Computer Network Encryption with WPA in IEEE 802.11i Environment

謝景棠
淡江大學電機研究所
E-mail: hsieh@ee.tku.edu.tw

蔡文章
淡江大學電機研究所
E-mail: kevin.tsai@gigabyte.com.tw

摘要

無線區域網路（WLAN）產品代名詞的 Wi-Fi，其實源自於 Wi-Fi 聯盟，它是全球非營利產業組織中，最成功的範例之一。WPA 是 IEEE 802.11i 標準的前身，可解決目前已知的各種入侵攻擊，提昇 WLAN 產品的安全性，在以往的 WLAN 都是採用 Wired Equivalent Privacy (WEP)作加密，但這種加密的方式，對於一般的駭客是無法防範，也就是說只要選擇適當的設備或工具，便可以搜集到資料加以分析，而取得加密的 Key。Wi-Fi Protected Access (WPA) 的 Temporal Key Integrity Protocol (TKIP)是 WEP 的增強版的技術，使用了混合函數(Mixing Function)來混合 Temporal Key 和 TSC 來改成 WEP Seed，進而增加其強健性。本篇論文是在 IEEE 802.11i 的環境下，利用 WPA 作加密的動作，經測試與比較證實其有效性。

關鍵詞：WLAN, WPA, WEP, Encryption

一、簡介

近幾年來，可攜式的電腦(例如 Intel Centrino notebook) 的快速成長，無線區域網路對今日的電腦及通訊工業來講，將成為一項重要的觀念及技術。在無線區域網路的架構中，電腦主機不需要像在傳統的有線網路裡，必須保持固定在網路架構中的某個節點上，而是可以在任意的時間作任何的移動，也能對網路上的資料作任意的擷取。

無線區域網路正逐漸受到重視，為了使各種競爭產品之間能相容互通，標準的制定就成了重要的工作，而 IEEE 802.11[1] 無線區域網路的標準就在這樣的情況下誕生。無線網路的軟體架構可由下列二大類所組成:

1. 工作站服務 (Station Services, 簡稱 SS) ，包含：身份確認服務(Authentication)與隱密性服務(Privacy)。

身份確認服務(Authentication)：此服務的主要目的是用來確認每一個工作站的身份。IEEE 802.11 支援一種叫做(盤問/回應)(Challenge/Response，簡稱 C/R) 的身份確認方法。

隱密性服務 (Privacy)[2] ：此服務的主要目的是避免傳送資料的內容被竊聽，而主要功能就是提供一套「隱密性服務」的演算法 (privacy algorithm) 將資料做加密與解密，WPA 則屬於此部份。在 WLAN 認證的目的是確認對方身分的合法性，以避免與身分不明的對象溝通，而將重要的資料洩漏出去。也就是在雙方進行通訊溝通之前，必須先經過認證的程序要求。而 IEEE 802.11 提供了兩種隱密性服務的認證服務：

a. 開放系統式 (Open System)，此方式都可通過認證，不須認證演算法的認證。

b.金鑰共享式 (Shared Key)，需要有一組 64bit 或 128bit 的 Key 才能連上工作站，為了避免密匙曝光，我們需要利用 WEP[2]加密演算法。認證步驟(1).要求認證者送出認證訊框 (Authentication frame) 要求對方認證(2).被要求認證者先檢查雙方認證方法是否相同 (3)要求加密認證的 Key (4).認證成功與否。

2. 分散式系統服務(Distribution System Services，簡稱 DSS)，由分散式系統所提供。此部份則是提供資料的分送，甚至是資料的優先權(priority)[6]等等。

在 IEEE 802.11i[1]當中，身份確認服務的有 EAP(定義在 RFC2284)[5]，802.1X 以及 RADIUS(定義在 RFC2138，RFC2548)[5] ..等;

而 WPA[1]則屬隱密性服務，WPA 是為了改進 WEP 的加密性不足。 例如: WPA 利用來源、目的位址，優先權和資料再透過一特定的演算法求出，並將它附在資料的後端，再將整個處理後的資料作加密。其目的主要是用來作資料正確性的驗算，增加其加密性;另外配合 TKIP[1]的技術，大大的改進了 WEP 的加密性不足。本篇論文是在 IEEE 802.11i 的環境下，利用 WPA 作加密的動作，其第二節敘述 WEP 的原理，而第三節介紹 IEEE802.11i 的環境下，設計 WPA，第四節則為 WEP 與 WPA 的測試與比較，最後為本篇論文的結論與未來展望。

二、WEP 原理

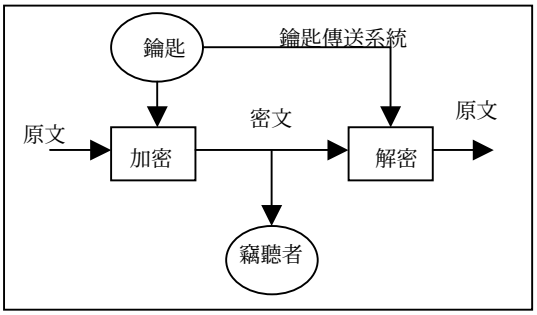
密碼演算法 (Cryptographic algorithm，或稱為 Cipher) 就是一種用來對資料進行加密及解密的數學函式。近代密碼演算法大都採用鑰匙 (key，在此簡稱 k) 的技術來進行加密及解密的工作。加密函式 (Encryption function，簡稱 E) 處理原文。而所謂加密 (Encryption)，其實就是將原始二進位資料經過處理後，將其資訊內容隱藏起來。沒有經過加密處理的資料稱為原文 (Plaintext, 簡稱 P)，而經過加密處理的資料則稱為密文 (Ciphertext，簡稱 C)。將密文還原成原文的過程稱為解密 (Decryption，簡稱 D) 。

P 後得到密文 C :

$$E_k(P) = C \qquad (1)$$

欲還原時，解密函式 利用相同的鑰匙處理密文 C 後得到原文 P :

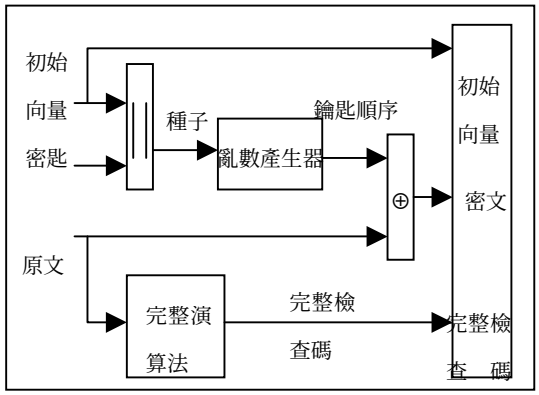
$$D_k (C) = D_k (E_k(P)) = P \qquad (2)$$



圖一．原文加密及解密基本過程

WEP 演算法是一種對稱性的演算法，就是加密與解密都用相同的鑰匙。我們假設鑰匙可經由另外的鑰匙管理服務將之傳給其他有關的工作站。WEP 演算法的主要技術在於將一段原文區塊 (Plaintext block) 與一個等長的隨機鑰匙 (random key sequence) 做 bit 與 bit 間的互斥運算 (XOR operation)。而此隨機鑰匙則是由 WEP 演算法所產生。如圖二 所示，加密的過程由一個重要的密匙 (secret key) 開始。密匙後面串接一個初始向量 (Initialization Vector, IV) 之後成為一個種子 (seed)，此種子則是亂數產生器 (pseudo random number generator, PRNG) 的一個輸入參數。亂數產生器則輸出一個具隨機性質的鑰匙順序 (key sequence, k), 其長度等於 MSDU(MAC Service Data Unit) 的可能最大長度。

原文必須經過兩種處理程序:a.為了保護原文未經授權被修改，原文先經過一個完整演算法 (Integrity algorithm) 的處理得到一個完整檢查碼 (Integrity Check Value, ICV)，b.原文和鑰匙順序進行互斥的運算得到密文。而結果所輸出的訊息 (message) 則包含三部分：1.密文，2.初始向量 (IV)，3.完整檢查碼 (ICV)。



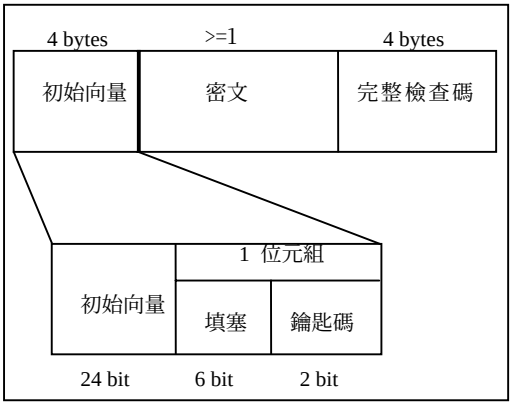
圖二. WEP 演算法加密過程

WEP 亂數產生器可以簡化鑰匙傳遞的負擔，因為欲進行通訊之工作站間只要傳遞密匙即可，而在整個過程中可說是最關鍵的零組件。它負責將相對較短的密匙轉換成任意長的鑰匙順序。這樣做。在通訊進行期間，由於初始向量 (IV) 可以週期性的變換而密匙則可保持不變，因此初始向量具有延長密匙有效期的功用並且提供此演算法自我同步的重要特性，且與鑰匙順序 (k) 間具有一對一的關係。每一個新的初始向量都可以得到一個新的種

子及鑰匙順序。為了避免竊聽者有足夠的時間或資訊破解密文，初始向量可以經常變換，甚至每一個 MPDU 都使用不同的初始向量。

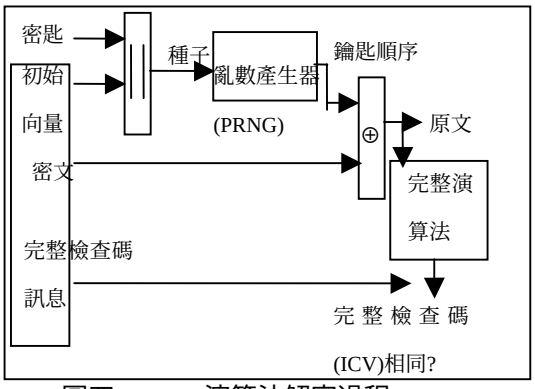
初始向量: 1.和訊息是一起傳送的，接收端工作站可以很容易的用來解密。並不會因為初始向量經常變換而造成困擾。 2.並無提供任何與密匙有關的資訊，因此在傳送上不必加密。所以竊聽者可以清楚看到初始向量，但是無法用它來猜出密匙。

輸入亂數產生器(PRNG)的種子長度為 64 bit 或 128 bit，其組成方式是將密匙當成是最左邊的 40 bit (128 bit 則為 104 bit)，而將初始向量(IV)當成是最右邊的 24 bit。WEP 演算法處理的資料單位是一個 MPDU (MAC Protocol Data Unit)，輸出則依序是: 1.IV, 2. MPDU, 3. ICV。其中 IV 與 ICV 的長度都是 4 個位元組。如圖三 所示，初始欄位雖然佔 4 個位元組，初始向量事實上只有 3 個位元組。另外一個位元組則包含一個填塞 (PAD，6 位元) 及鑰匙碼 (Key ID, 2 位元)。其中鑰匙碼是用來通知接收端在解密時應該使用四個可能的密匙中的哪一個。至於完整檢查演算法是最常用的 CRC-32 演算法。



圖三.經 WEP 處理過的 MPDU 架構

至於 WEP 演算法的解密過程則與加密的過程相反。如圖四所示，當工作站收到一筆訊框時，其上的初始向量(IV) 先與事先取得的密匙合併成為亂數產生器(PRNG)的種子(Seed)，經由亂數產生器的處理後得到鑰匙順序。此順序與密文進行 XOR 的運算後便得到原文。為了進一步檢查資料在傳送的過程中是否被修改過，此原文(Plaintext)還必須經過完整檢查演算法的處理，所得到的完整檢查碼則與訊框上的完整檢查碼比較。如果不同則表示資料被竄改過。此時除了通知 MAC 管理軟體外，並不將錯誤的訊框傳給上層軟體。



圖四. WEP 演算法解密過程

三、WPA 的設計

Wi-Fi Protected Access (WPA) 目前的規範為 IEEE802.11i drift 的版本，而由於 WEP 的設計上某些缺失，無法抵抗駭客的攻擊，更無法有效防堵網路工具(例如: Sniffer Pro tool)或設備的擷取資料，因為許多的軟體可以設成 Monitor mode (監聽模式)。

也因如此，Wi-Fi 聯盟對於強化 WEP 加密而推出 WPA，WPA 為一個 128-bit 的 AES 加密演算法，其主要為: 1. 一個強健且隱藏性取代 WEP 演算法。2. 產品經 Wi-Fi 認證，可以得到產品的保證。3. 可以有效的應用在家庭與大的公司企業[3]。

4-Way HandShake

WPA 定義了 Pre Shared Key (PSK)[1]的機制，也就是您可在 AP 與 Station 端利用手打的方式，手動設定一組 PSK，WPA 會利用此一 PSK 再透過 4-Way HandShake 產生一組加密用的 Key，在產生 Key 的過程是分別在 AP 與 Station 端利用演算法算出，因此不會擔心 Key 值會外流。以下是 4-Way HandShake 的字串說明，用來表示一個 EAPOL-Key messages：EAPOL-Key(S, M, A, T, N, K, KeyRSC, ANonce/SNonce/GNonce, MIC, GTK)。

說明:

S: 最初的 4-Way HandShake Key 是否完成。

M: 除了 4-Way HandShake 的第一個 message 外，都得設 1，用來指明傳送的 Key data 是否作 MIC(Message Integrity Code)。

A: 回應的請求訊息，這是 EAPOL-Key 訊息

的 Act bit。

T: Tx/Rx 給 Group Key 及 Pairwise Key 的訊息

N: Key 的 Index，EAPOL-Key 訊息作 Index bit

K: Key 的 Type –P (Pairwise) 或 G(Group)

KeyRSC : Key Receive Sequence Counter

ANonce/SNonce,/Gnonce : Authenticator/ Supplicant/Group Nonce

MIC : Message Integrity Code

GTK : Group Temporal Key

EAPOL-Key messages：

Message 1. Authenticator -> Supplicant：EAPOL-Key(0,0,1,0,0,P,0,ANonce,0,0)

Message 2. Supplicant -> Authenticator：EAPOL-Key(0,1,0,0,0,P,0,SNonce,MIC,IE)

Message 3. Authenticator -> Supplicant：EAPOL-Key(0,1,1,1,0,P,IV,ANonce,MIC,IE)

Message 4. Supplicant -> Authenticator：EAPOL-Key(0,1,0,0,0,P,0,0,MIC,0)

ANonce：Authenticator 產生的 Nonce，Message 1 和 3 中 ANonce 相同。

SNonce：Supplicant 產生的 Nonce ，P：指的是 Key Type 為 pairwise ，MIC：指的是需將整個 message 做一次 MIC 驗算，並將驗算的結果填入 Key MIC 欄位中，IE：指的是 Beacon 所帶的 WPA IE。

整個 **4-Way HandShake** 的流程包含如下：

1. Authenticator 產生 ANonce 並以 message1 的格式傳給 Supplicant 端 。

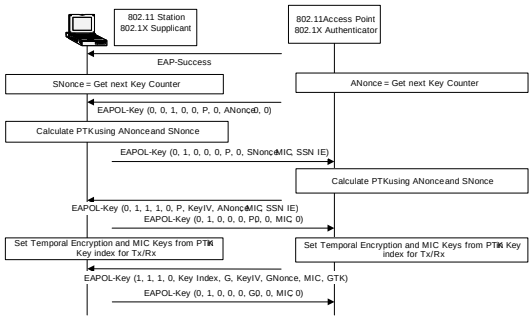
2. Supplicant 收到 ANonce 後再與自己產生的 SNonce 來算出 PTK。

3. Supplicant 將自己產生的 SNonce 與 IE 以 message2 的格式傳給 Authenticator 端

4. Authenticator 收到 SNonce 後再與自己產生的 ANonce 來算出 PTK，並驗證 MIC 是否正確。

5. Authenticator 送出 message3。

6. Supplicant 收到 message3 後就可以開始做 TKIP 的加密。並回傳 message4。



圖五. WPA 4-Way HandShake 的流程

Temporal Key Integrity Protocol (TKIP)可說是 WEP 的增強版，它基本上還是使用 WEP 來作資料加解密，只是它改進了 WEP 的幾個缺失:

1. AP 或 STA 端要傳送資料時會先算出 MIC (Message Integrity Code) ，這是利用來源、目的位址，優先權和資料再透過一特定的演算法求出，並將它和附在資料的後端，再將整個處理後的資料作加密。其目的主要是用來作資料正確性的驗算，當彼端在收到來源端送過來資料時，也會利用相同的演算法和資訊算出 MIC，再比對兩端的 MIC 是否相同，若相同則繼續往下處理，若不同則將封包丟棄。

2. TKIP 使用 TSC(TKIP sequence counter)，來對它送出的資料編排順序，彼端將不在目前順序上的封包丟棄。

3. TKIP 使用混合函數(Mixing Function)來混合 Temporal Key 和 TSC 來改成 WEP Seed，其中包含 WEP IV，再丟入 WEP 演算法中，接收端在收到資料後也會利用相同的混合函數求出 WEP Seed，再利用 WEP 解出所要的資料。

WPA 的 TKIP 編碼與解碼

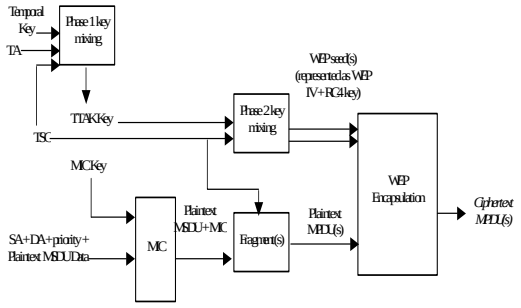
TKIP 利用幾個額外的 Function 來加強 WEP 的編碼動作，如圖六:

1. TKIP 利用 SA(Source Address) + DA (Destination Address) + Priority + Data 透過 MIC 演算法求出 MIC，並附在 MSDU 之後。

2. TKIP 將欲送出的 MSDU，分解成一個或多個 MPDU(s)，並對每個 MPDU 加上一個 TSC。

3. 再針對每個 MPDU 利用 Key Mixing Function 來求出 WEP Seed。

4. WEP Seed 中包含 WEP IV 和 Web Key，再將 WEP Seed 丟入 WEP 演算法來將 MPDU 加密，此 1~4 步驟即為 TKIP 加密的動作。



圖六. TKIP 加密 Block Diagram

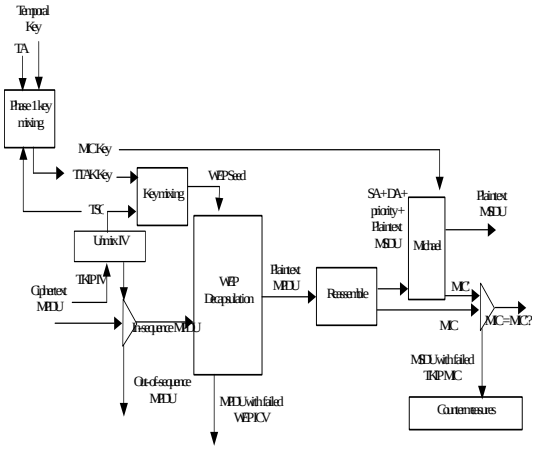
TKIP 利用幾個額外的 Function 來加強 WEP 的解碼動作，如圖七:

1. 在作 WEP 解密之前，TKIP 會先求出 TSC，並丟棄不在順序中的封包，之後再利用 TSC 和 Key Mixing Function 來建立 WEP Seed。

2. TKIP 將 WEP Seed 和 MPDU 丟入 WEP 解密。

3. 若 WEP 檢查 ICV 正確，則將每個收到的 MPDU 組成一個 MSDU，並取出 MSDU 中彼此端帶過來的 MIC，再將其與自己求出的 MIC 作比較，若不同則丟棄這封包。

4. 若比對成功，則將封包往上層傳送。



圖七. TKIP 解密 Block Diagram

四、測試與比較

在傳統的 802.11 資料加密過程是利用一長度 40bit 或 104bit 的 Web Key 再串上一個 24 bit 長度的初始向量(IV)，再進行 RC4 的運算取得一個加密金鑰。利用此一加密金鑰與封包進行 XOR 的加密運算，並將 24 bit 的 IV 附於加密後的資料中送出，傳統的加密方法有幾個問題：

1. 24 bit 長度的 IV 造成加密的密鑰會有重覆利用的機會，當密鑰重覆時，一定程度的攻擊者就有可能加以利用並破解加密的保護。

2. 加密用的 Web Key 太短，40 bit 的長度已經不敷使用，104 bit 長度的 Web Key 該是最低需求，長度越長攻擊者就越不容易破解。

3. 缺乏適當的 Web Key 管理機制，一般使用者對於 Web Key 的管理總沒有適當的方法，因而造成一再的被使用而沒有改變，若是沒有一個定期自動換 Key 的機制，則 Web Key 可能會是整個無線網路中最脆弱的地方。

WPA 改善了上述的缺點，WPA 利用 802.1x 與 Temporal Key Integrity Protocol (TKIP)來補強傳統 802.11 的缺失:

1. 為了改善 Web Key 管理的機制，WPA 利用 802.1x 的功能再搭配 Radius 伺服器做使用者驗證管理，可以達到自動換 key 的機制，因此可以利用 Radius 伺服器，使用者就不需擔心 Web Key 有一再被使用的問題。或許您會有個疑問，若是在您的網路環境中沒有 Radius 伺服器該如何解決，WPA 定義了 Pre Shared Key (PSK)的機制，也就是您可在 AP 與 Station 端利用手打的方式，手動設定一組 PSK，WPA 會利用此一 PSK 再透過 4-Way HandShake 產生一組加密用的 Key，在產生 Key 的過程是分別在 AP 與 Station 端利用演算法算出，因此不會擔心 Key 值會外流，而產生的 Key 值長度為 128 bit，也可解決 Web Key 長度的問題。

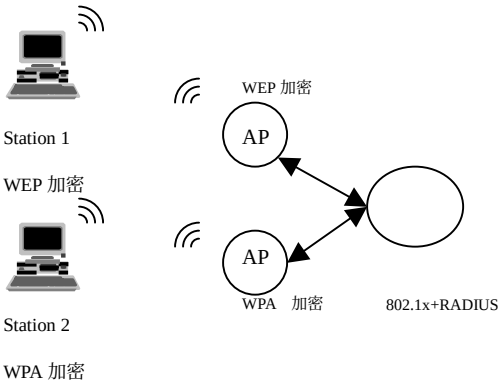
2. 傳統的 Web 加密機制有其演算法上的缺失，因此攻擊者很容易就可破解其加密演算法並取得資料，WPA 為了改善此限象定義了 TKIP。

WEP 加密與 WPA 加密測試

本論文的測試，是使用無線網卡，作業系統為 Windows XP 來作測試。在圖八中為 WEP 及 WPA 的測試環境圖，Station 1 無線網卡為任一家無線網卡皆可，啟用 WEP 加密 64 bit，Station 2 為本實驗的 WPA 無線網卡；而 AP1 為 WEP 基地台+802.1X，AP2 為 WPA 基地台+802.1X，再連結至 RADIUS Server[4]作認證。

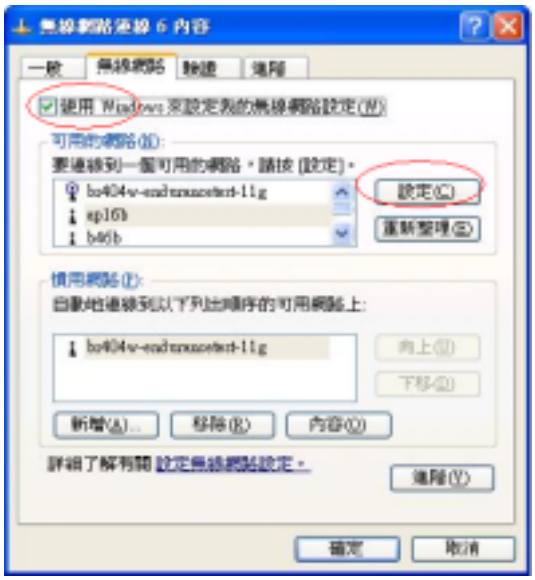
而圖九為 WEP 加密的顯示，WEP 的地方顯示“Yes”，為使用 WEP Key 的方式。而其可以使用 Windows XP，配合 802.1X 便可自動輕易的取得 WEP 的 Key，如圖十顯示，我們可勾選“使用 windows 來設定我的無線網路設定”，然後按 “設定”，便出現圖十一畫面，最後勾選 “資料加密(啟用 WEP)”， “金鑰自動地提供給我”， 便可自動輕易的取得 WEP 的 Key。

WPA 加密+PSK 用 Windows XP 方式配合 TKIP 加密方式：如圖十二，網路驗證選“WPA-PSK”，資料加密 “TKIP”、 圖十三，使用 TKIP Key 的方式，則可使加密的 Key 不會被破解，可增加加密的強健性。



圖八.WPA 及 WEP 的測試環境圖

圖九.WEP 加密+802.1x 使用 XP 的方式



圖十.選擇由 Windows 來自動設定

圖十一.Windows 可設定自動取得 WEP 的 Key

圖十二.WPA 加密+PSK 用 Windows XP 方式

圖十三.WPA 使用 TKIP 加密方式

一般網路駭客對於 WEP 的破解，大致上皆以亂數產生器所產生的亂數有瑕疵，來作攻擊，因為根據研究顯示，視無線網路的通訊量大小，IV 可能在幾分鐘或數天內產生重複使用的現象，而攻擊者只要使用無線網卡監聽模式，將所有可能的 IV 以及相對應的 Key 建立一個表，只要發現相同的 IV，攻擊者即能馬上找出相對應的 Key，所以 WEP 的 40 bit 長度，則可能被駭客在短時間內破解。

在 802.11 WLAN 上可將某些無線網卡，設成監聽模式，藉以進行網路監聽，在此收錄相關類似程式供參考，如表一所示:

表一．相關類似程式參考表

軟體名稱	功能簡介
Airopeek 及 Observer	多種有用的通訊協定分析及過濾(Filter)，可在 windows 2000 及 XP 上執行
Sniffer Pro Wireless	多種分析及過濾工具內建，可在 windows 2000 上執行
Mognet	開放原始碼(Java)，基本分析追蹤無線基地台、使用者及網路流量，在 Linux 上執行
Kismet	開放原始碼，在 Linux 上執行，文字式界面，功能同 Mognet 軟體

五、結論與未來展望

在 Wireless LAN 的使用當中，安全的問題一直都是存在的，而無線網路所傳輸的資料其除了安全，還需考慮方便性以及成本之間的評估取的平衡點。而根據一般的使用習慣大概只有四分之一的人，對於使用存取點(Access Point ,AP)，啟動了加密的 Key(WEP/WPA)，所以網路的安全值得大家來探討。目前網路當中最理想的配合，當屬 WPA+ IEEE 802.1X，其身份認證與密鑰管理協定，也因如此，WPA 為 Wireless LAN 的第一道關卡，所以說對網路安全相當的重要，WPA 也可以說是目前 Wireless 中最具強健性、相容性，可解決目前已知的各種入侵攻擊了。

在未來展望， Wi-Fi 聯盟已在 2003 年 4 月 29 日完成首次 WPA 認證，第三季起，所有與 PC 相關的 WLAN 產品，都須通過 WPA 測試，才能獲得 Wi-Fi 認證。802.11i 預計 2004 年第二季正式核准，Wi-Fi 聯盟將在 2004 年第三季，接受 WPA v2（第二版）認證。

六、參考文獻

[1] 1999, IEEE 802.11 standard & IEEE 802.11i drift 3.0 standard wireless LAN document .

[2] The dangers of mitigating security design flaws: a wireless case study
Petroni, N.L., Jr.; Arbaugh, W.A.;
Security & Privacy Magazine, IEEE , Volume: 1 Issue: 1 , Jan.-Feb. 2003

[3] Security architecture for wireless LANs: corporate and public environment
Prasad, A.R.; Moelard, H.; Kruys, J.;
Vehicular Technology Conference Proceedings, 2000. VTC 2000-Spring Tokyo. 2000 IEEE 51st , Volume: 1 , 15-18 May 2000

[4] FreeRADIUS , http://www.freeradius.org.

[5] RFC2284,RFC2138 & RFC2548 document for Authentication.

[6] Priorities in WLANs, Computer Networks, Volume 41, Issue 4, 15 March 2003, Pages 505-526 Imad Aad and Claude Castelluc