Network Administration/System Administration Homework #10

B10202012 劉仲楷

1 Wireless

1.1 Miscs

ref: Wiki: Service set、WiFi 網路的識別

1. - SSID（Service Set Identifier）是無線網路對外顯示的網路名稱，用來讓使用者分辨不同的 Wi-Fi。BSSID（Basic Service Set Identifier）則是 AP 的唯一識別碼，通常就是該 AP 的 MAC address。
   - 兩者的關係是：SSID 表示同一個無線網路的名稱，而 BSSID 則代表提供該 SSID 的其中一個 AP 實體。同一個 SSID 可以由多個 AP 廣播，因此會有多個不同的 BSSID。
2. - 同一個 AP 可以同時提供多個 SSID。許多 AP 支援 virtual AP，以一張無線網卡同時廣播多個網路名稱（例如：一個 SSID 給內部使用者電腦、一個 SSID 給內部使用者手機、一個 SSID 給訪客）。
   - 不同 AP 有可能共用同一個 SSID。如學校 WiFi、公共場所 WiFi 會讓所有 AP 使用相同的 SSID，以讓使用者換手 (handoff)。在此情況下，不同 AP 會有不同的 BSSID，但 SSID 相同，讓使用者可以在區域內移動時保持連線。

1.2 HTML's Wi-Fi Problem

1. $$\frac{P_r}{P_t} = G_t G_r \left(\frac{\lambda}{4\pi d}\right)^2 = G_t G_r \left(\frac{c}{f}\frac{1}{4\pi d}\right)^2 \Rightarrow P_r \propto 1/f$$

   所以 2.4 GHz 接收訊號強度較高

2. $$G_t = G_r = 0 \text{ dB} = 1$$
$$\frac{P_r}{P_t} = G_t G_r \left(\frac{c}{f}\frac{1}{4\pi d}\right)^2 = 1 \cdot 1 \left(\frac{3 \cdot 10^8}{5 \cdot 10^9}\frac{1}{4\pi \cdot 1}\right)^2 = 2.28 \times 10^{-5}$$
$$10 \log_{10}(2.28 \times 10^{-5}) \approx -46.4 \text{ dB}$$

3.

$$\frac{P_r}{P_t} = G_t G_r \left(\frac{\lambda}{4\pi d}\right)^2 \Rightarrow P_r \propto d^{-2}$$
$$d^2_{\text{front}} = 5^2 + 20^2 = 425$$
$$d^2_{\text{front2}} = 5^2 + 0^2 = 25$$
$$d^2_{\text{rear}} = 25^2 + 10^2 = 725$$
$$\text{SINR}_i = \frac{P}{I+N} \approx \frac{P_{r,\text{front}}}{P_{r,\text{rear}}} = \frac{1/d^2_{\text{front}}}{1/d^2_{\text{rear}}} \approx 1.7$$
$$\text{SINR}_f = \frac{P}{I+N} \approx \frac{P_{r,\text{front2}}}{P_{r,\text{rear}} + P_{r,\text{front}}} = \frac{1/d^2_{\text{front2}}}{1/d^2_{\text{rear}} + 1/d^2_{\text{front}}} \approx 10.7$$

$\text{SINR}_f > \text{SINR}_i \Rightarrow$ 有提升

1.3 Tiaosu's Hotspot

1.3.1 Gimme expensive French meal

1. Ref: MIT hostapd conf

```
# /etc/hostapd/hostapd.conf

interface=wlan0
driver=nl80211
bridge=br0

ssid=tiaosu
hw_mode=g
channel=6
country_code=TW

macaddr_acl=0
auth_algs=2
wpa=0
wep_key0=xxxxxxxxx
wep_tx_keyidx=0
```

1.3.2 WEP is dangerous!

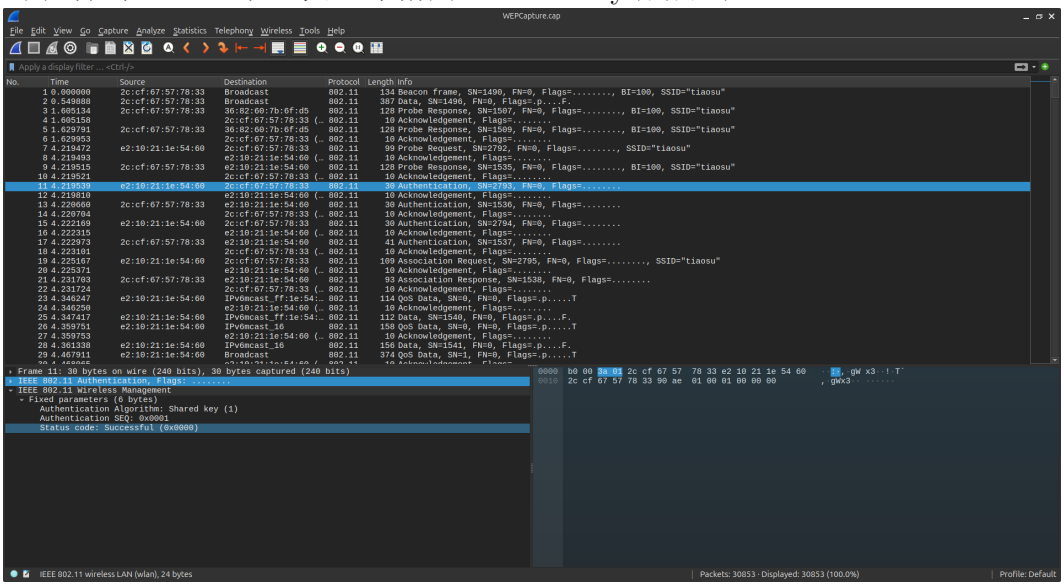
2. Ref: Open System Authentication, Shared Key Authentication, and Deauthentication

- Open System Authentication: Client 只需要送出 Authentication Request，AP 幾乎無條件接受，回應成功的 Authentication Response。
- Shared Key Authentication 是一種基於 Challenge–Response 的流程，需要雙方都具備相同的 WEP static key。流程如下：
  (a) Client 送出 Authentication Request。
  (b) AP 回傳一段明文的 Challenge。

(c) Client 使用 WEP key 加密這段 Challenge，並送回 AP。

(d) AP 使用自己的 WEP key 解密並比對原本 Challenge，若一致則驗證成功。

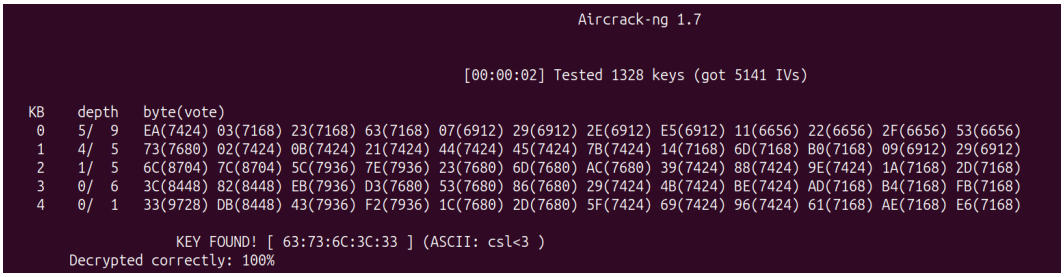
3. (a) 可以看到 Client 第一次連線藉由 Shared Key 成功的。



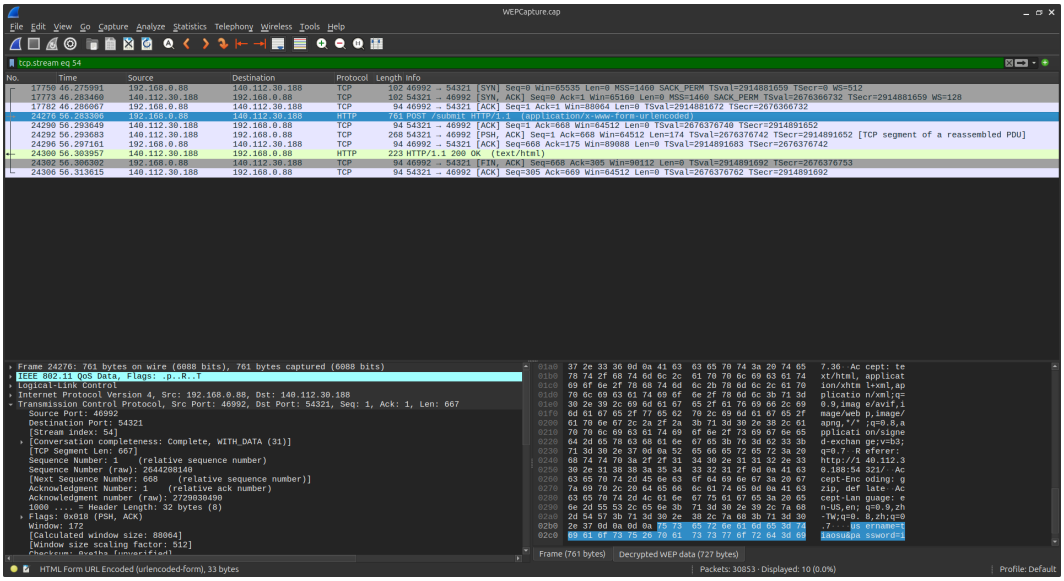
(b) 攻擊者常用 ARP 封包來產生大量 traffic，並重放 ARP request 封包以强制 AP 不停回應，被迫產生大量 WEP 加密資料與重複的 IV。這叫 ARP replay attack，利用 WEP 的 24-bit IV 太短、會重複的弱點，讓攻擊者能快速收集足夠多的封包來破解 WEP 金鑰。

(c) 用以下指令得到金鑰

```
sudo apt install aircrack-ng
aircrack-ng WEPCapture.cap
```



(d) 接在 `Edit > Preferences > Protocols > IEEE 802.11`
找到 `Enable decryption > Decryption keys > Edit` 進入後按 `+`，輸入 `WEP`、`63:73:6c:3c:33`，再按 `OK` 接下來我們就得到了明文封包，藉由 tcp stream 找到：
IP Port: 140.112.30.188:54321
username: tiaosu、password: ilovecsl
flag: `NASA_HW10{W3P_15_N07_50_54F3}`



4. WEP 被攻破後，攻擊者能解密大部分連線，包含明文 HTTP、未加密的應用資料等，但要直接破解 HTTPS（TLS）加密的帳號密碼是沒辦法的。只有在存在額外弱點（例如 HTTPS 被 downgraded 成 HTTP 時才會發生。單純 WEP 破解本身並不足以在破解 TLS。

1.3.3 I must get free hotspot

5. Ref: 4-Way Handshake

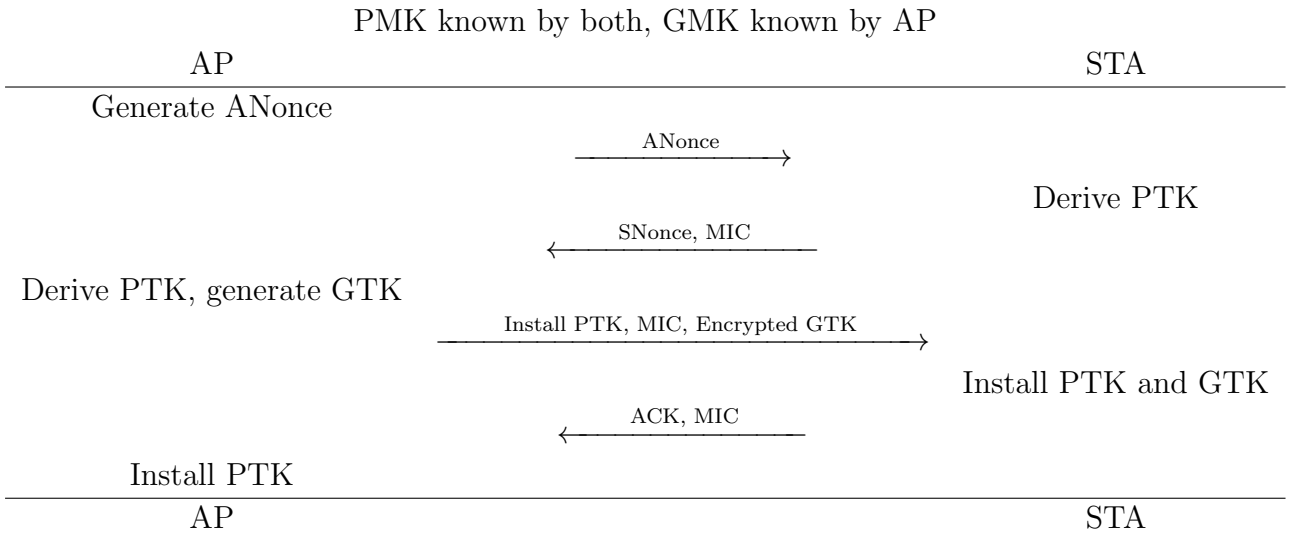


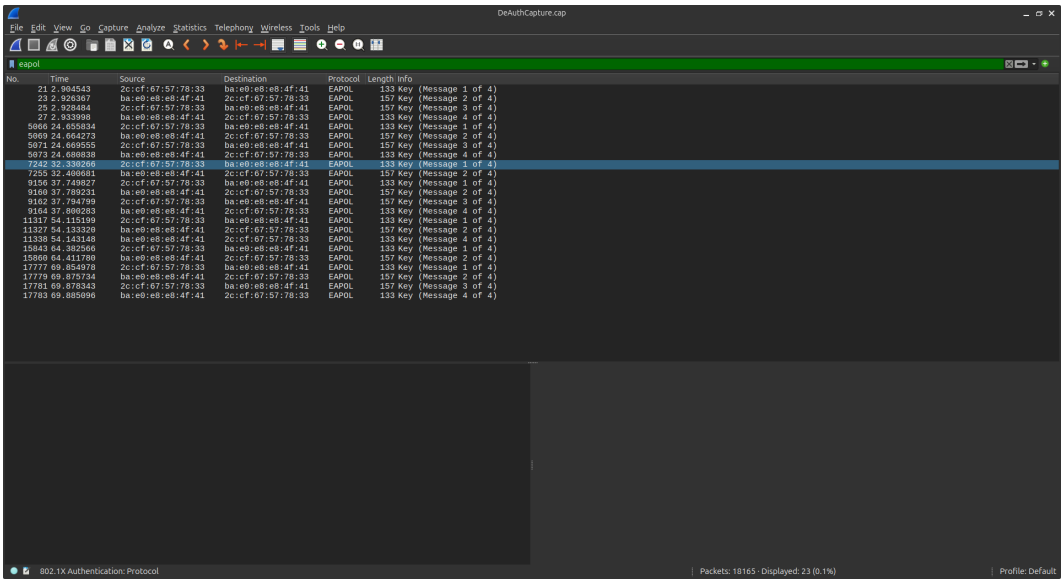
Table 1: Caption

6. Ref: Wiki: Wi-Fi deauthentication attack
Deauthentication Attack 是一種 WiFi 的 DOS attack。攻擊者利用 802.11 標準中「Deauthentication frame 不需要加密也不需要驗證」的弱點，攻擊者只要偽造一個來自 AP的 deauth frame，就能强制斷開 Client 與 AP 的連線。由於這個管理框架在 WPA/WPA2 中仍是明文傳送，因此攻擊者只需 MAC spoofing，即可讓 Client 認定自己被 AP 踢下線。當 Client 被迫重新連線時，會重新進

行 Four-Way Handshake。攻擊者監聽並擷取 ANonce、SNonce、MIC，攻擊者就能利用其做 離線字典攻擊 (offline dictionary attack)。攻擊者離線嘗試常見的 Passphrases，每次計算 PMK、PTK 及預期 MIC，若 MIC 匹配，則找到正確的 Passphrase。

7. (a) Client MAC address: `ba:e0:e8:e8:4f:41`
   AP MAC address: `2c:cf:67:57:78:33`

   (b) 21



   (c) 從上圖可以看到 5 次（其中有一次沒擷取到第 3 個封包）。

   (d) 利用以下指令找到 passphrase: `felwinter`。

   ```
   aircrack-ng DeAuthCapture.cap -w rocktiaosu.txt
   ```

```
                          Aircrack-ng 1.7

[00:15:38] 12043392/14344392 keys tested (13038.98 k/s)

Time left: 2 minutes, 56 seconds                          83.96%

                      KEY FOUND! [ felwinter ]


Master Key     : 00 9C 4C 3F 61 98 5F 1D BE 96 78 EC C3 AC 9F 5C
                 5E 8E 83 85 65 7B C9 95 3B FB 5B C2 5B 27 C0 2C

Transient Key  : DF 11 68 59 39 E2 FF 14 46 CB 85 DE 95 C0 E6 F4
                 4C FF 47 6A CE C2 2B 1F 5A C2 6E A1 11 A8 B4 E9
                 34 03 B2 C5 F0 74 9F B4 9A 0B D1 FA 0C 93 E5 00
                 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

EAPOL HMAC     : E8 EB 69 68 A2 6C 38 03 2E F1 7F 56 57 77 75 D5
```

   (e) 和前面一樣，`Edit > Preferences > Protocols > IEEE 802.11`
   找到 `Enable decryption > Decryption keys > Edit` 進入後按 `+`，輸入 `WPA-PWD`、`felwinter`，再按 `OK`

filter 打 DHCP，即可看到第一次連線分配的 IP 是 `192.168.0.81`