國防科技學術合作研究計畫成果報告

IEEE 802.11 WLAN 鏈路層之安全問題研究

計畫編號： NSC96-2623-7009-003-D

執行期間： 96 年 1 月 1 日 至 96 年 12 月 31 日

計畫主持人：葉義雄教授

執行單位：國立交通大學資訊工程學系

中華民國 96 年 12 月 31 日

摘要

由於無線區域網(WLAN)路使用 RF，使得 WLAN 更容易受到攻擊。尤其當 WLAN 用於內部網路，一些機密且敏感的資訊將會吸引許多攻擊者。然而，許多已部署的 WLAN 系統都不是很安全，甚至是開放系統，這些情形都將限制其發展。雖然 WLAN 安全標準逐漸完備，然而複雜又多樣的認證方法有可能使安全的演算法因協定的運作產生漏洞，而這樣的情形在 WEP 已經發生。因此有必要對新的 WLAN 安全標準做有系統的分析，才能推廣更多的應用。

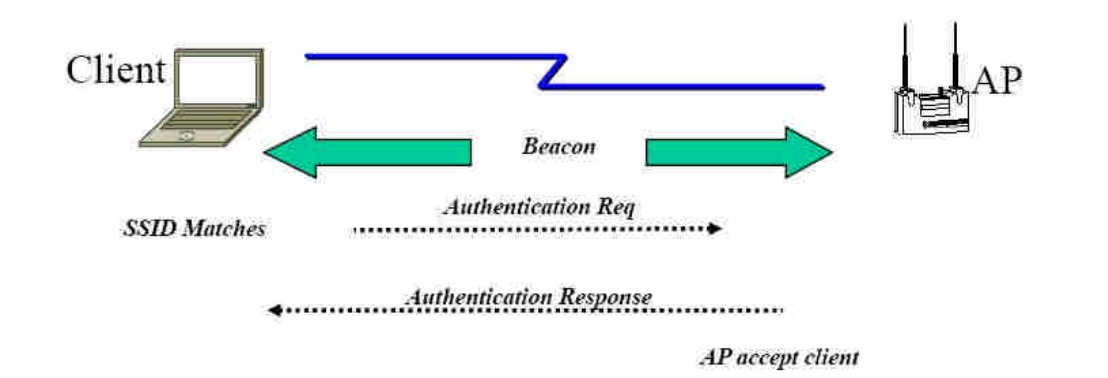
Abstract

Since WLANs (Wireless LANs) use radio waves, wireless LANs are open to hackers trying to accesssensitive information or spoil the operation of the network. In fact, most wireless LANs doesn't implement any form of reliable security, enabling access to just about anyone. Although the security standards of WLANs are complete progressively, their complexity will make security leaks. So, we need to make a systematic analysis for the security standrds.

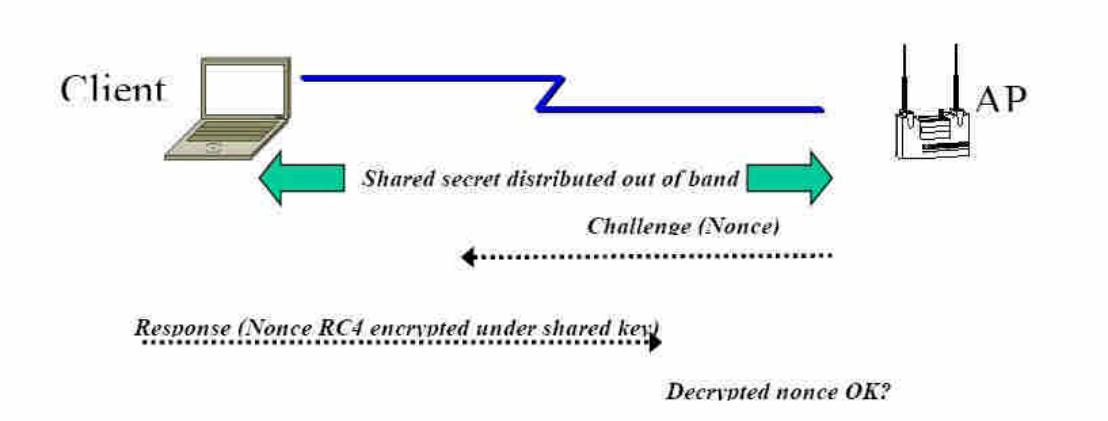
一、前言

在無線通訊中，因為 RF 有人人可及的特性，傳輸資料被竊聽是常見的現象。任何欲竊聽者只要將其竊聽器的接收頻率調至傳送頻率即可順利進行竊聽的工作。為了解決這個問題，IEEE 802.11 [7]標準中制定了一個有線等效的資料保密演算法(WEP, WiredEquivalent Privacy Algorithm)，希望可以保護無線網路之授權使用者免於被竊聽的煩惱。有線網路上要進行竊聽的工作至少要連接到線上，然後才可以進行攻擊。無線網路雖然不具備這種特有的安全屬性，802.11 卻希望能提供與此功能相當的安全性。因此，IEEE 802.11 標準定義兩種不同的驗證方法：開放系統(open system)與共用金鑰(shared key Authentication)。

開放系統是最簡單的認證架構，client 端對 AP 送出 Authentication 要求，再由 AP 送回 Authentication 回應就可，如下圖所示。



這樣的架構是不需要任何密碼演算法，也就是 Authentication Req 及 AuthenticationResponse 是沒有經加解密就傳送，因此不具任何認證效用。Shared key 認證架構，則是藉由 AP 與 client 間共享的金鑰做認證，如下圖所示



在 Shared key 認證架構中，Client 首先送出 Authentication 要求，AP 跟著

就送出 challenge 給 client，client 加密後回送給 AP，最後由 AP 檢查是否可解密成功，若是則認證 client。由上面的描述，802.11 所定義的安全協定無法滿足多 client 的情況，因為沒有動態金鑰管理的機制。同時，在始用靜態金鑰的 WEP，也被發現解的方式。802.11 標準有下列安全性問題：

- 多個 client 使用同一把金鑰做認證；
- 不支援延伸驗證方法 (例如，憑證/智慧卡)；
- 不支援金鑰管理，包括動態、每個站台或每個 session 的金鑰管理。

因此，IEEE 標準組織訂定 802.1X 來解決這些問題。基本上，802.1X 提供下列功能來解決 802.11 的安全問題：

- 每個 client 使用不同的 secret 做認證；
- 支援延伸驗證方法，也就是可延伸的驗證通訊協定 (EAP)；
- 支援動態金鑰管理，並支援每一 client 或每一 session 有不同的加解密金鑰。

IEEE 802.11i 是更近的安全標準，802.1X 為其子集。802.11i 解決 WEP 加密所留下的所有安全性問題，它定義新的演算法 CCMP (Counter Mode CBC MAC Protocol)及 TKIP 取代原有的 WEP，其中 TKIP 沿用 RC4 演算法是 WI-Fi [10] 業界聯盟提出，而 CCMP 則使用 AES 是更安全的演算法，在 802.11i 中，屬於必要選項。

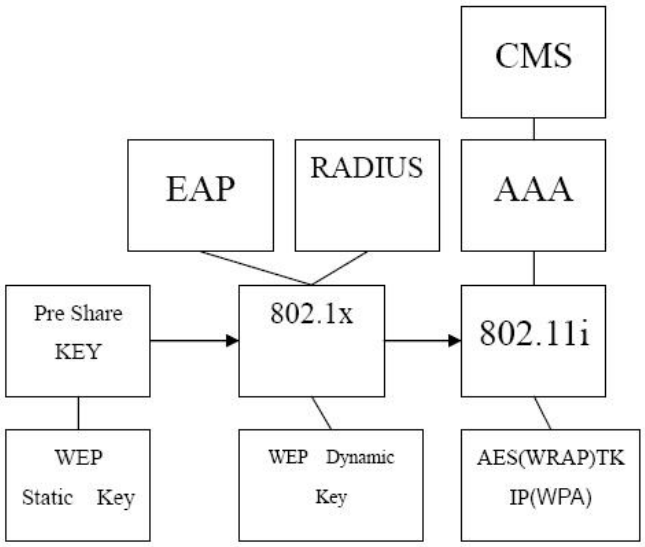
本計畫將針對現有 WLAN 安全協進行分析，首先會針對加解密演算法加以分析，包括 RC4，AES 以及相對應不同 session key 的產生演算法，如動態 WEP，TKIP 及 CMMP。在這階段將會建立 802.1X 環境，實際去分析金鑰變化的狀態，在各種攻擊假設下，進行密碼分析。在 802.1X 的環境，會有各種認證方法配合不同的加解密演算法，我們將會依據已知的攻擊模式，來假設可取得的資訊，進而分析最新的安全標準。同時，也會依據不同設定來進行攻擊及分析，這是因為 802.1X 的設定包了重新認證(re-auth)，金鑰更新(keyrefresh)及金鑰管理方式，都會影響密碼分析的可行性。本計劃將對最新的無線區域網路的安全標準做有系統的分析，希望藉由此次的研究，把安全標準與實際的設定運作做比較，列出各種合於標準的各種設定的安全度。

三、研究重要性

由於 WLAN 安全標準逐漸完備，然而複雜又多樣的認證方法有可能使安全的演算法因協定的運作產生漏洞，這樣的情形在 WEP 已經發生。因此，本計劃會有系統的分析各種認證協定及金鑰管理方法，嘗試找出新的安全漏洞，以加強無線區域網路的安全。除此之外，WiMAX (最新無線廣域網路標準)也將採取相同的架構，因此，若仍分析出 WLAN 安全標準各種組合的安全度，將推廣應用在更多的地方。

四、國內外有關本計畫之研究情況

(1). 無線區域網路安全協定簡介無線區域網路安全標準原本只是 IEEE 802.11b 標準的一部份，造成現有產品需要手動管理 WEP 金鑰，即是當使用者要使用加密的通道時，必須向系統管理者事先取得金鑰。以目前的產品為例，客戶端(client)與存取點(access point, AP)會互相分享四把金鑰,同時作為認證及授權使用此通道兩種用途，由於金鑰無法線上動態交換，因此 client 與 AP 會長時間使用相同的金鑰，而無法即時取消對某使用者的使用，造成認證上的失誤。幾篇探討 WLAN 安全問題的文章，可歸納成探討 WLAN 管理機制的不足，如 University of Berkeley [3]的教授在 2001 年 2 月發表文章指出 WEP 協定需要額外的金鑰管理機制，2001 年 4 月 University of Maryland [2]教授發表的文章則指出 IEEE 802.11b 原有的認證機制的問題及同樣也是 University of Maryland 教授發表的文章指出最新定義的 IEEE 802.1X 易遭受攻擊同時也模擬相關情境證明可行。另一類則是由 RC4 的分析，破解 WLAN 系統金鑰，這是由 University of Berkeley [5]的教授提出，同時可在網站(http://wepcrack.sourceforge.net)上下載相關套件。因此，IEEE 標準組織定依出一系列的標準解決這些安全問題[9]，同時相容業界目前的作法，如下圖所示：



WPA : WIFI Protected Access is a subset of 802.11i
WRAP : wireless robust authenticated protocol use AES as its encryption algorithm
CMS : AAA間的安全協定,其實就是PKCS7

這些安全協定的目標為新增或加強下列的功能：

- 存取控制及互相認證；
- 認證的程序由更高層的協定完成；
- 每個認證回合即交換金鑰；
- 修正現有使用 RC4 的問題；
- 能夠快速部署新定義的認證方式。

(2). WLAN 加密演算法簡介

CCMP 為計數器模式的 CBC-MAC 的 AES 演算法，是最新定義的演算法，只使用於較新的網卡中，也稱為 WPA2 (Wi-Fi Protected Access 2)。WPA 則是使用 TKIP 演算法，而 TKIP 則是改良 RC4 金鑰的產生方式，主要目的是相容於舊網卡的硬體，下表為這些演算法的整理。

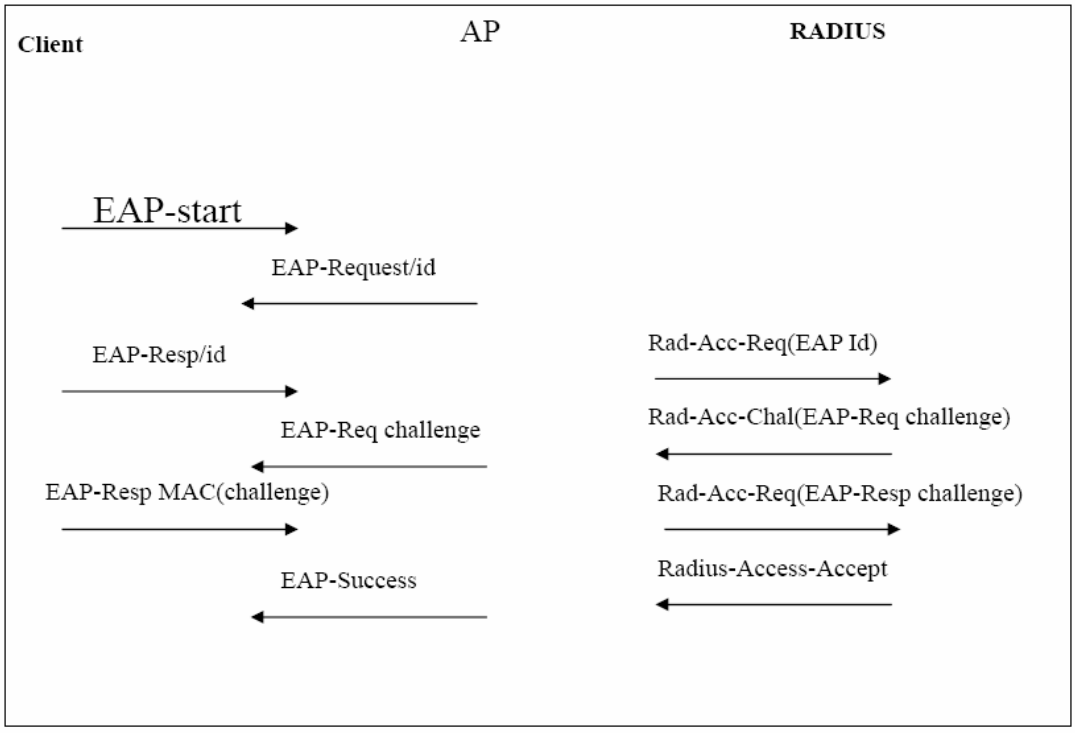
	WEP	TKIP	CCMP
Cipher	RC4	RC4	AES
Key Size	40 or 104 bits	128 bits	128 bits
Key Life	24-bit IV	48-bit IV	48-bit IV
Data Integrity	None	Michale	CCM
Key management	None	EAP-based	EAP-based

(3). IEEE 802.1X [6]的認證方式

IEEE 802.1X 的認證方式大約可分成三類，

- 基於密碼方式(Password base)；
- 基於電子憑證方式(Certificate base)；
- 基於 SIM 卡方式(SIM card base)。

對應這三類的認證方式且適用於無線區域網路的有 EAP-MD5、EAP-TLS 及 EAP-SIM，其中混合 1,2 類的認證方式為 EAP-TTLS。接下來將一一介紹這些認證方式。EAP-MD5 認證方式是假設客戶端與認證伺服器事先共享一把金鑰，再利用 MD5 演算法保護客戶端密碼，這樣的認證方式與其他方式比較的缺點是無法達成互相認證的效果及無法於認證過程動態產生金鑰。EAP-TLS 認證方式是由 MicroSoft 與 Cisco [8]共同提出的標準，需要公開金鑰基礎建設(PKI, Public Key Infrastructure)，也就是假設客戶端與認證伺服器事各自擁有電子憑證，以數位簽章的技術達到互相認證的效果，並同時可在客戶端與認證伺服器間交換金鑰。理論上，這樣的機制最具彈性，不過因為 PKI 的建製相當複雜，將使得大規模的部署產生很大的困難，基本上即是缺乏完整的 PKI 建設。下圖為 EAPS 基本架構，客戶端及 RADIUS 利用 TLS[4]協定將產生的數位簽章互相傳給對方，達到互相認證的功能。



EAP-SIM 認證方式則是由 3GPP [1]所提的標準，主要想要結合電信業者現有的 SIM 卡認證體系，因為電信業者的認證體系相當成熟，因此不需重新建設後端認

證系統，但是客戶端需要額外設備，並且因使用電信網路，可能需要較高的連線費用，因此是否可結合後端認證系統優勢及原有廣大的客戶群，而成強勢的標準，還不可知。主要利用 SIM card 與 Operator 認證中心(AuC, Authentication Center)互相共享的金鑰及相關演算法，達成互相認證的功能。

(4)金鑰還原之方法

這裡將會針對 WEP 和 WPA-PSK 的加密協定的攻擊方法做理論的闡述。

- **對 WEP 進行還原金鑰**

針對 WEP 進行金鑰還原攻擊主要有下列兩種方法：

暴力攻擊法：

在有限的 Secret Key Space 內，一直去測試 key，直到找出 User 所使用的 Secret Key 為止，如果 keylength 很長的話，則此法不適用。

FMS 攻擊法：

這是由 Fluhrer、Mantin and Shamir 三人提出來的攻擊法，攻擊的重點在於 RC4 將 Secret Key 展開成 Keystream 時所產生的問題。藉由收集特定型式的 IV 值(或稱為 Weak IV)的封包，來進行統計攻擊。他們發現若 IV 符合(B+3，N-1，X)這種型式，則會洩漏金鑰的資訊，其中 B 代表的是 Secret Key 的 index，N 代表 256，X 代表 8-bit 的任意值。

WEP protocol 的一個很嚴重的問題是 Encrypted payload 的第一個 byte 是已知的，因為 payload 是以 SNAP header 為首，而 SNAP header 的 first byte 是 0xAA，所以藉由 plaintext 的第一個 byte 和 ciphertext 的第一個 byte 做 exclusive-or 就可以還原 keystream 的第一個 byte。

- **破解步驟：**

假設 K[B+3] 為欲破解的 key byte (表示 K[0]，…，K[B+3-1]為已知)

考慮 round B+3 時，

$i_{B+3}=B+3$

$j_{B+3}=j_{B+3-1} + S_{B+3-1}[B+3] + K[B+3]$ (1)

$Swap(S_{B+3-1}[B+3]，S_{B+3-1}[j_{B+3}])$ (2)

由(2)得知：

$S_{B+3}[B+3]=S_{B+3-1}[j_{B+3}]$

$\therefore j_{B+3}=S^{-1}{}_{B+3}\text{-}1[S_{B+3}[B+3]]$

($S^{-1}{}_t[X]$表示 X 值在 S_t 的 index)

由(1)得知：

$K[B+3] = j_{B+3} - j_{B+3-1} - S_{B+3-1}[B+3]$

$= S^{-1}{}_{B+3-1}[S_{B+3}[B+3]] - j_{B+3-1} - S_{B+3-1}[B+3]$

如果 $S_{B+3}[B+3]$是 PRGA 之 first output，則 K[B+3] 破解。

若要 output = $S_{B+3}[B+3]$，考慮 PRGA round 0：

i = i + 1 = 1

j = j + S[1] = S[1]

output = S[S[i]+S[j]] = S[S[1] + S[S[1]]]

若 S[1] = 0，S[0] = B + 3 (這就是(B+3，N-1，X)為 weak IV 的原因)，S[1]+S[S[1]] = B+3，output 將會是 S[B+3]。因為 S[0]，S[1]，S[B+3]在 first output 會被利用到，所以當 S[0]，S[1]，S[B+3]定位之後，直到最後都不被打亂，則 output = $S_{B+3}[B+3]$ 成立。

- **還原 WEP key 步驟：**

(1).收集具 Weak IV 封包；

(2).還原 keystream 的第一個 byte；

(3).$K[B+3]=S^{-1}{}_{B+3-1}[S_{B+3}[B+3]]\text{-}j_{B+3-1}\text{-}S_{B+3-1}[B+3]$這個式子去算出 secret key 的第 B byte 的值；

(4). 統計每一個不同第 B byte 值出現的次數，選擇出現次數最多的作為還原的 key byte；

(5). 重複上面的步驟直到還原所有 WEP key。

- **總結：**

B=0 時，S[0]，S[1]，S[B+3]不被打亂的機率為

$$\Pr = \left(1-\frac{2}{256}\right)\left(1-\frac{3}{256}\right)^{256-4} \approx 0.05$$

比其他的值出現的機率多了 10 倍多，因此只要收集越多的封包，則結果會更明顯。若是 IV [2]或中間破解的 key byte 有打亂，則捨棄這個 IV，一但破解的 Byte 越多，則機率會越高。Weak IV 不只有(B+3，N-1，X)型式[3]，然最早是由 Fluhrer，

Mantin and Shamir 三人所提出來，但現今已經不只這些。統計每一個不同的K[B+3]值出現的次數，選取出現次數最多的作為還原的 key byte。此外，FMS attack 和 brute force 也可以搭配著用。

- **對 WPA-PSK 進行還原金鑰**

由於目前 WPA-PSK 沒有有效的統計攻擊法，只有透過斷線攻擊，來得到認證封包，退而求其次地使用字典攻擊，也就是暴力法的一種。

- **字典攻擊法：**

所謂的字典攻擊法，使用字典中常見的單字、片語、數字、名字和引語去解出密碼。由於一般的使用者常會選擇短的、有意義的英文字、常用的號碼等，做為其密碼，而這些密碼，數量是有限的，因此攻擊者可以快速地反覆猜測與比對，在短時間內就有可能猜出一個使用者密碼。

由於 WPA 將 WEP 的許多缺點修正過來，所以原本的統計攻擊法不再適用於 WPA，目前也沒有好的統計方法，因此只能由工作站和存取點在進行 four-way handshake 時來收集這些 handshake 的封包，藉由這些封包來複製他們的交換 key 的程序，進行字典攻擊法。

五、實驗目的

嘗試對不同的認證環境和加密協定做攻擊，藉此來比較安全性。

六、實驗設備

工作站 1:(攻擊者)

- 目的
  - 嘗試對其他無線設備做攻擊。
- 硬體
  - 筆記型電腦
    - ✓ 品牌：Toshiba

- ✓ 型號：Portege M500
- ✓ 處理器速度：1.6 GHz
- ✓ 記憶體：512 MB

✧ 無線網路卡

- ✓ 品牌：D-Link
- ✓ 型號：DWL-G650
- ✓ 介面卡型式：32bit (Card Bus)
- ✓ 傳輸速率/無線頻率：802.11g/2.4GHz
- ✓ 加密技術：64, 128, 256-bit WEP、WPA/WPA2

➢ 軟體

✧ 作業系統

- ✓ 套件：Ubuntu 6.06
- ✓ 核心：Linux 2.6.15-26-386

✧ 攻擊軟體

- ✓ Aircrack-ng 0.91

工作站 2: (申請網路者)

➢ 目的

✧ 為正常欲尋求網路連線的工作站，作為被攻擊對象。

➢ 硬體

✧ 筆記型電腦

- ✓ 品牌：Asus
- ✓ 型號：M2400
- ✓ 處理器速度：Pentium M 1.7GHz
- ✓ 記憶體：512 MB

✧ 無線網路卡

- ✓ 品牌：ZyXEL
- ✓ 型號：G-220 v2
- ✓ 介面卡型式：USB bus
- ✓ 傳輸速率/無線頻率：802.11g/2.4GHz
- ✓ 加密技術：64, 128, 256-bit WEP、WPA/WPA2

- 軟體
  - 作業系統
    - ✓ 版本：Windows XP service pack 2
  - 連線軟體
    - ✓ wpa_supplicant

存取點(Access Point)

- 目的
  - 在 infrastructure mode 下，銜接無線網路和有線網路的橋樑。
- 型號
  - DI-624S 802.11G 2.4GHz 高速無線寬頻路由器/伺服器

RADIUS server

- 目的
  - 主要是提供認證識別機制，用來辨認使用者的身份與密碼，確認通過之後，經由授權使用者登入網域使用相關資源，並可提供記帳機制，保存使用者的網路使用記錄。
- 硬體
  - 個人電腦
    - ✓ VMware
- 軟體
  - 作業系統
    - ✓ 套件：Fedora core 4
    - ✓ 核心：Linux 2.6.11-1.1369
  - 連線軟體
    - ✓ FreeRADIUS

八、環境架設

工作站 1 (攻擊者)

- 安裝 Ubuntu 6.06，安裝並設定好網路後執行以下程式

  sudo apt-get update

  sudo apt-get upgrade

sudo apt-get build-essential

- **執行下面指令以安裝 aircrack-ng 0.91**

  wget http://download.aircrack-ng.org/aircrack-ng-0.9.1.tar.gz

  tar -zxvf aircrack-ng-0.9.1.tar.gz

  cd aircrack-ng-0.9.1

  make

  make install

工作站 2 (申請網路者)

- 安裝 Windows XP service pack 2 並執行網路更新。
- 安裝 wpa_supplicant for Windows

  ✧ 需事先的安裝軟體

  (1)WinPcap development package:

  下載http://www.winpcap.org/install/bin/WpdPack_3_1.zip

  解壓縮到 C:\dev\WpdPack

  (2)OpenSSL:

  到http://www.slproweb.com/products/Win32OpenSSL.html

  下載 Win32 OpenSSL

  安裝後,將資料夾{Win32OpenSSLRoot}\include 和 lib 複製到 C:\dev\openssl

  (3)developer's pack for WinPcap (WPdpack.zip)

  到http://winpcap.polito.it/install/default.htm

  下載 WinPcap.exe, 安裝

  ✧ 解壓縮 wpa_suplicant 並開啟 wpa_supplicant 資料夾：

  (1) 修改 wpa_supplicant.conf

  ```
  ap_scan=1
  ctrl_interface=
  eapol_version=1
  network={
  ssid="Radius"
  proto=RSN WPA
  key_mgmt=WPA-EAP
  pairwise=TKIP
  ```

group=TKIP

eap=TTLS　#根據不同認證協定來做修改，ex PEAP, MD5

identity="EEE3"

anonymous_identity="ICL1111EEE"

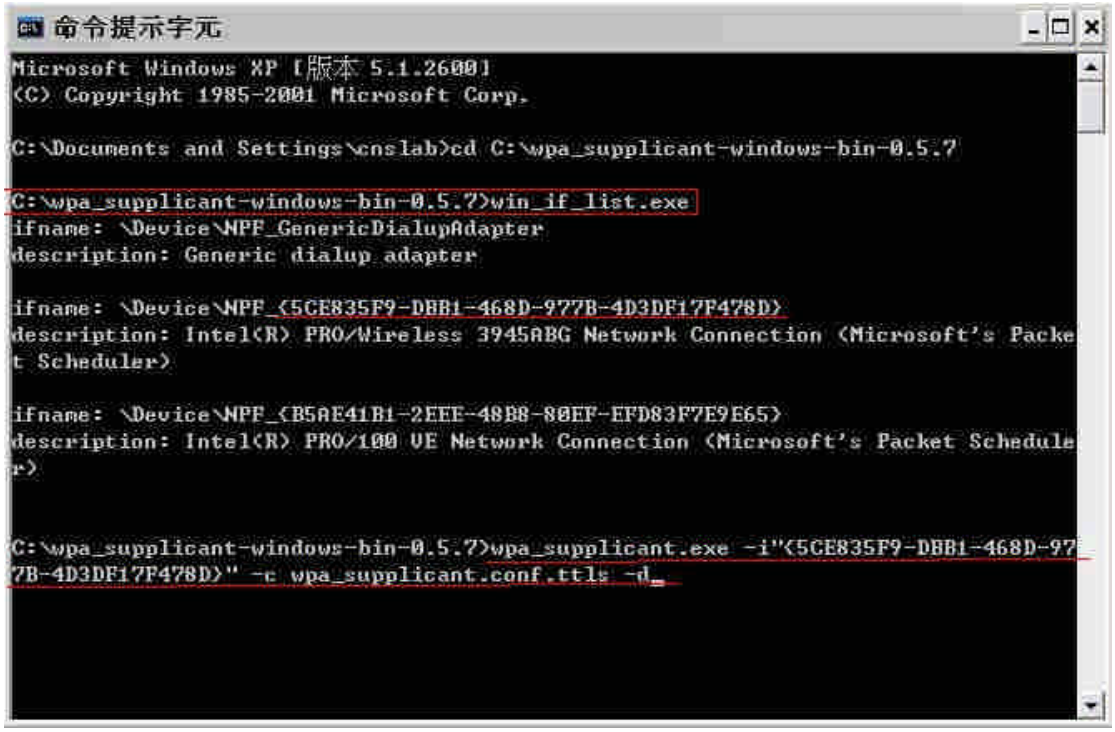
password="test123"

priority=1

phase2="auth=PAP"

mode=0

(2)執行 win_if_list 取得網卡實際 NPF id 並執行 wpa_supplicant.exe，如下圖：



Radius Server

- 安裝 FreeRadius，執行下面指令：

  wget ftp://ftp.freeradius.org/pub/radius/freeradius-1.1.0.tar.gz

  tar xzvf freeradius-1.1.0.tar.gz

  cd freeradius-1.1.0/;

  ./configure

  make

  make install

- 需修改的設定檔
  - ✧ 設定檔目錄/usr/local/etc/raddb

- ✓ radiusd.conf
- ✓ clients.conf
- ✓ eap.conf
- ✓ users

➢ radiusd.conf

✧ 需設定的地方

- ✓ authorize 段：設定認證資料庫來自
  - ■ files ◊users 檔(預設)
  - ■ sql ◊mysql or postgresql
  - ■ etc_smbpasswd ◊ samba server
  - ■ ldap ◊LDAP server

✧ 若 Windows XP 使用 PEAP+EAP/MSCHAPv2 進行使用者帳號密碼認證，則認證資料庫中的密碼需以明碼方式記錄。

➢ clients.conf

編輯 clients.conf，加入 radius client IP 相關資料區段如下

例:

AP IP=192.168.0.1

Radius 密語=xxxxxx

➢ eap.conf

編輯 eap.conf

將 default_eap_type = md5 改為 default_eap_type = ttls

➢ 將 tls 段設定啟用（去除#）

```
tls {
        private_key_password = whatever
        private_key_file = ${raddbdir}/certs/cert-srv.pem
        certificate_file = ${raddbdir}/certs/cert-srv.pem
        CA_file = ${raddbdir}/certs/demoCA/cacert.pem
        dh_file = ${raddbdir}/certs/dh
        random_file = ${raddbdir}/certs/random
      }
```

八、實驗步驟與結果

- **攻擊工具**
  - **Airodump Discription:**

    藉由 Airodump 來截取封包的 IV 值,也可以從中獲取 station 和 AP 的資訊。

    Usage－airodump-ng<interface> <output prefix> [channel]
  - **Aireplay Discription**

    主要做兩個動作：

    (1). De-authentication (發出 De-authentication，讓使用者斷線，而將重新與 AP 連線，使我們有機會截取 Four-Way Handshake 的封包。)

    (2). ARP request re-injection (發出 ARP Request 封包以誘使 AP 送出 ARP Reply 封包，藉此大量產生封包以增加攔截 IV 的機會。)

    Usage－aireplay-ng [options] <replay interface>
  - **Aircrack Discription**

    Aircrack 是用來破解 airodump 所收集到的封包，藉此得到 WEP 或 WPA-PSK 的 key。

    Usage－aircrack-ng [options] <capture file(s)>

- **WEP64 之金鑰還原**

步驟

(1) 進入 AP 之硬體設定畫面

- WEP 有兩種的設定：
  - Open System

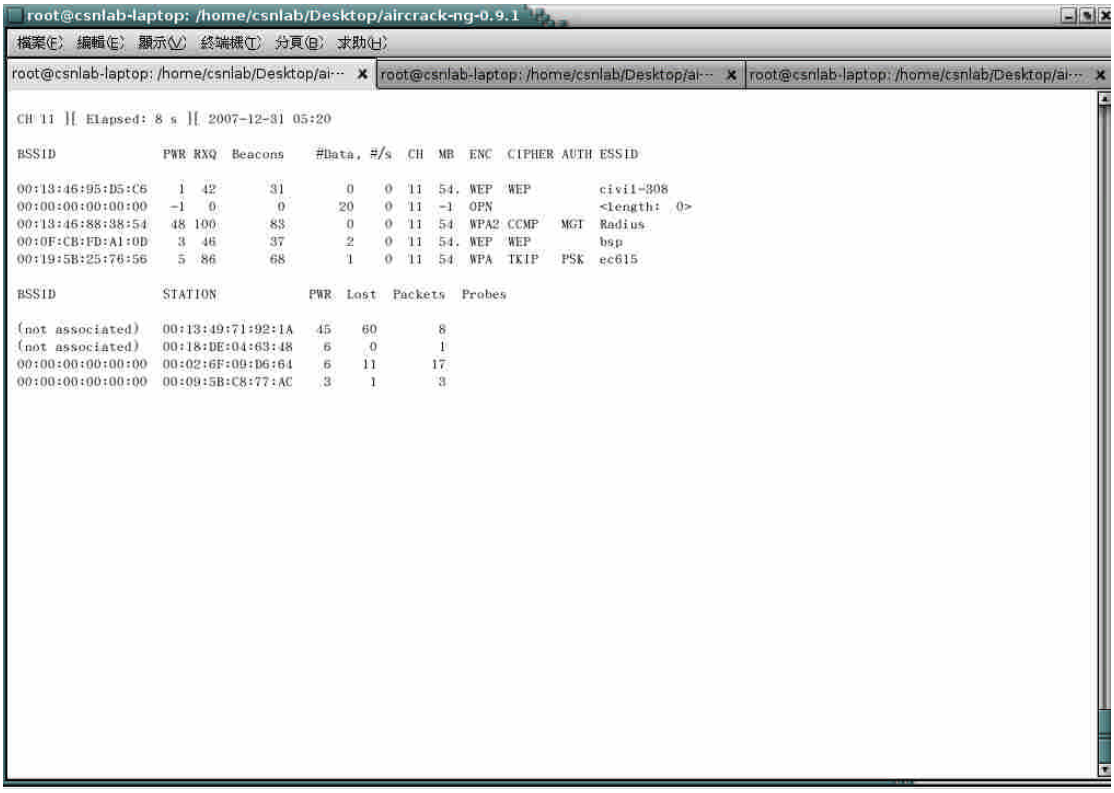
    則只有擁有相同 WEP 金鑰的無線用戶端,可以繼續存在於該無線網路上,但是無線網路基地台 (AP) 則會被在網路上的所有裝置看見。
  - Shared Key

    則無線網路基地台 (AP) 將不會被顯示於無線網路中,但是除了共用同一個 WEP 金鑰的無線用戶端，並且其 MAC 位址也必須要在過濾器清單中出現且被允許存取。

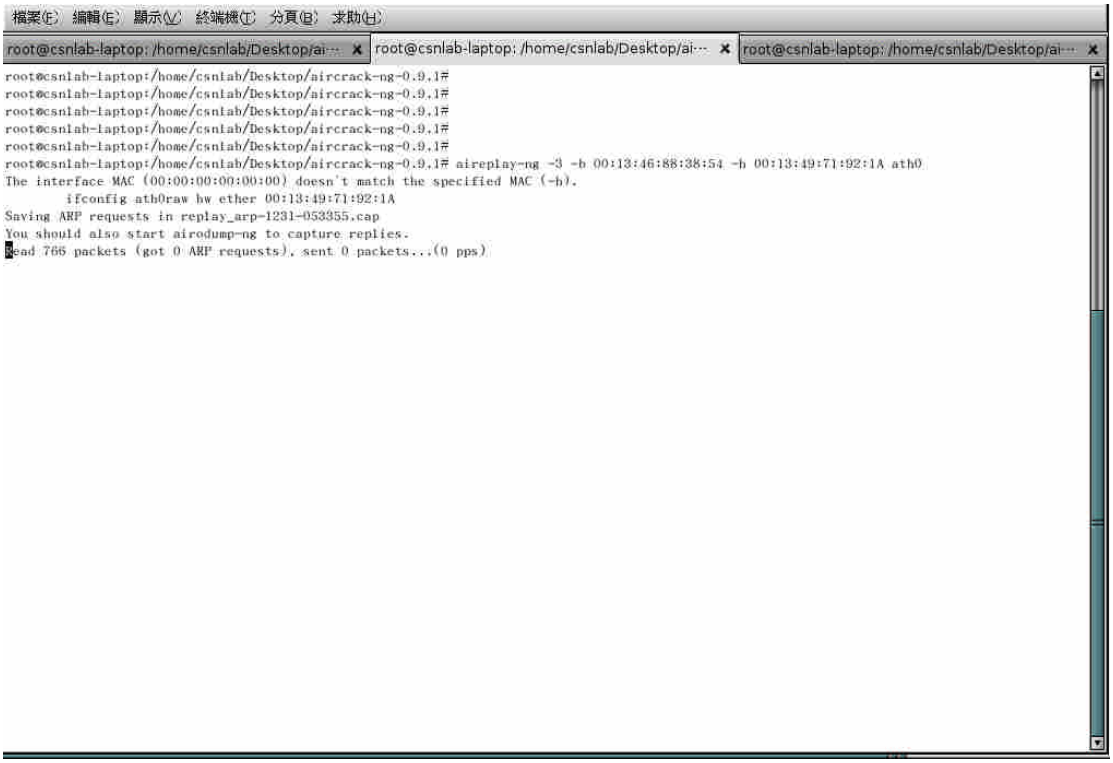

DI-624S
主頁
進階功能
工具
狀態
幫助
設定精靈
無線通訊
廣域網路
區域網路
DHCP伺服器
檔案分享
FTP伺服器
WEB伺服器
無線通訊設定
無線通訊設定讓您可以設定 DI-624S 的無線網路基地台 (AP) 功能。您可以自行變更無線網路通訊設定，以更換現有的無線網路頻道設定或是自訂無線網路組態。透過無線網路加密設定，還可以讓您的無線網路更加安全。
WCN 啟用 停用
無線網路訊號 開啟 關閉
Wireless QoS(WMM) 啟用 停用
SSID : Radius
頻道 : 11 自動選擇頻道
Super G 模式 : 停用
無線網路加密方式 : Open System Shared Key WPA WPA-PSK WPA2 WPA2-PSK
WEP 加密 : 啟用 停用
WEP 加密類型 : 64Bit
WEP 金鑰格式 : HEX
金鑰 1 : 1111111111
金鑰 2 :
金鑰 3 :
金鑰 4 :


Wireless 108G Storage Router
DI-624S
主頁
進階功能
工具
狀態
幫助
設定精靈
無線通訊
廣域網路
區域網路
DHCP伺服器
檔案分享
FTP伺服器
WEB伺服器
無線通訊設定
無線通訊設定讓您可以設定 DI-624S 的無線網路基地台 (AP) 功能。您可以自行變更無線網路通訊設定，以更換現有的無線網路頻道設定或是自訂無線網路組態。透過無線網路加密設定，還可以讓您的無線網路更加安全。
WCN 啟用 停用
無線網路訊號 開啟 關閉
Wireless QoS(WMM) 啟用 停用
SSID : Radius
頻道 : 11 自動選擇頻道
Super G 模式 : 停用
無線網路加密方式 : Open System Shared Key WPA WPA-PSK WPA2 WPA2-PSK
WEP 加密 : 啟用 停用
WEP 加密類型 : 64Bit
WEP 金鑰格式 : HEX
金鑰 1 : 1111111111
金鑰 2 :
金鑰 3 :
金鑰 4 :

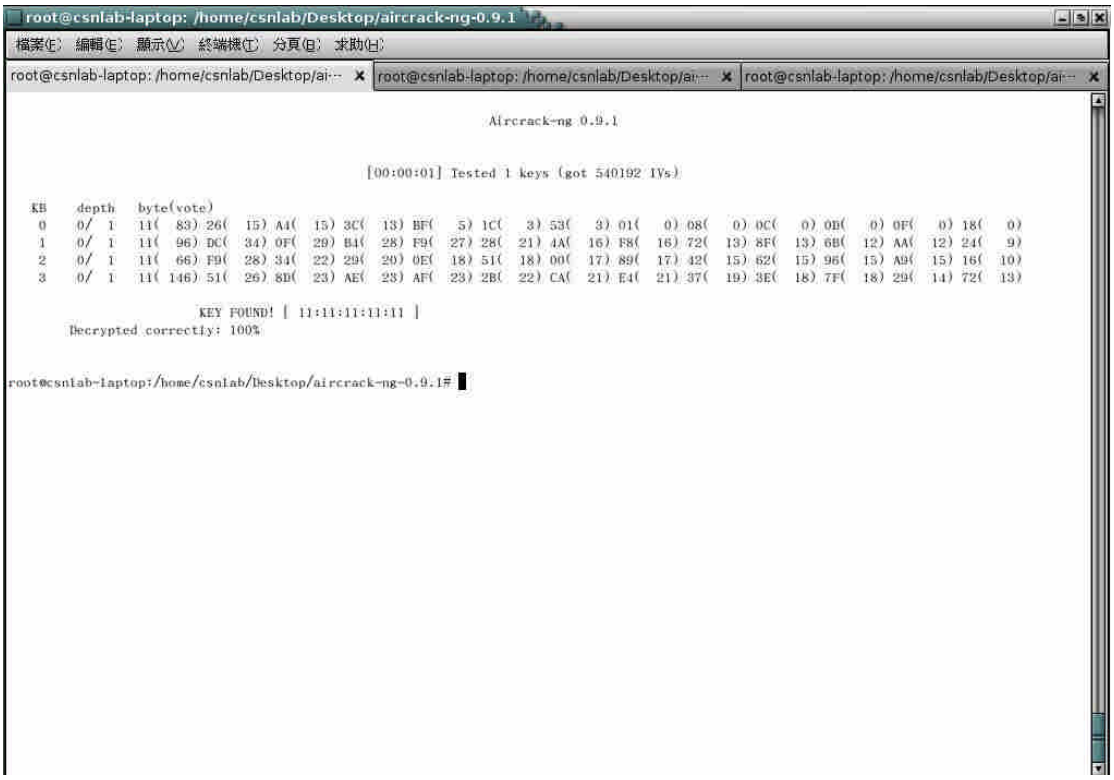
(2) 啟動 airodump 收封包；



(3) 用 aireplay 注入封包，增加 IV 值；



(4) 用 aircrack 破 WEP。



- **實驗結果**

  - **WEP64 的還原金鑰攻擊統計**

名稱	IV 數量	時間
WEP64-01.cap	201354	3 分 11 秒
WEP64-02.cap	180147	3 分 05 秒
WEP64-03.cap	172584	2 分 50 秒

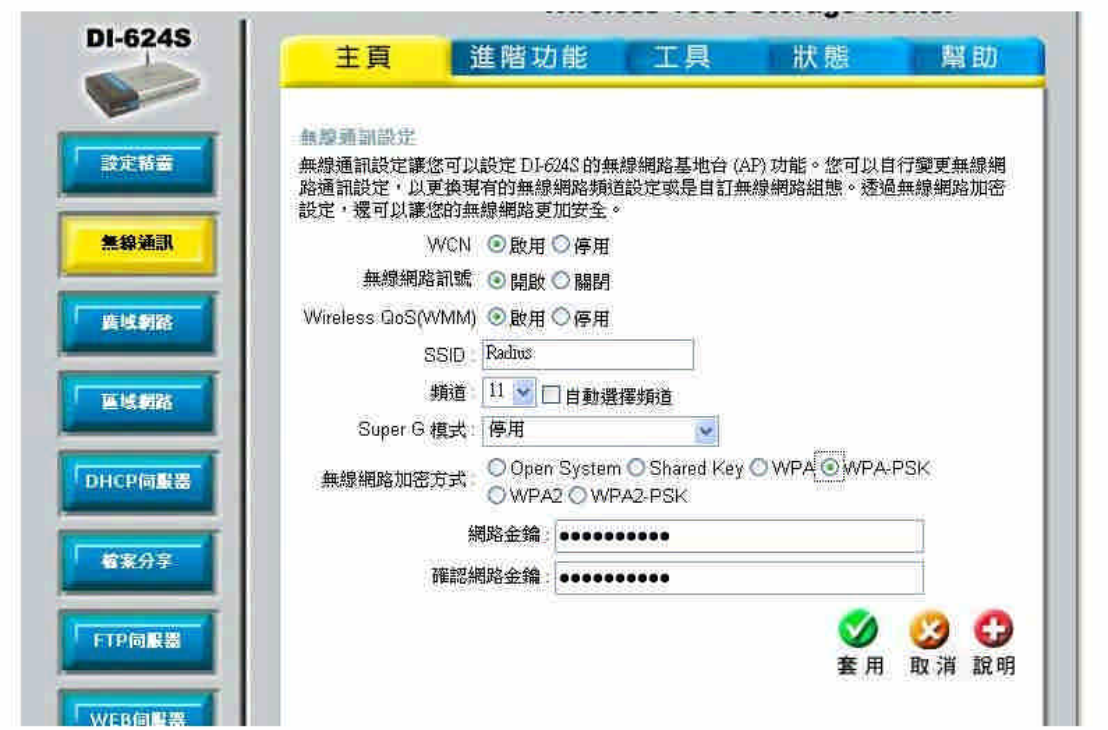
  - **WEP128 的還原金鑰攻擊統計**

名稱	IV 數量	時間
WEP128-01.cap	399279	4 分 24 秒
WEP128-02.cap	529800	5 分 12 秒
WEP128-03.cap	1457862	14 分 47 秒

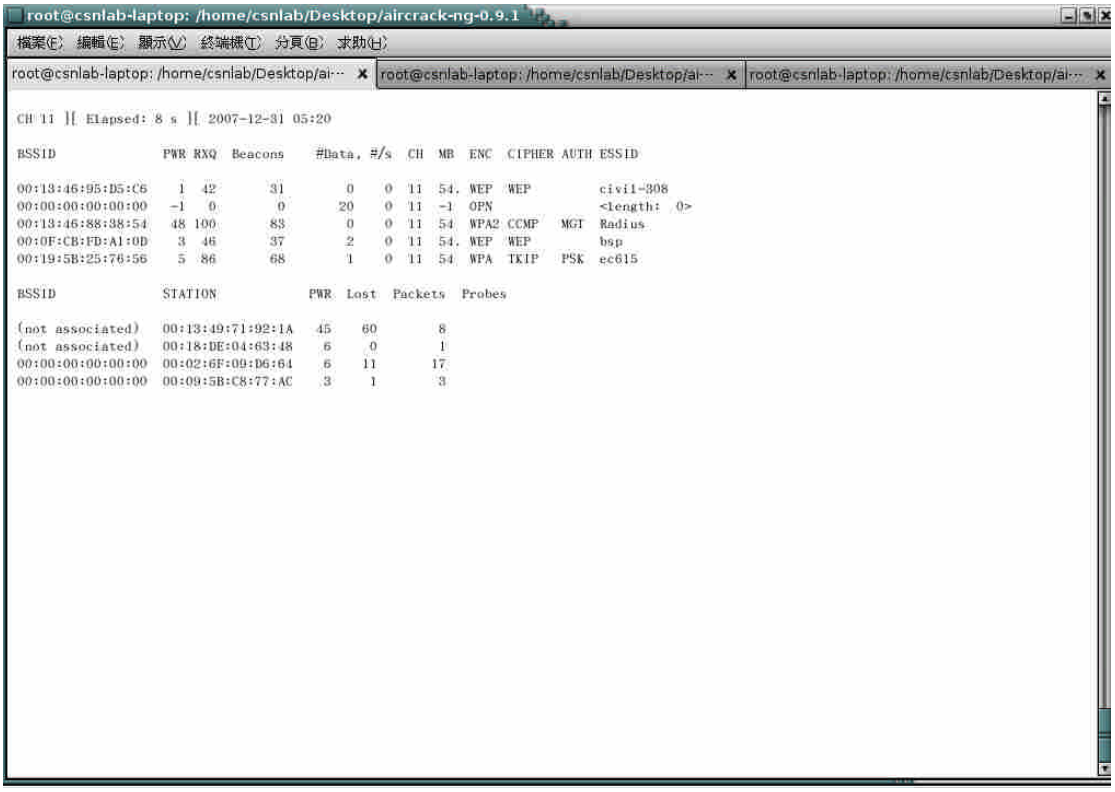
➢ **WPA-PSK 之金鑰還原**

步驟

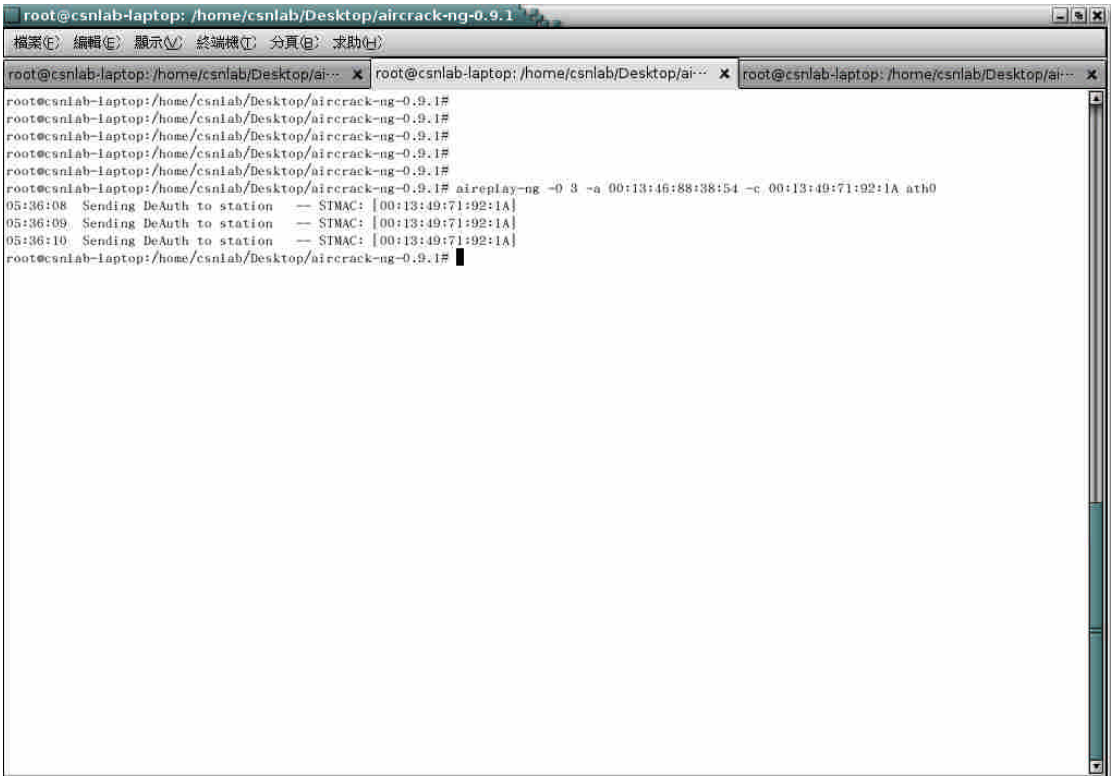
(1).進入 AP 的硬體設定畫面，設定為 WPA_PSK；



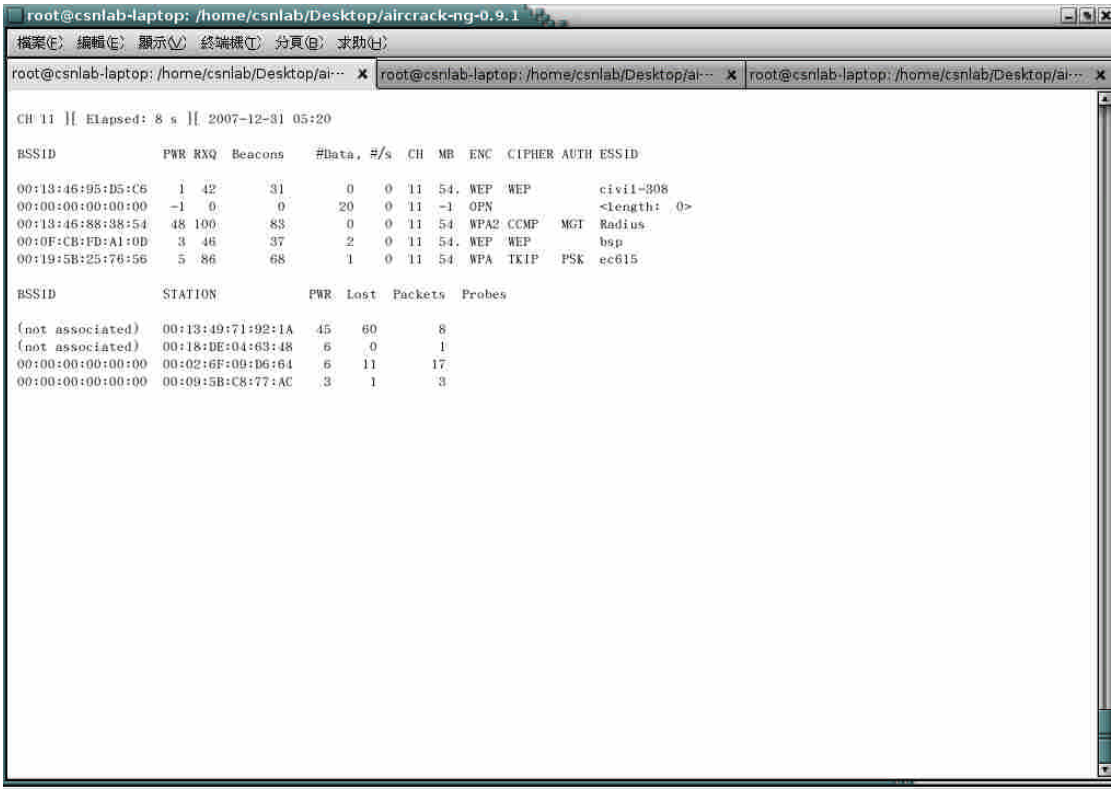
(2).用 airodump 來偵測 AP 的 MAC 及 Channel 並且抓 handshake packet；



(3).用 aireplay 注入 de-authentication 的 packet；



(4).用 aircrack 破 WPA-PSK。



➢ **WPA2 之金鑰還原**

步驟

同 WPA

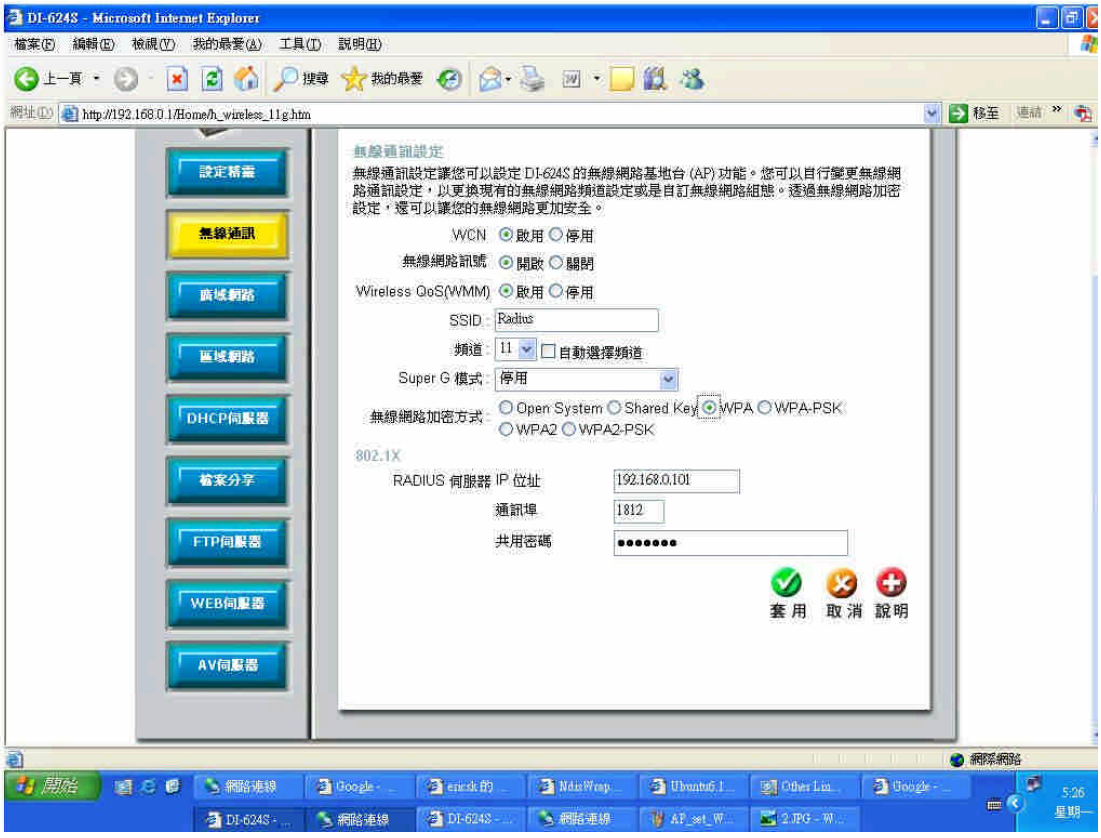
➢ 實驗結果

✧ **WPA/WPA2 的還原金鑰攻擊統計**

名稱	時間
WPA1_PAK-01.cap	**5 分 10 秒**
WPA1_PAK-02.cap	**10 分 29 秒**
WPA2_PAK-01.cap	**5 分 13 秒**
WPA2_PAK-02.cap	**10 分 18 秒**

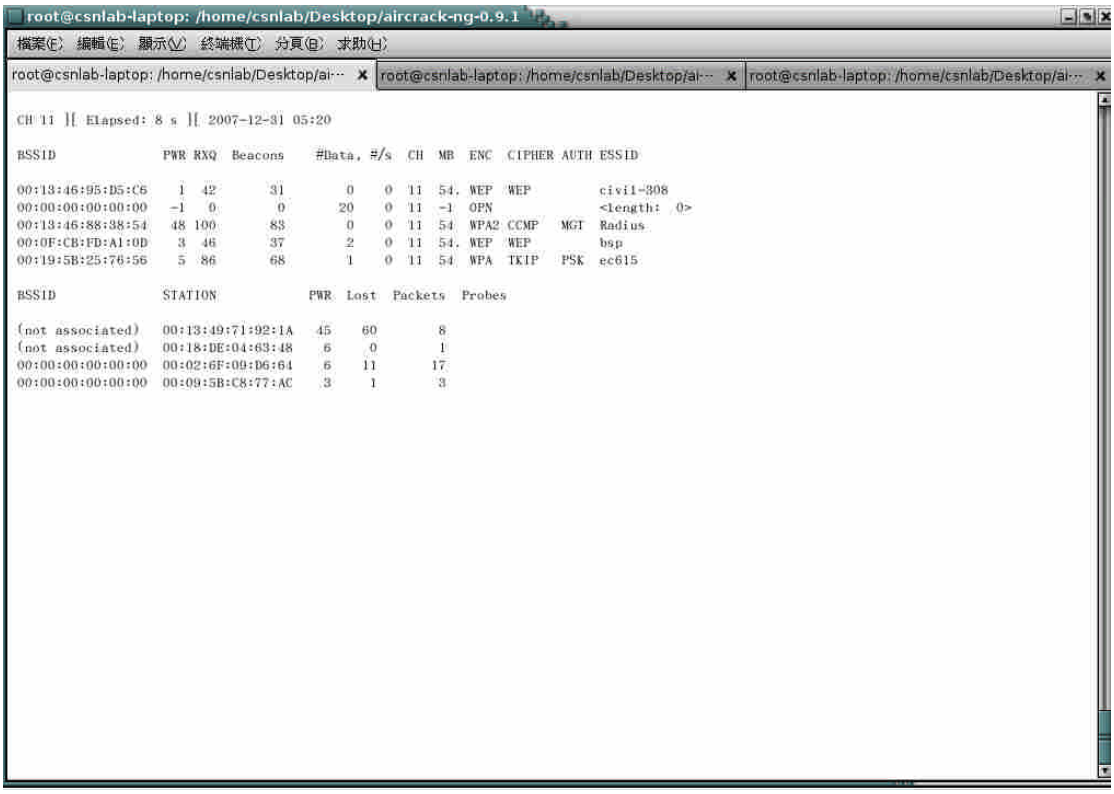
➢ 對設有後端 Radius Server 的 WPA 和 WPA2 做斷線攻擊

(1).進入 AP 硬體設定畫面

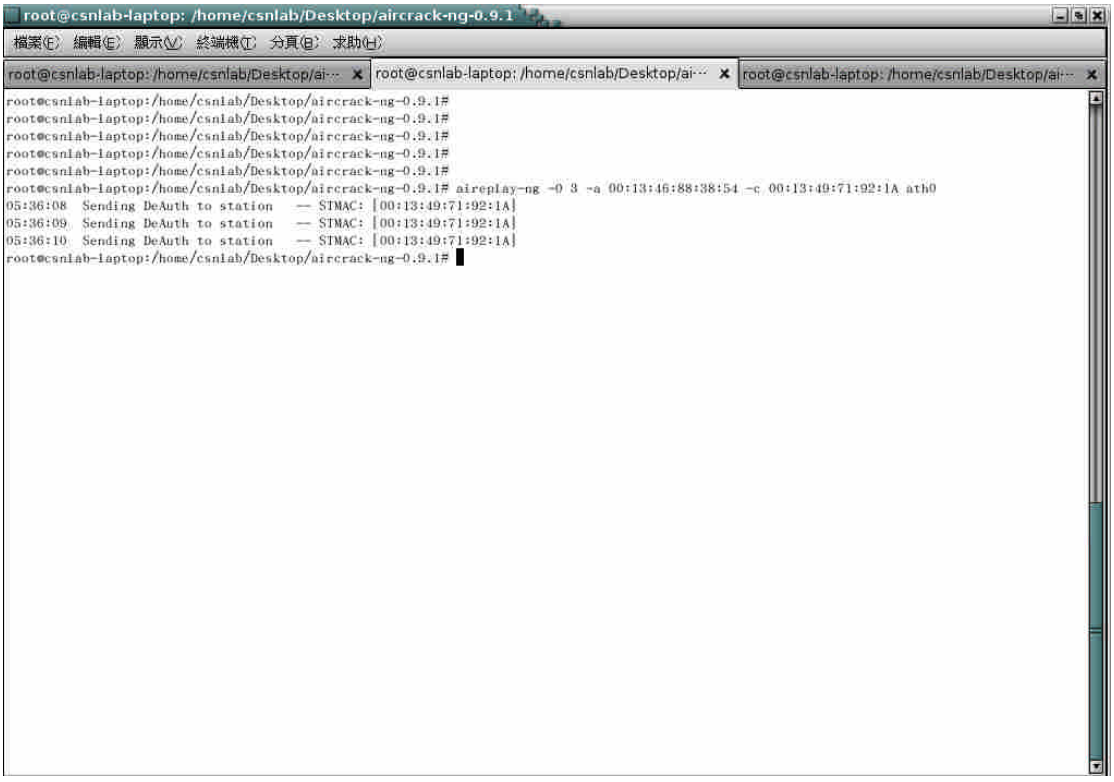


從這裡可以看到他還要在設定 Radius 的一些資訊。

(2).利用 airodump-ng 收集 AP 和 Station 的資訊



(3).利用 aireplay-ng 進行斷線



➢ 實驗結果

持續的對對方發送斷線封包，造成對方斷線。

九、結論

透過前人的一些研究發現，無線網路鏈路層的加密協定存在的許多缺失及弱點。本篇論文首先用理論的方法探討金鑰的還原，接下來再透過實作徹底完成金鑰還原的結果，最後對這些被還原的金鑰做分析，探究這些金鑰為什麼如此容易還原，並且提出一個安全的金鑰範例做參考。完成鏈路層安全問題研究，了解這些缺失所造成人們對於無線網路安全性的疑慮與不安，以期望之後的加密協定之設計能以此為鑒，進而設計出更具安全性之加密協定。

在 WEP 加密系統底下，要還原金鑰，主要是要藉由收集封包來做統計攻擊，以現在的技術和硬體效能而言，只要封包足夠，就可立即將金鑰還原。所以 WEP 主要影響 WEP 破解速度的關鍵在於封包收集的速度，只要封包收及夠快，十分鐘左右就可以把 WEP 的金鑰還原。以現有的資源來做收集封包，可以每分鐘最多抓五萬到六萬的封包數量，通常破解 WEP64 約需二十萬左右的封包。在 WEP128 約需六十萬左右的封包，有機率問題存在，所以實際情況不一定。不過可以確定的是，在使用 WEP 的加密協定下，必定是不安全的。

在 WPA-PSK 加密系統下，有分 TKIP 和 CCMP 兩種不同的加密協定，一種是使用 RC4，另一種是使用 AES 做加密。這兩種加密協定是為了改善無線網路的安全性而推行的，所以改善的非常多 WEP 所衍生出的種種問題。因此在這個環境下加密是非常安全的。不過 WPA1 和 WPA2 都有一個共同的問題，就是在做 4-way handshake 的時候，容易被攻擊者抓到認證封包而在離線下做暴力法攻擊。或是攻擊者可以主動作斷線攻擊，迫使工作站斷線，讓她重新發送認證封包，使得攻擊者有機可乘。因此在這個環境下，如果要有安全的網路環境，Pre-shared key 的密碼強度要夠強，因為只要密碼夠複雜就算對方使用暴力法攻擊，也是無法在有效率的時間內還原密碼。

若是想要讓自己的無線網路更安全，可以使用有支援後端 Radius Server 認證

的無線網路系統，雙方的 Session Key 必須要先經過身份的認證才能產生，因此不同的客戶端，在不同時間點下所產生的 Session Key 都不一樣。所以既使攻擊方成功破解雙方的 Session Key，在下次連線的時候還是無效的。

而在支援身份認證的網路系統下，若是要嘗試作金鑰還原攻擊，可能是不具效果的。不過從金鑰還原的經驗中得知，斷線攻擊和仿冒封包攻擊的威脅還是存在。在實作斷線攻擊時，雖然對方會重新嘗試連線，但是攻擊端可以不斷發送假封包做斷線，雖然不會有資訊外洩或網路資源被盜用的疑慮，不過被斷線的麻煩還是不堪其擾。

十、參考文獻

[1] 3GPP Technical Specification 3GPP TS 33.105 V3.5.0: "Technical Specification Group Services and System Aspects; 3G Security; Cryptographic Algorithm Requirements (Release 1999)," 3rd Generation Partnership Project, October 2000.

[2] Arbaugh, W., Shankar, N., and Wan, J., "Your 802.11 Wireless Network has No Clothes," Department of Computer Science University of Maryland College Park, Maryland, March, 2001.

[3] Borisov *et. al*, "Intercepting Mobile Communications: The Insecurity of 802.11," Jan 2001.

[4] Blake-Wilson, S, Hopwood, D., Mikkelson, J., Nystrom, M., and T. Wright, "TLS Extensions," TLS Working Group Internet-Draft, draft-ietf-tls-extensions-00.txt, June 2001.

[5] Fluher, S., Mantin, I., and Shamir, A., "Weaknesses in the Key Scheduling Algorithm of RC4," http://downloads.securityfocus.com/library/rc4_ksaproc.pdf

[6] IEEE, "IEEE 802.1X-2001 (ISO/IEC 802-1x: 2001), Part 11: Wireless LAN Medium Access Local and metropolitan area networks: Port-Based Network Access Control," URL:http://www.ieee802.org/1/pages/802.1X.html

[7] IEEE Std 802.11-1997, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.

[8] Myers, M., Ankney, R., Malpani, A., Galperin, S., and C. Adams, "Internet X.509 Public Key Infrastructure: Online Certificate Status Protocol – OCSP," RFC 2560, June 1999.

[9] Karagiannis, Konstantino, Ten Steps to a Secure Wireless Network, Feb. 25, 2003, http://www.pcmag.com/article2/0,4149,844020,00

[10] Wi-Fi Alliance, http://www.weca.net/OpenSection/index.asp?noFlash=true