Homework #10

Due Time: 2025/05/13 (Tue.) 21:59
Contact TAs: `vegetable@csie.ntu.edu.tw`

Instructions and Announcements

- **NO LATE SUBMISSION OR PLAGIARISM IS ALLOWED.**
- Discussions with others are encouraged. However, you should write down your solutions **in your own words**. In addition, for **each and every** problem you have to specify the references (the URL of the web page you consulted or the people you discussed with) on the first page of your solution to that problem.
- Some problems below may not have standard solutions. We will give you the points if your answer is followed by reasonable explanations.

Submission

- Please place your answers in the same order as the problem sheet and do not repeat problem descriptions, just organize them by problem number in a tidy manner.
- Please zip the pdf file and optionally other files (you may include it in the pdf or submit them separately) Name the zip file "`{your_student_id}.zip`", and submit it via NTU COOL. The directory layout should be the same as listed below:

```
{your_student_id}/
+-- {your_student_id}.pdf
+-- ({your_student_id}.conf)
+-- ({your_student_id}.png)
```

Grading

- The total score for the correctness and completeness of your answer is 100 points.
- It's possible you don't get full credits even if you have the correct answer. You should show how you get the answers step by step and list the references.
- Tidiness score: 3 bonus points, graded by TA.
- Final score = correctness score + tidiness score.

Wireless

- 請盡可能寫出你所知道/查到的內容，我們會依照作答的完整程度及詳細程度評分
- 請務必附上資料來源；如果使用 chatGPT 等 LM 提供的資訊，請不要全部照抄，請用自己的話寫，並附上 LM 生成回覆的截圖或是連結
- 黑色邊框內的文字是與題目無關的前情提要，可直接跳過而不影響作答。
- Flag format：`NASA_HW10{[0-9A-Za-z_]+}`

A. Miscs (10%)

1. 請簡述 SSID 與 BSSID 分別是什麼？兩者之間是什麼關係？(5%)
2. 同一個 AP 是否有可能同時有很多 SSID？不同 AP 是否有可能共用同一個 SSID ？如果可以，請稍微描述一下可能的情境，如果不行，請解釋原因。(5%)

B. HTML's Wi-Fi Problem (20%)

成為無線組（i.e. 線 Wire 少 less 組）一員的你在某個週一下午，在宿舍發現你修的課「超文本標記語言」的教授上課過了十幾分鐘都還沒開直播，與此同時在教室的麻吉也在 DC 標注你，叫線少組滾出來修 csie-5G，你才發現 R103 又双叒叕連不上 csie-5G 了。

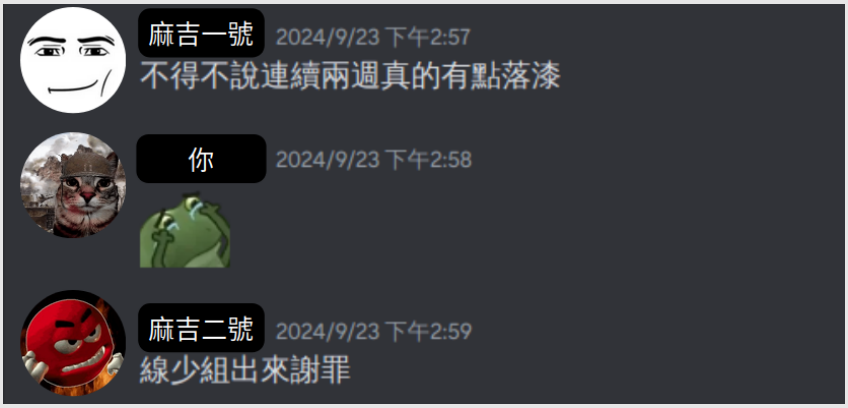

Figure 1: 你和麻吉的對話

為了挽回無線組尊嚴的你，不惜斥巨資添購了一台 Ruckus R600 來加強 R103 教室的信號強度，希望下次超文本標記語言上課時教授能順利開直播。

在課程中我們有介紹到 Friis transmission equation，這個公式能用來計算無線網路中傳輸端功率 P_t 與接收端功率 P_r 間的關係。假設接收端與傳輸端天線的增益各為 G_r, G_t（注意：在這個公式內，G_r, G_t 的單位**不是 dB** ！）天線間的距離為 d，訊號的波長為 λ，則：

$$\frac{P_r}{P_t} = G_t G_r (\frac{\lambda}{4\pi d})^2$$

請你使用這個公式（以及該公式的所有假設，如傳輸端與接收端均為 isotropic radiator，不存在 multi-path propagation 等，詳細可參考 Wikipedia - Friis transmission equation）以至多三句話（和/或算式）回答下列問題（答案相對誤差在 10% 以內即可）：

1. 對於 2.4 GHz 和 5 GHz 的 Wi-Fi，在僅根據 Friis transmission equation，且於相同距離 d、相同發射功率 P_t、相同傳輸及接收天線增益 G_t, G_r，何者接收訊號強度較高？(5%)

2. 對於一個頻率為 5 GHz 的 Wi-Fi，假設 $G_t = G_r = 0$ (dB)，且接收端與傳輸端的距離為 1 (m)，在僅根據 Friis transmission equation 下，請計算 P_r/P_t 為何？請將答案以 dB 表示。(5%)

3. 下圖是 R103 教室的俯視圖，粉色方框是目前教室中兩台 AP(R103-front/R103-rear)的位置，圖片左下角是教授平常上課的使用的裝置所在位置，而你希望將 AP 設置在下圖中的 R103-front-2（藍色方框）的位置。圖片中標示的數對 (a, b) 是上述位置在二維平面（單位：m）的座標。假設：

   - 教授的裝置會優先與距離最接近的 AP 建立連線。
   - 四台裝置均為 $G_t = G_r = 1$。
   - 三台 AP 均隸屬 csie-5G 這個 SSID，使用相同的頻道，並且 P_t 值相同。
   - 在 Downlink transmission 中，干擾來自**所有**其他使用**相同頻段的 AP**，且 Inter-symbol interference 可以忽略。(真實情況中因 CSMA，來自其他 AP 的干擾通常會較小，此題請假設 CSMA 失效)
   - 環境及接收電路中的 Noise 遠小於干擾，因此在干擾存在時可以忽略。

   請你計算出新 AP 設置前後，教授的裝置所分別接收到的 Downlink SINR 值。若只考慮 SINR 值，你覺得新 AP 的設置位置有沒有改善教授的連線品質？(10%)

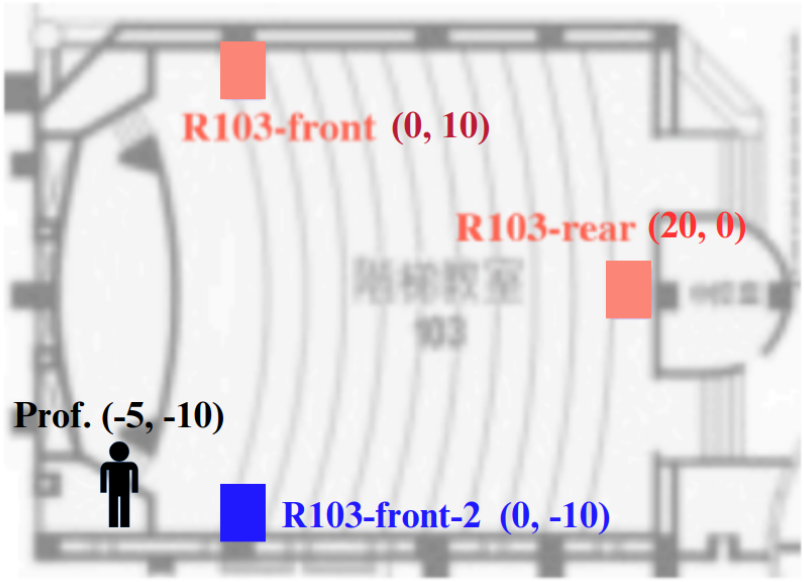

Figure 2: AP locations in R103

C. Tiaosu's Hotspot (70%)

身為富二代的條斯最近買了一台樹莓派，為了向朋友們展示他的財力，他決定用這台樹莓派架設一台 AP，免費提供無線網路給朋友們使用！因此，他決定以118 巷 6000 元的法餐作為交換，請身為 NASA 專家的你幫他架設 AP。

Gimme expensive French meal (10%)

在查詢 ArchWiki 後，你決定使用 `hostapd` 這個套件來架設他的 AP，以下是條斯的要求：

- 使用 `wlan0` 這個介面作為 AP，並將送到 AP 的封包藉由橋接介面 `br0` 轉送到這台樹莓派的乙太網路介面。你可以假設 `br0` 已經建立好，並且乙太網路介面已經加入到 `br0` 裡。
- 使用 WEP 這個安全協定。
- 朋友用手機連線的時候，會看到 Wi-Fi 名稱叫 `tiaosu`。(如下圖)
- AP 能支援符合 802.11g 標準的設備。
- AP 在使用的頻段符合 中華民國國內規定 與 IEEE 802.11g 標準的前提下（換句話說，你不能使用沒有開放的頻段，且使用頻道的間距需符合標準，需納入 guard band 的考量）不會受到使用 Channel 1, 11 的 AP 干擾 (Adjacent-channel interference)

Figure 3: Wi-Fi 名稱示意圖

1. 請你在不刪減已有的設定的前提下，完成 這個 `hostapd` 設定檔 以達成條列出的所有要求。檔案中的 `wpa_key0` 欄位不需要修改。
   Note：本題不需要實際將 AP 架設起來，請閱讀 `hostapd` 的相關文件完成設定檔即可。
   Note：你可以選擇在 pdf 中直接附上檔案，或者另外繳交 `{your_student_id}.conf`。

WEP is dangerous! (30%)

> 有了 WEP 的「保護」，條斯決定之後上網都不需要 SSL/TLS 了～
> 然而，聰明的你知道 WEP 超級不安全，為了說服你的雇主使用更安全的加密協定，你決定偷偷紀錄了條斯使用這台 AP 的過程並保存在 WEPCapture.cap 這個檔案裡，並且破解出他和某個祕密組織「CSL」的對話作為證明。

2. WEP 有提供兩種 Authentication 的方式：Open System Authentication 和 Shared Key Authentication，請簡述他們個別如何運作。(6%)

3. 請你使用 Wireshark（如果你不熟悉這個工具，可以看這邊的簡單教學）分析 WEPCapture.cap 這個封包記錄檔，已知這個紀錄檔記錄了一個 Client、一個使用 WEP 作為驗證方式的 AP 和一個 Attacker 之間的連線，請回答下面幾個問題：(18%)

   (a) 接續你在 2. 的答案，請你判斷 Client 第一次連線是藉由哪一種 Authentication 方法驗證成功的？(4%)

   (b) WEP 因為其封包中過短的 IV 欄位，藉由蒐集足夠多的封包可以讓 Attacker 破解 WEP 的加密連線（why?）為了蒐集封包，在此情境中的 Attacker 利用了什麼網路協定 (2%)，竊聽並重複發送該協定的封包給 AP 以達成蒐集 IV 欄位的目的？這種攻擊手法又叫做什麼？(2%)

   (c) 這個連線設置的金鑰是什麼？你可以使用任何方式找到答案，惟請說明你執行的步驟。(4%)

   (d) 請你利用找到的金鑰解密 Client 和 AP 間的 Traffic。Client 在封包紀錄期間上了某個服務並送出了他的在這個服務使用的帳號密碼，請你找出 Host 這個服務的 Server IP、服務所屬的 Port，Client 輸入的帳號密碼，以及該服務回傳給他的 Flag。(6%)

   - Hint 1：`aircrack-ng` 這個工具或許能幫得上你？
   - Hint 2：怎麼叫 Wireshark 幫我破解 WEP traffic？

4. 你的朋友 Shaxx 在跟你討論 WEP 的安全性時提到：「連到使用 WEP 的熱點絕對不安全！任何能夠竊聽我們連線的 Attacker 可以輕易的破解熱點密碼，然後解密我的任何封包，甚至能偷走我透過 HTTPS 傳輸的帳號密碼。」你是否同意他的論點？請簡述你的判斷理由。(6%)

I must get free hotspot (30%)

> 發覺祕密洩漏的條斯非常錯愕，於是決定把他的 AP 改成使用 WPA-PSK 作為驗證方式，這樣你就炸不出加密的金鑰了！但因為你偷窺的行為，他決定不告訴你他設置的 passphrase，讓你只能淪落到去跟其他人搶 csie 的頻寬。決定一定要蹭到免費熱點的你，決定在條斯朋友輸入 passphrase 的時候在他後面 Shoulder surfing。雖然在你看到完整密碼前你就被他們趕走了，但你總感覺那個密碼似曾相識 (?

5. WPA 相較於 WEP 的最大不同之一就是加入了四向交握的協定，請你填入 PTK/GTK/ANonce/SNonce/AP/STA（可能有重複）來完成下面四向交握的循序圖（圖片檔案）並說明至少兩點四項交握希望達成的目標。注意此圖中並不包含 group key handshake。(8%)
   Note：你可以選擇在 pdf 中直接附上圖片，或者另外繳交 `{your_student_id}.png`。

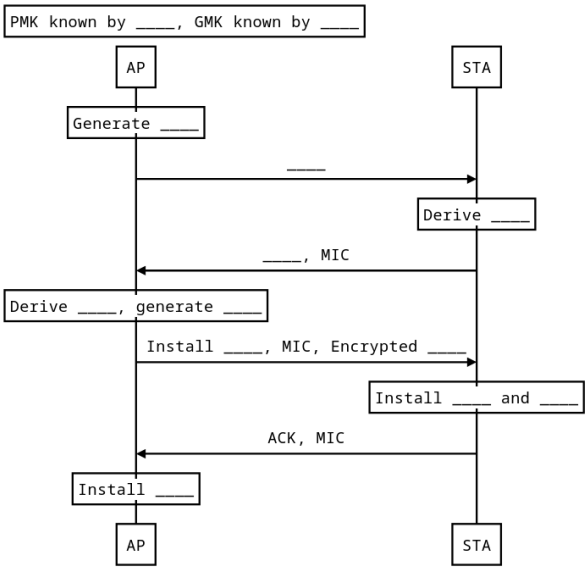

Figure 4: 四向交握循序圖

6. 請解釋何謂 Deauthentication Attack，以及這個攻擊手法如何讓我們得到用來對 Passphrase 進行字典攻擊的所有資訊？(4%)

7. 在你進行了上述的攻擊手法後，你得到了你所需要的封包，並存在 DeAuthCapture.cap 這個檔案裡。已知這個紀錄檔記錄了一個 Client、一個使用 WPA-PSK 作為驗證方式的 AP 和一個 Attacker 之間的連線，請你使用 Wireshark 分析封包紀錄，並回答下面幾個問題：(18%)

   (a) Client/AP 的 MAC address 分別是？(2%)

   (b) Client 第一次進行 4-way handshake 的 Message 1 對應的封包編號為？(2%)

   (c) 請問 Victim 在檔案紀錄的期間一共與 AP 進行了幾次完整的 4-way handshake？(4%)

   (d) 這個 AP 設置的 Passphrase 是什麼？你可以使用任何方式找到答案，惟請說明你執行的步驟。(4%)

   (e) 已知這台 AP 上有架設 DHCP server，請你用上一題找到的 Passphrase 解密 Client 和 AP 間的 Traffic，並找出 Client 在第一次連線後被分配的 IP 是？(6%)

   - Hint 1：Passphrase 藏在 rocktiaosu.txt 這個檔案裡。
   - Hint 2：`aircrack-ng` 這個工具或許又能幫上你的忙？

> 在你知道條斯的 Passphrase 後，你每天都偷偷坐他旁邊蹭他的免費熱點內卷。在你享受高速連線的同時，你不禁思考如果條斯設置的是特別強的密碼，那他的 WPA 熱點是不是就絕對安全了？

8. (本題不計分) 何謂 KRACK attack，這個攻擊能夠達成什麼目標，針對的是哪一種/哪些無線安全協定 (WEP/WPA/WPA2/WPA3)？請搭配你在 (5) 回答的四向交握循序圖說明這個攻擊的執行細節，請假設 Client 安裝 PTK/GTK 後仍然會接收來自 AP 未加密的 Message 3。(0%)

   - Hint：或許參考原論文能幫你了解這個攻擊的細節。