
    1000 .... = Subtype: 8
-> Flags: 0x01
    .... ..01 = DS status: Frame from STA to DS via an AP (To DS: 1 From DS: 0) (0x1)
    .... .0.. = More Fragments: This is the last fragment
    .... 0... = Retry: Frame is not being retransmitted
    ...0 .... = PWR MGT: STA will stay up
    ..0. .... = More Data: No data buffered
    .0.. .... = Protected flag: Data is not protected
    0.... .... = +HTC/Order flag: Not strictly ordered
    .000 0000 0011 1100 = Duration: 60 microseconds
-> Receiver address: Cisco_70:18:d0 (50:0f:80:70:18:d0)
-> Transmitter address: Sony_50:73:db (40:40:a7:50:73:db)
-> Destination address: Cisco_70:18:d0 (50:0f:80:70:18:d0)
-> Source address: Sony_50:73:db (40:40:a7:50:73:db)
-> BSS Id: Cisco_70:18:d0 (50:0f:80:70:18:d0)
-> STA address: Sony_50:73:db (40:40:a7:50:73:db)
    .... .... .... 0000 = Fragment number: 0
    0000 0000 0001 .... = Sequence number: 1
    [WLAN Flags: ....T]
-> Qos Control: 0x0006
-> Logical-Link Control
-> 802.1X Authentication
```

# Encrypted data

```
▶ Frame 12: Packet, 132 bytes on wire (1056 bits), 132 bytes captured (1056 bits)
▶ Radiotap Header v0, Length 36
▶ 802.11 radio information
└ IEEE 802.11 QoS Data, Flags: .p....F.
    Type/Subtype: QoS Data (0x0028)
    ▶ Frame Control Field: 0x8842
        .... ..00 = Version: 0
        .... 10.. = Type: Data frame (2)
        1000 .... = Subtype: 8
    ▶ Flags: 0x42
        .... ..10 = DS status: Frame from DS to a STA via AP(To DS: 0 From DS: 1) (0x2)
        .... .0... = More Fragments: This is the last fragment
        .... 0... = Retry: Frame is not being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .1.. .... = Protected flag: Data is protected
        0.... .... = +HTC/Order flag: Not strictly ordered
        .000 0000 0010 1000 = Duration: 40 microseconds
    ▶ Receiver address: Sony_50:73:db (40:40:a7:50:73:db)
    ▶ Transmitter address: Cisco_70:18:d0 (50:0f:80:70:18:d0)
    ▶ Destination address: Sony_50:73:db (40:40:a7:50:73:db)
    ▶ Source address: Cisco_9c:6a:e4 (18:80:90:9c:6a:e4)
    ▶ BSS Id: Cisco_70:18:d0 (50:0f:80:70:18:d0)
    ▶ STA address: Sony_50:73:db (40:40:a7:50:73:db)
        .... .... .... 0000 = Fragment number: 0
        0000 0000 0000 .... = Sequence number: 0
        [WLAN Flags: .p....F.]
    ▶ Qos Control: 0x0000
    ▶ CCMP parameters
    ▶ Data (62 bytes)
        Data: 425140326b1d4fd39c6d3a9247d3c82ec709c89a58457d06fb7062e892a08daaceb3023a3e71dd811fe08a3d82d6e03045942cdc55a218bc3e0680faf030
        [Length: 62]
```

# Decrypted data with wpa-pwd

No.	Time	Source	Destination	Protocol	Length Info
1	0.000000	Cisco_70:18:d0	Broadcast	802.11	298 Beacon frame, SN=3039, FN=0, Flags=....., BI=102, SSID="ikeriri-5g"
2	37.245000	Sony_50:73:db	Broadcast	802.11	130 Probe Request, SN=379, FN=0, Flags=....., SSID=Wildcard (Broadcast)
3	37.247000	Cisco_70:18:d0	Sony_50:73:db	802.11	292 Probe Response, SN=1748, FN=0, Flags=....R..., BI=102, SSID="ikeriri-5g"
4	50.744000	Sony_50:73:db	Cisco_70:18:d0	802.11	54 Authentication, SN=482, FN=0, Flags=.....
5	50.744000	Cisco_70:18:d0	Sony_50:73:db	802.11	54 Authentication, SN=3802, FN=0, Flags=.....
6	50.744000	Sony_50:73:db	Cisco_70:18:d0	802.11	243 Association Request, SN=483, FN=0, Flags=....., SSID="ikeriri-5g"
7	50.746000	Cisco_70:18:d0	Sony_50:73:db	802.11	173 Association Response, SN=3803, FN=0, Flags=.....
8	50.746000	Cisco_70:18:d0	Sony_50:73:db	EAPOL	179 Key (Message 1 of 4)
9	50.789000	Sony_50:73:db	Cisco_70:18:d0	EAPOL	179 Key (Message 2 of 4)
10	50.798000	Cisco_70:18:d0	Sony_50:73:db	EAPOL	213 Key (Message 3 of 4)
11	50.798000	Sony_50:73:db	Cisco_70:18:d0	EAPOL	157 Key (Message 4 of 4)
12	50.799000	192.168.100.3	224.0.0.1	IGMPv2	132 Membership Query, general
13	50.990000	0.0.0.0	255.255.255.255	DHCP	408 DHCP Request - Transaction ID 0x5e51762c
14	50.990000	192.168.100.254	192.168.100.121	DHCP	662 DHCP ACK - Transaction ID 0x5e51762c
15	51.126000	Sony_50:73:db	Broadcast	ARP	102 ARP Announcement for 192.168.100.121
16	92.162000	Sony_50:73:db	Cisco_70:18:d0	802.11	50 Disassociate, SN=966, FN=0, Flags=.....

# Disassociate

```
► Frame 16: Packet, 50 bytes on wire (400 bits), 50 bytes captured (400 bits)
► Radiotap Header v0, Length 24
► 802.11 radio information
▼ IEEE 802.11 Disassociate, Flags: .....
    Type/Subtype: Disassociate (0x000a)
    ▼ Frame Control Field: 0xa000
        .... .00 = Version: 0
        .... 00.. = Type: Management frame (0)
        1010 .... = Subtype: 10
        ▼ Flags: 0x00
            .... ..00 = DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0 From DS: 0) (0x0)
            .... .0.. = More Fragments: This is the last fragment
            .... 0... = Retry: Frame is not being retransmitted
            ...0 .... = PWR MGT: STA will stay up
            ..0. .... = More Data: No data buffered
            .0... .... = Protected flag: Data is not protected
            0... .... = +HTC/Order flag: Not strictly ordered
            .000 0000 0011 1100 = Duration: 60 microseconds
    ► Receiver address: Cisco_70:18:d0 (50:0f:80:70:18:d0)
    ► Destination address: Cisco_70:18:d0 (50:0f:80:70:18:d0)
    ► Transmitter address: Sony_50:73:db (40:40:a7:50:73:db)
    ► Source address: Sony_50:73:db (40:40:a7:50:73:db)
    ► BSS Id: Cisco_70:18:d0 (50:0f:80:70:18:d0)
        .... .... 0000 = Fragment number: 0
        0011 1100 0110 .... = Sequence number: 966
        [WLAN Flags: ....]
    ▼ IEEE 802.11 Wireless Management
        ▼ Fixed parameters (2 bytes)
            Reason code: Unspecified reason (0x0001)
```

# 3주차 취약점 공격 실습

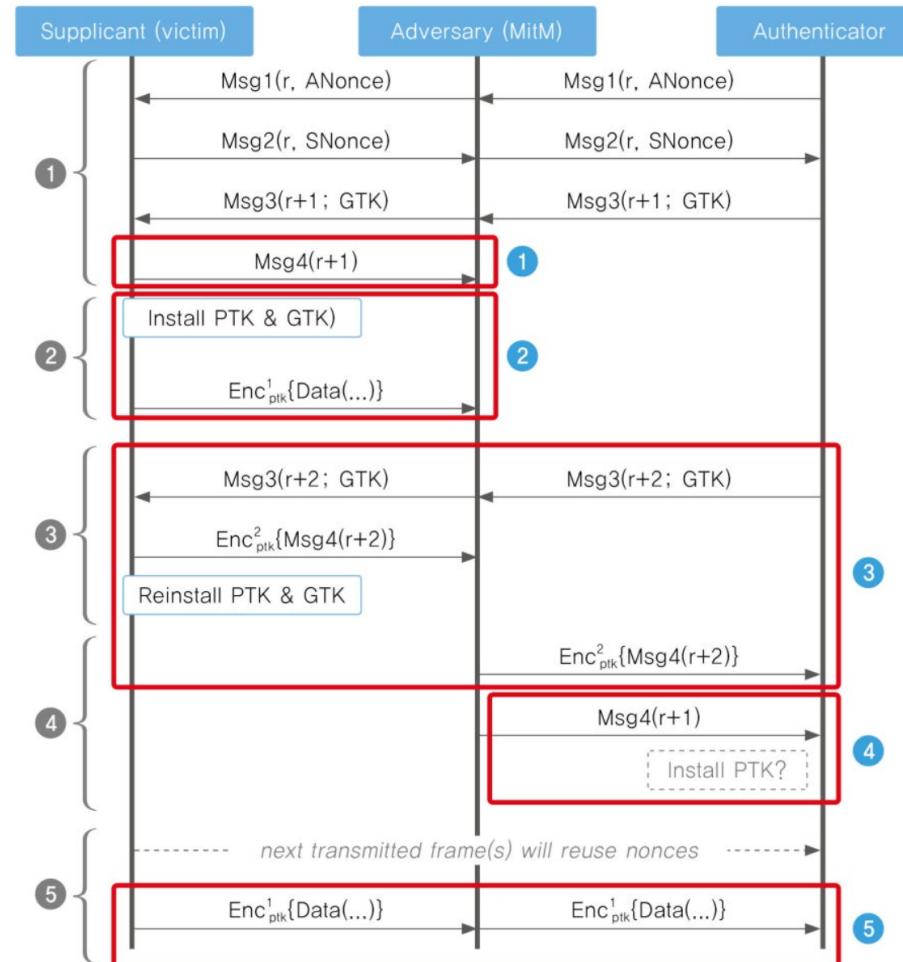
- Fragattack, Dragonblood Attack : 개념 이해 (1주차 완료)
- KRACK, PMKID offline dictionary match: 실습 (3주차 예정)
  - 무선 랜카드를 이용하여 kali linux 환경에서 직접 테스트 가능
  - 기제공된 pcap 파일 등을 활용하여 PMKID attack 해보기

# Fragattack/KRACK

[vanhoefm/fragattacks](https://github.com/vanhoefm/fragattacks)

[vanhoefm/krackattacks-scripts](https://github.com/vanhoefm/krackattacks-scripts)

kali linux 환경에서 테스트



# PMKID Offline dictionary match

- Full handshake 없이 첫 번째 메시지만으로도 알아낼 수 있음
- Hcxdump tool을 이용하여 패킷을 캡쳐
- Hashcat을 이용하여 Pre shared key 추출

[New attack on WPA/WPA2 using PMKID](#)