

NASA HW10

B11901164 陳秉緯

A. Miscs

ref: 1 (<https://community.cisco.com/t5/wireless/ssid-vs-bssid/td-p/1001487>)

- SSID 是一個無線網路的名稱或識別碼，用來標識一個無線區域網路。它是最多 32 個字元的字串，用來讓使用者能夠辨識和連接到特定的無線網路。SSID 是可以被手動更改的，且在網路設定中可以選擇是否對外廣播。
 - BSSID 是一個無線接入點 (AP) 的唯一硬體位址，通常是 AP 的 MAC 地址。它是 48 位的 MAC 地址格式，例：00:1A:2B:3C:4D:5E，自動分配且無法更改。
 - 關係：
 - SSID 是網路的名稱，BSSID 是具體設備的位址
 - 當一個無線網路具有多個 AP，例：企業環境中的漫遊網路，它們可以共享相同的 SSID，但每個 AP 都有獨立的 BSSID
- 可以：在系館內，使用相同硬體設備但提供不同的網路，給本系學生用的 csie 與外系學生或訪客用的 csie_guest。
 - 可以：在校園環境中，不同樓層或區域的 AP 具有相同 SSID，當使用者在不同區域移動時，設備會自動切換到訊號較強的 AP，達到無縫漫遊。

B. HTML's Wi-Fi Problem

ref: 1 (https://en.wikipedia.org/wiki/Friis_transmission_equation), 2 (<https://info.support.huawei.com/info-finder/encyclopedia/en/SNR.html>)

- 因相同距離 d 、相同發射功率 P_t 、相同傳輸及接收天線增益 G_t, G_r ，所以 P_r 正比於 λ^2 ，也就正比於 $(\frac{1}{f})^2$ ，故頻率愈高的 Wi-Fi，接收訊號強度愈低。所以 2.4 GHz 的 Wi-Fi 接收訊號強度較高。
- $G_t = G_r = 0 \text{ dB} \Rightarrow G_t = G_r = 1$
 - 接收端與傳輸端的距離為 1 m $\Rightarrow d = 1 \text{ m}$
 - $\frac{P_r}{P_t} = 1 \cdot 1 \cdot (\frac{3 \cdot 10^8}{4\pi \cdot 1.5 \cdot 10^9})^2 \approx 9.12 \times 10^{-7} \approx -60.4 \text{ dB}$
- 根據 Friis transmission equation，在 $G_t = G_r = 1$ 與 P_t 相同以及都是 csie-5G 的情況下，可以得知 P_r 與 d^2 成反比
 - 新 AP 設置前：
 - $d_f = \sqrt{(0 - (-5))^2 + (10 - (-10))^2} = \sqrt{425} \approx 20.62$
 - $d_r = \sqrt{(20 - (-5))^2 + (0 - (-10))^2} = \sqrt{725} \approx 26.93$
 - $SINR_{\text{前}} = \frac{S_{\text{前}}}{I_{\text{前}}} = \frac{26.93^2}{20.62^2} \approx 1.71 \approx 2.3 \text{ dB}$
 - 新 AP 設置後：
 - $d_f \approx 20.62$
 - $d_r \approx 26.93$
 - $d'_f = 0 - (-5) = 5$
 - $SINR_{\text{後}} = \frac{S_{\text{後}}}{I_{\text{後}}} = \frac{(\frac{1}{20.62})^2 + (\frac{1}{26.93})^2}{(\frac{1}{5})^2} \approx 10.73 \approx 10.3 \text{ dB}$
 - 有改善教授的連線品質，因為 $SINR_{\text{後}}$ 比 $SINR_{\text{前}}$ 大了 8 dB

C. Tiaosu’s Hotspot

Gimme expensive French meal

ref: 1 (https://wiki.archlinux.org/title/Software_access_point#Wireless_client_and_software_AP_with_a_single_Wi-Fi_device), 2 (<https://wireless.docs.kernel.org/en/latest/en/users/documentation/hostapd.html>)

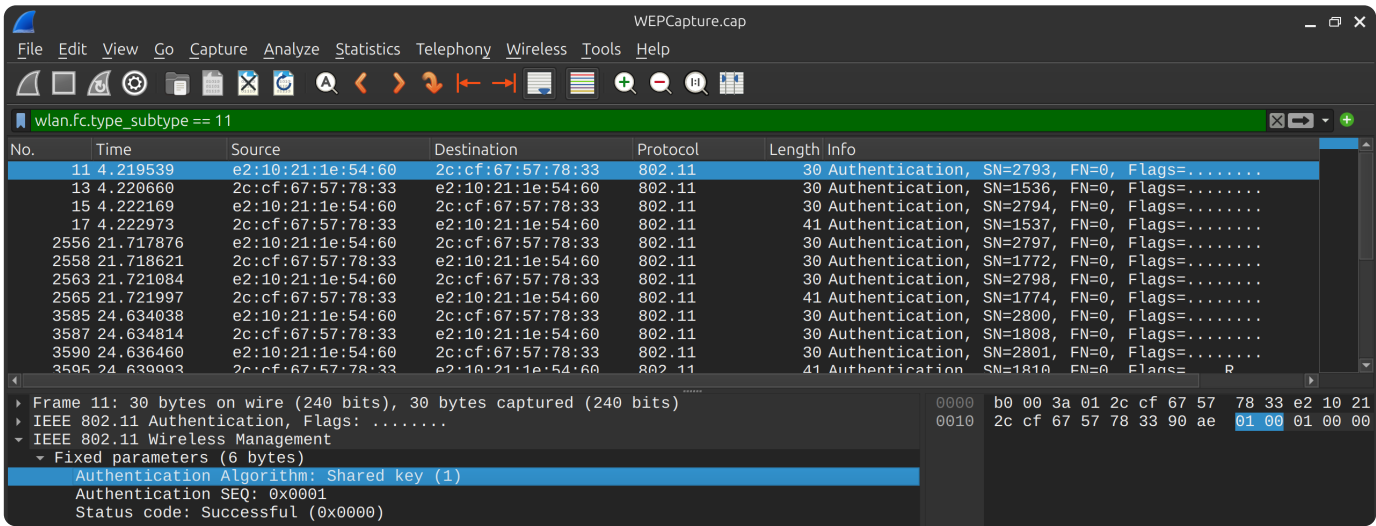
- 1. 另外繳交 b11901164.conf

WEP is dangerous!

ref: 1 (https://www.informationsecurity.com.tw/article/article_detail.aspx?aid=153), 2 (https://www.aircrack-ng.org/doku.php?id=arp-request_reinjection)

- 2.
 - Open System Authentication:
 - 1. 用戶端向 AP 發出連線請求
 - 2. AP 直接允許，即使密碼錯誤也可認證成功
 - 3. 用戶端再透過 WEP 密鑰進行資料加密傳輸，若密鑰錯誤，雖然能認證，但資料無法正確加解密，連線會中斷或無法用
 - Shared Key Authentication:
 - 1. 用戶端向 AP 發出連線請求
 - 2. AP 傳送一個隨機 challenge text
 - 3. 用戶端用事先設定好的 WEP 密鑰對這個字串加密，回傳給 AP
 - 4. AP 用自己的 WEP 密鑰解密後，檢查是否正確， 果正確則認證通過，但若錯誤則拒絕連線

3. (a) Shared Key



(b)

- ARP (Address Resolution Protocol)
- 因為 ARP 封包格式簡單、封包小，而且頻繁，幾乎每台設備都會定時 broadcast ARP request，讓 attacker 容易重複發送
- ARP Request Replay Attack：反覆送 ARP 封包 → AP 會用不同 IV 加密回傳 → 收集大量 WEP 封包和 IV 值
→ 用來破解 RC4 金鑰

(c)

- 1. sudo apt install aircrack-ng -y
- 2. aircrack-ng WEPCapture.cap
- 3. 金鑰為 63:73:6C:3C:33 對應 ASCII 為 cs1<3

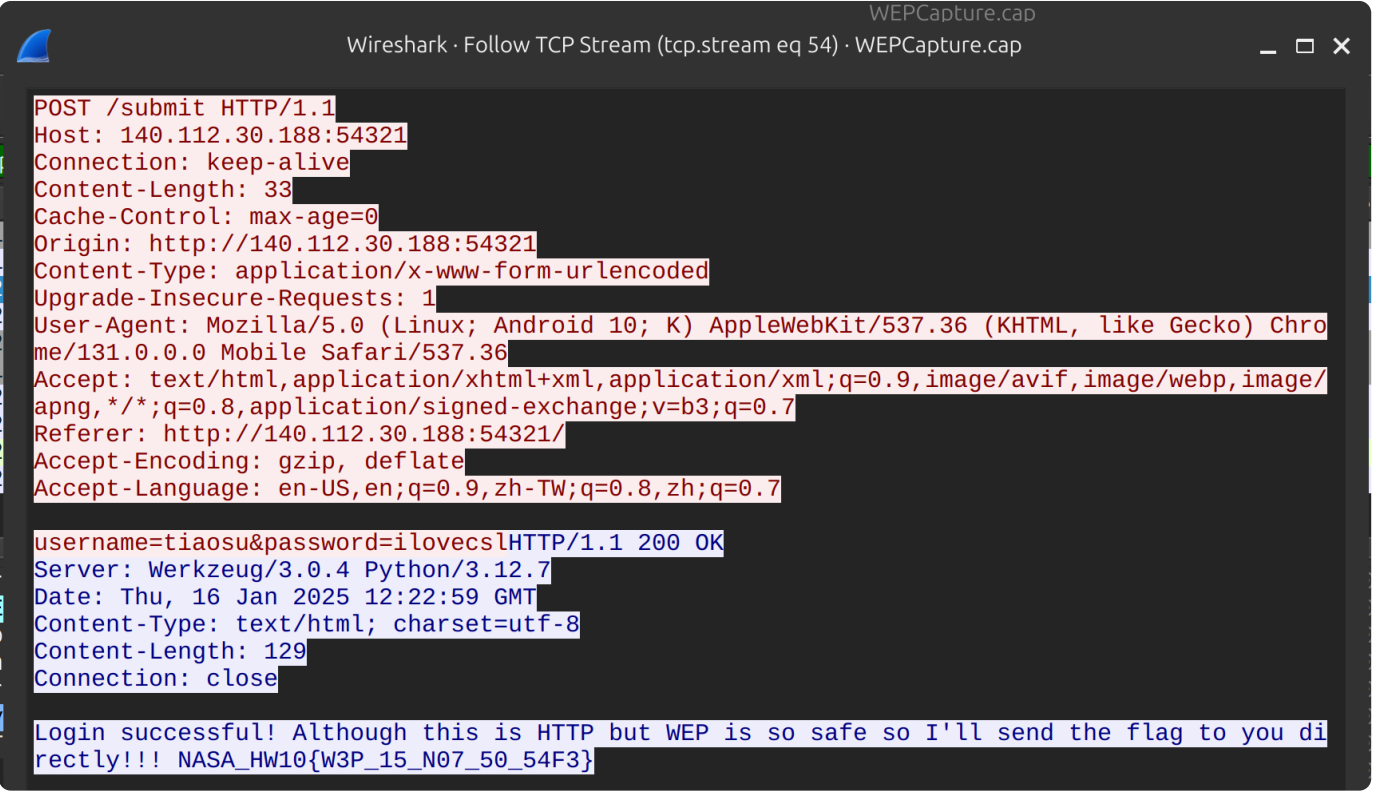
```
Aircrack-ng 1.7

[00:00:02] Tested 1328 keys (got 5141 IVs)

KB   depth  byte(vote)
0    5/ 9    EA(7424) 03(7168) 23(7168) 63(7168) 07(6912) 29(6912) 2E(6912) E5(6912) 11(6656) 22(6656)
1    4/ 5    73(7680) 02(7424) 0B(7424) 21(7424) 44(7424) 45(7424) 7B(7424) 14(7168) 6D(7168) B0(7168)
2    1/ 5    6C(8704) 7C(8704) 5C(7936) 7E(7936) 23(7680) 6D(7680) AC(7680) 39(7424) 88(7424) 9E(7424)
3    0/ 6    3C(8448) 82(8448) EB(7936) D3(7680) 53(7680) 86(7680) 29(7424) 4B(7424) BE(7424) AD(7168)
4    0/ 1    33(9728) DB(8448) 43(7936) F2(7936) 1C(7680) 2D(7680) 5F(7424) 69(7424) 96(7424) 61(7168)

KEY FOUND! [ 63:73:6C:3C:33 ] (ASCII: csl<3 )
Decrypted correctly: 100%
```

(d)



```
Wireshark · Follow TCP Stream (tcp.stream eq 54) · WEPCapture.cap

POST /submit HTTP/1.1
Host: 140.112.30.188:54321
Connection: keep-alive
Content-Length: 33
Cache-Control: max-age=0
Origin: http://140.112.30.188:54321
Content-Type: application/x-www-form-urlencoded
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Mobile Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Referer: http://140.112.30.188:54321/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9,zh-TW;q=0.8,zh;q=0.7

username=tiaosu&password=ilovecslHTTP/1.1 200 OK
Server: Werkzeug/3.0.4 Python/3.12.7
Date: Thu, 16 Jan 2025 12:22:59 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 129
Connection: close

Login successful! Although this is HTTP but WEP is so safe so I'll send the flag to you directly!!! NASA_HW10{W3P_15_N07_50_54F3}
```

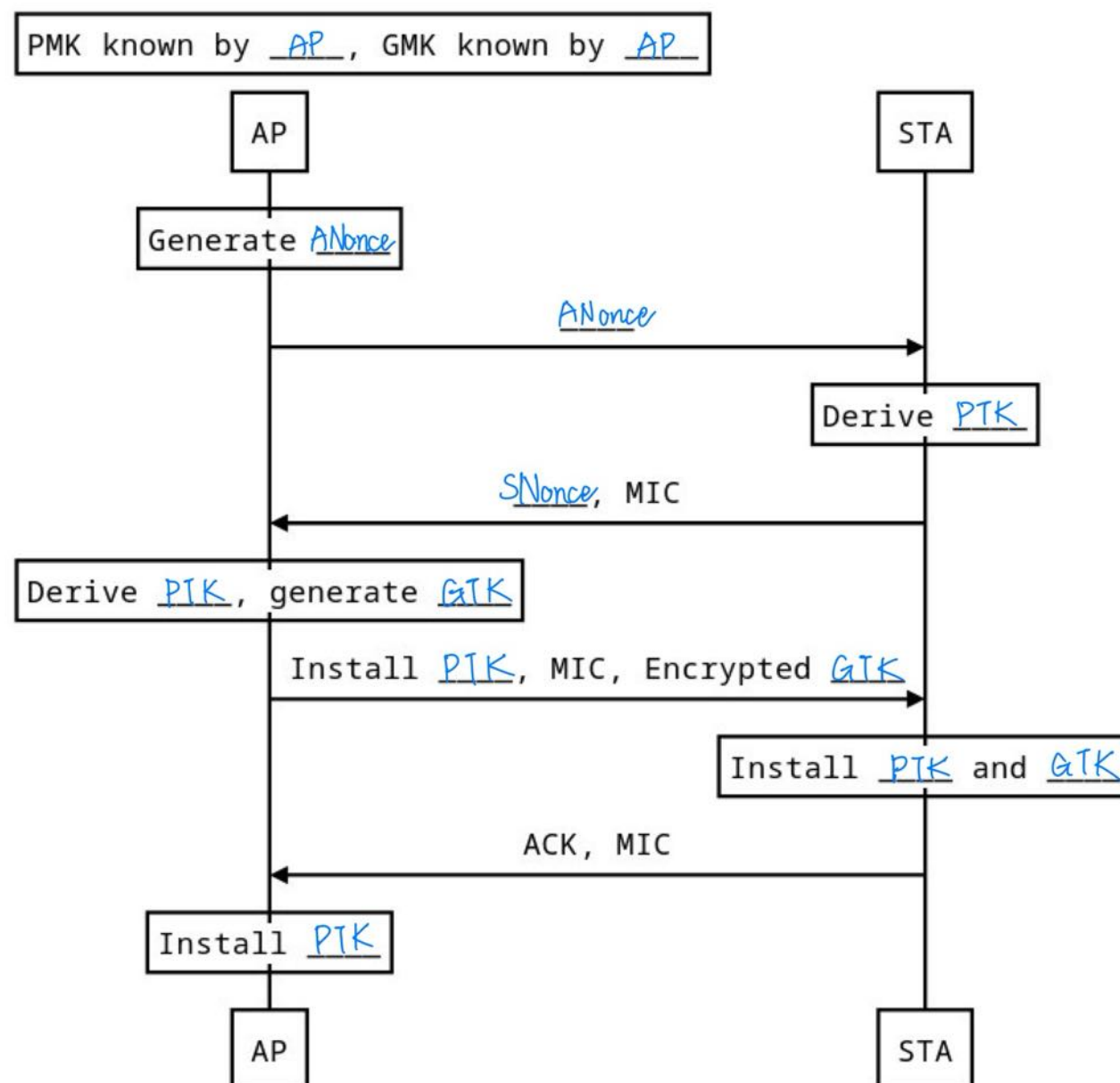
- Server IP: Server IP
- Port: 54321
- 帳號：tiaosu
- 密碼：ilovecsl
- Flag: NASA_HW10{W3P_15_N07_50_54F3}

4. 我不同意他的論點，因為即使 WEP 被破解，攻擊者無法直接解密 HTTPS 流量，攻擊者即使能看到 HTTPS 封包，也只能看到經過 TLS 加密後的資料，無法還原成明文內容。

I must get free hotspot

ref: 1 (<https://hackmd.io/@Veternal1226/H1AaSJCiL>), 2 (<https://yuanchieh.page/posts/2019/2019-01-20-%E5%A6%82%E4%BD%95%E7%94%A8%E8%A7%A3%E9%99%A4%E6%8E%88%E6%AC%8A%E6%94%BB%E6%93%8A%E5%BC%B7%E8%BF%AB%E8%A3%9D%E7%BD%AE%E6%96%B7%E7%B7%9A-wifi-%E9%80%A3%E7%B7%9A/>), 3 (<https://www.cnblogs.com/lstdb/p/10075508.html>)

5. ○ 四向交握的循序圖：



希望達成的目標：

- 雙方驗證彼此是否持有相同的 PMK：透過 ANonce 和 SNonce 雙方計算相同的 PTK，用 MIC 驗證對方是否真的持有正確 PMK 來防止中間人攻擊。
- 動態協商生成並分發 GTK：AP 在第三步裡用 PTK 保護 Encrypted GTK 傳給 STA，確保廣播與多播訊息也能安全加密傳送給所有合法 STA。

6. Deauthentication Attack（解除認證攻擊）是一種針對 Wi-Fi 網路的攻擊手法，攻擊者透過發送偽造的 Deauthentication 封包，強制將目標用戶端踢下 Wi-Fi 熱點，當用戶端被踢下線後，若它設定為自動重新連線，它會馬上重新連線，觸發 WPA 的 4-way handshake，攻擊者這時只要在附近監聽，利用像 airodump-ng 這類工具則能捕捉到完整的 4-way handshake 封包。
- 這組 4-way handshake 裡就包含了可以用來對 Passphrase 進行字典攻擊的必要資訊：AP 和 STA 的 MAC 位址，ANonce 和 SNonce，MIC，攻擊者透過這些資訊，就能離線進行字典攻擊，暴力測試大量可能的 passphrase，直到算出正確的 MIC，成功還原密碼。

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

(b) 21

(c) 4 次完整的

(d) aircrack-ng -w rocktiaosu.txt -b 2c:cf:67:57:78:33 DeAuthCapture.cap 找到
Passphrase: felwinter

```
Aircrack-ng 1.7

[00:15:30] 12004198/14344392 keys tested (13105.54 k/s)

Time left: 2 minutes, 58 seconds                        83.69%

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   : 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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) 去 Edit > Preferences > Protocols > IEEE 802.11, 把 wpa-pwd felwinter:tiaosu 加到 Decryption keys 內, 並以 bootp 為 filter 找到第一組 DHCP ACK 封包, 找到 Your (client) IP address: 192.168.0.81

