

無線網路
安全
白皮書



台灣電腦網路危機處理暨協調中心

民國九十二年二月

802.11 無線網路安全白皮書

目錄索引

前言.....	1
無線網路概說.....	2
無線網路的涵擴範圍.....	2
802.11 通訊模式.....	5
802.11 無線網路安全機制.....	7
使用者認證.....	8
資料保密.....	11
資料完整性確認.....	13
802.11 安全認證措施與威脅.....	15
802.11 認證措施分類.....	15
網路攻擊的分類.....	16
802.11 安全措施相關弱點分析.....	18
未使用加密認證方式相關弱點與攻擊.....	19
網路監聽.....	19
開放式系統認證及相關攻擊.....	21
封閉式系統認證及相關攻擊.....	22
使用加密認證相關弱點與攻擊.....	23
窮舉及字典攻擊法.....	24
已知或猜測原文攻擊法.....	25
密鑰弱點攻擊法.....	26
網路設備相關弱點.....	27
Telnet 管理介面.....	27
TFTP 管理介面.....	28
WWW 管理介面.....	28
SNMP 管理介面.....	28
預設管理密碼.....	29
緩衝區溢位攻擊.....	29
用戶端安全問題.....	30
用戶端密鑰儲存問題.....	30
以偽造存取點攻擊用戶端.....	30
其他的攻擊方式.....	31
阻絕服務式攻擊.....	31
中間人(MITM)攻擊.....	31

增進無線網路安全的方法.....	33
修改預設的設定.....	33
預設的密碼.....	33
預設的 SNMP 社群碼.....	34
預設的 SSID.....	34
預設的通訊頻道.....	34
修改網路設計.....	35
DHCP 伺服器的使用.....	35
使用適當的加密技術.....	35
網路卡號管理.....	36
防火牆區隔網段.....	36
802.1x 使用者認證.....	36
VPN 的使用.....	39
相關管理措施.....	41
制定無線網路安全政策.....	41
授權無線網路使用.....	41
確認無線網路活動範圍.....	41
確認無線網路相關安全操作標準.....	41
確認無線網路管理權責.....	41
無線網路設備清查.....	42
無線網路基地台清查.....	42
無線計算設備清查.....	42
無線網路安全應變與稽核.....	42
無線網路安全應變機制.....	42
無線網路安全稽核.....	42
結論.....	43
參考資料.....	44
作者介紹.....	46

圖次

圖 1、無線網路包含之領域.....	2
圖 2、802.11 無線網路安全涵蓋範圍.....	4
圖 3、802.11b 基礎建設模式網路拓譜.....	5
圖 4、802.11b 簡易模式網路拓譜.....	6
圖 5、802.11b 認證模式.....	8
圖 6、Challenge-Response 使用者認證模式.....	10
圖 7、簡化後的挑戰-回應認證模式.....	11
圖 8、WEP 加密流程.....	12
圖 9、WEP 用於資料完整性確認.....	14
圖 10、802.11b 認證模式.....	15
圖 11、網路攻擊的分類方式.....	17
圖 12、Airopeek 探測週遭網路節點狀況實例.....	23
圖 13、WEP 加密流程.....	25
圖 14、802.1x 網路拓譜.....	37
圖 15、802.1x 應用於 802.11 網路.....	38
圖 16、VPN 應用於無線網路.....	39
圖 17、VPN 與 WEP 安全的關係.....	40

表次

表 1、802.11 無線網路特性	3
表 2、無線網路重要的安全問題.....	19
表 3、無線網路監聽程式列表	20
表 4、無線網路掃描程式列表	22



前言

自十九世紀末電磁波的發現以來，無線通訊的發展可說是日新月異。不論是在軍事或商業用途、人們的日常生活裡幾乎都已經跟無線通訊脫離不了關係了。從收音機裡的廣播、電視裡的影像，到今天行動電話所傳遞的聲音與影像在在都是無線通訊進展的最佳見證。

而無線網路科技也日新月異，從早期利用 AX.25 傳遞網路資料到今日的 802.11、802.15 與 802.16 幾乎把小到個人空間 (Wireless Personal Area Network, 802.15)，然後區域空間 (Wireless Local Area Network, 802.11)，以及大到整個都市空間 (Wireless Metropolitan Area Network, 802.16) 的無線網路技術都包含在內。各種技術百家爭鳴不說，安全問題也是層出不窮。這也是這份白皮書產生的動機。

之所以挑選無線區網 (WLAN, 802.11a/b/g) 作為研究目標並不只是因為美國國防部把這科技列為恐怖份子覬覦的對象而已，也是因為無線區網可說是近幾年來竄起最快的新科技，不論自大型企業到中小企業或是家庭用戶，使用無線網路可說已經成為一股風潮。

在享受科技帶來的便利性的同時，安全問題更是不可忽略的，我們自然不希望使用者因噎廢食，捨棄無線網路的方便不用，但是我們也希望藉由這篇白皮書讓讀者了解到當前無線網路的安全問題為何以及有什麼方法可以降低使用者的風險。資訊安全界最重視的不是讓你絕對安全，而是採取適當的步驟將風險降低到可以接受的程度以達到科技的便利性與兼顧安全性的平衡。

無線網路概說

無線網路的涵括範圍

隨著網路以及電腦科技的逐漸普及，資訊與生活的關係也日漸緊密起來，實體世界與虛擬世界的界限也越來越模糊。利用手機或無線網路進行資料交換、分享、傳播，甚或無線商業資料的傳送也日漸普及。從前幾年推行的 WAP 手機無線上網，到近年來的 GPRS、i-mode 上網等等，都是無線網路嘗試融入我們日常生活的無線網路生活計畫。

一般所謂的「無線網路」涵蓋的範圍包括了常見的無線電話網路 (GSM, GPRS, WAP)、設計作為短距離無線資料交換(例如 PDA、家電等等使用)的藍芽(Bluetooth)或 802.15 (WPAN) 無線網路，以及最近非常熱門的當紅炸子雞 – 802.11 (802.11b、802.11a 等等)無線網路，還有長距離的 802.16 (WMAN)；這幾種網路的關聯性請見圖 1。在本白皮書中我們將對目前最普及的 802.11 無線網路及其安全性進行介紹。文中除了提出目前已知常見的安全漏洞，也同時提出各種防範知道以供管理者參考使用。

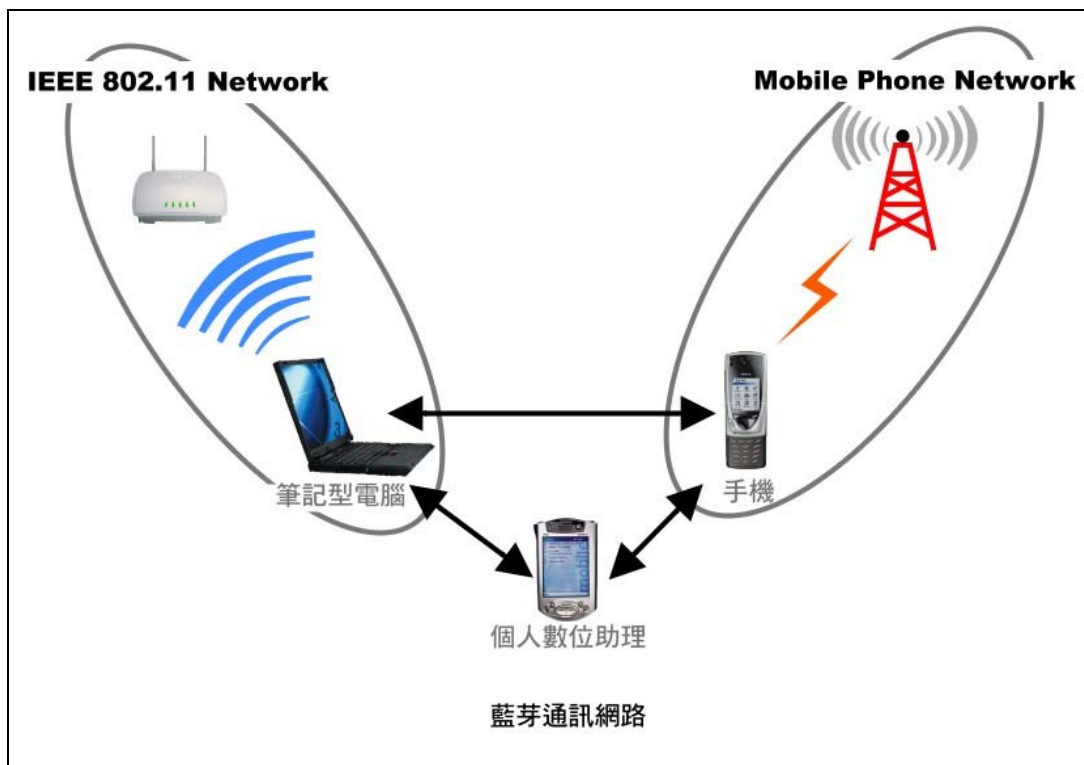


圖 1、無線網路包含之領域(資料來源：NIST)

自從九〇年代初期 IEEE 開始研究一個使用無線技術進行網路通訊的通

訊標準，直到 1997 年公佈了 802.11 標準後，又於 1999 年通過了 802.11b 與 802.11a 無線通訊標準，其中的 802.11b 就是目前應用最為廣泛的電腦無線網路通訊標準。在不久的將來將由現有的 2.4 GHz 頻帶轉移至 5GHz 頻帶，並提供 54Mbps 的高速網路傳輸。關於 802.11 系列之特性如下表所列：

特徵	描述
實體層	Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), Infrared (IR)
頻率波段	2.4Ghz (ISM band) and 5 Ghz
資料傳輸速率	1Mbps, 2Mbps, 5.5 Mbps, 11Mbps (11b), 54Mbps(11a and 11g)
資料與網路安全	以 RC4 為基礎的加解密演算法來保護資料的隱密性，使用者身份認證以及資料完整性。提供有限度的密鑰管理。
作業範圍	室內約 45 公尺；室外約 455 公尺
Throughput	最高 11Mbps(11b)/54Mbps (11a,g)
優點	等同於不需要線的乙太網路；消費者選擇眾多；價格降低速度很快
缺點	先天設計缺陷導致安全問題；Throughput 隨著距離與負荷增加而減少

表 1、802.11 無線網路特性

802.11 無線網路主要的優點在於不需要實體佈線，而且因為有 IEEE 的標準規範使得每一家硬體設備廠商所提供的設備有一定的互通性，而由於大量廠商的投入製造使得設備成本大大地降低 (以 Orinoco 的 Gold 等級網路卡為例，由去年的一張近萬台幣到目前一張僅需四千台幣以下，其他的廠牌甚至有兩千元以下的價格)。

由於不需要拉設實體線路，加上美觀的考量，因此已經有不少家庭用戶與中小型辦公室開始使用無線網路作為網路的設備。

但是在設計 802.11 無線網路時必須注意的是，由於無線通訊的特性，在訊號的控制上有先天性的缺陷，無法確保通訊內容不被竊聽，甚至若存取控制沒有做好，則將造成網路資源遭受竊用。此外，2.4GHz 通訊頻帶有許多電子設備使用，例如微波爐，無線電話等，其干擾較為嚴重，而且通訊的速率不甚穩定，若距離較遠或是中間有建築物阻隔，通訊速率將會下降許多。

由於無線網路也屬於乙太網路的一個子集合，因此我們必須針對無線網路

安全討論的範圍加以探討。

802.11 無線網路探討的範圍在於通訊用戶 (Wireless Station, STA) 與存取點 (Access Point, AP) 端無線通訊過程中可能發生的問題，或是因無線通訊的特性無法避免會產生的一些安全議題，還有通訊用戶與存取點本身的安全問題。有趣的是，幾乎所有 802 系列網路可能出現的安全問題都會出現在無線網路安全問題上；我們探討的範圍如下圖 2 所示。

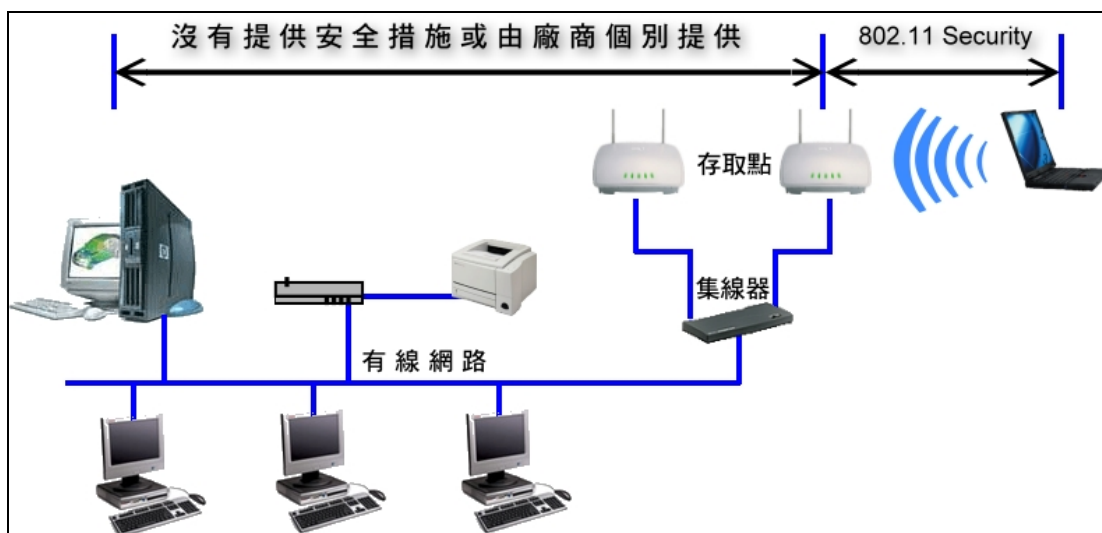


圖 2、802.11 無線網路安全涵蓋範圍

802.11 通訊模式

802.11b 標準中允許網路通訊以點對點(peer-to-peer, p2p)方式進行連接,這種模式稱為簡易模式(Ad hoc Mode);或是使用一個存取點(Access Point, AP),讓所有的用戶端連上以後作為資料交換的中心,這種方式稱為基礎建設模式(Infrastructure Mode)。

在基礎建設模式中,所有的 802.11b 設備,包括筆記型電腦、個人數位助理等等設備,皆連接到存取點,以存取點來接送(relay)網路通訊的內容,不論是到另外一個無線網路設備端或是 Internet。此時存取點扮演的角色是介於兩種不同實體通訊層(無線網路與乙太網路)間的橋接器(Bridge)一般。其部份特徵也與乙太網路中的橋接器很類似。基礎建設模式的網路拓譜如圖 3 所示。



圖 3、802.11b 基礎建設模式(Infrastructure Mode)網路拓譜

簡易模式與基礎建設模式不同的地方在於簡易模式並沒有一個中央的伺服器(如基礎建設模式中的存取點的角色),而直接可以進行點對點的資料交換。簡易模式的網路拓譜如圖 4 所示。



圖 4 、802.11b 簡易模式(Ad-Hoc Mode)網路拓譜

在典型的 802.11 無線網路環境中由不同的通訊設備所共同構成，這些設備可以包括桌上型電腦、筆記型電腦、個人數位助理(PDA)或是存取點(在基礎建設模式中)等等，他們透過無線網路卡作為實體溝通的管道。目前市面上可以見到的無線網路卡的形式包含了傳統的 ISA 卡、PCMCIA 卡以及 USB 介面的無線網路卡等等。

802.11b 網路的涵蓋範圍受到許多不同的因素的影響，這些因素包含了連線的速率(某些網路卡可以在驅動程式中強迫指定較高的通訊速率，如此會縮短通訊可能達到的距離)、環境周圍電磁波的影響、周圍實體環境的變因、電力損耗(某些網路卡可以啟動省電模式，降低網路卡功率以節省電源)以及是否使用天線等等。一般而言在室內的有效範圍大約為 50 公尺左右，而在室外則可達到約 400 公尺。在美國有人加大放射功率將室外距離拉長到 115 公里，還能有同樣的連通率 (throughput)。只可惜這麼做違反了 FCC 的規定，但是即使將功率降到合法的數值以內，連通率還可以高達 300Kbps。

以上介紹了無線區網的物理性質與常見的兩種網路拓撲，目的是讓讀者在了解有關於無線區網安全問題前能夠先對無線區網的運作方式有所了解，有了足夠的背景知識後也更容易替自己找出適當的改進方法。不過值得注意的是，以上這幾個段落只能提供初步的了解，讀者若欲更深入了解無線區網各層次的運作原理，可以參考坊間有關無線通訊的書籍。

802.11 無線網路安全機制

根據 IEEE 所制定的標準，一個無線網路必須提供的三項基本網路安全服務為：

1. 使用者認證 (Authentication)

在無線網路環境中必須對使用者身份進行基本的辨識。在 802.11 無線網路中身份辨識的方式主要有三種：開放系統認證 (Open System Authentication)、封閉系統認證 (Closed System Authentication) 以及分享密鑰認證 (Shared-key Authentication)。其中的分享密鑰認證有時也被稱為挑戰與回應認證 (Challenge-Response Authentication)。

2. 資料保密 (Confidentiality)

在無線網路環境中對於資料的傳輸能夠提供基本的安全防護，以防止第三者竊取通訊內容。在這部分主要是以 WEP (Wired Equivalent Privacy) 來達成；關於 WEP 的詳細運作方式將於下文中進行說明。由於 WEP 的問題太多，因此 IEEE 正在研擬新的標準來取代 WEP (802.11i, or WPA)。

3. 資料完整性確認 (Integrity)

在 802.11b 網路中使用的完整性確認與其他 802 家族相同，使用 CRC checksum 來進行封包內容的完整性確認。在啟動 WEP 的時候則可透過 WEP 的加密對傳送內容及 CRC 進行更嚴格的保護。

關於 802.11 無線網路的認證方式如下圖 5 所示。

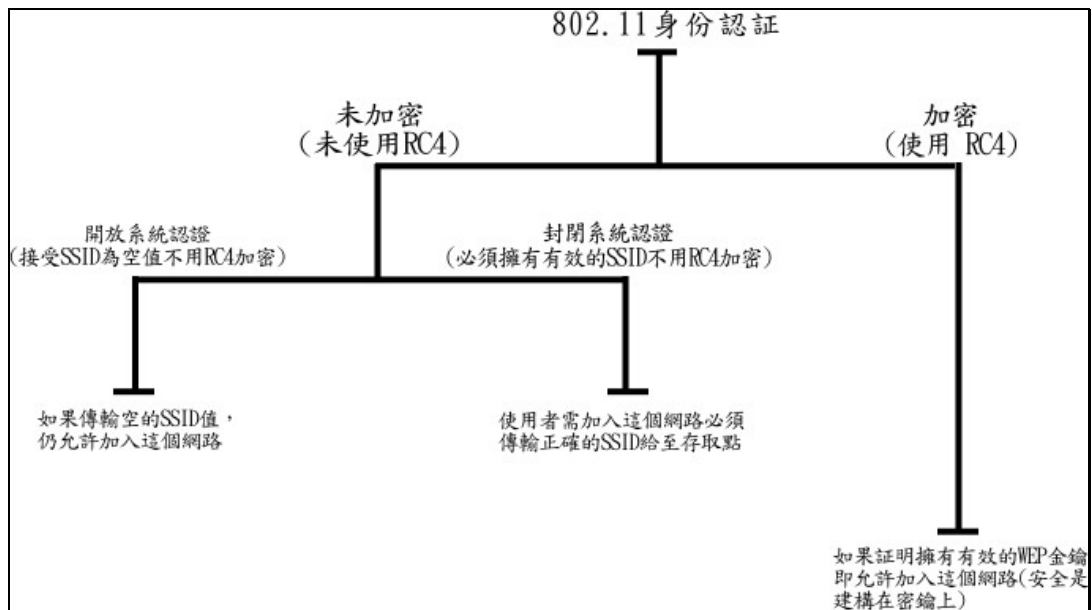


圖 5、802.11b 認證模式(資料來源：NIST)

使用者認證

使用者身份認證方式大致可以區分成加密認證與無加密認證兩大類：

無加密認證

無加密認證主要以 SSID (Service Set ID)作為最基本的認證方式，在無線區網的設計裡面，一個或多個“基地台”(base station) 形成一個“服務區域”(Service Set)。每個服務區域都有一個方便使用者辨識的名稱，這個名稱叫做“服務域名”(Service Set ID, SSID)。使用者只需要設定自己的無線網卡加入特定的服務域名就可以與基台建立連結使用此無線網路(在此假設沒有任何其他的身分認證機制)。因此一個無線網路的服務域名將是攻擊者想要知道的首要資訊。

在這種身分認證模式中，只要使用者能夠提出正確的 SSID，存取點就接受用戶端的登入請求。這種認證方式類似於大樓警衛在過濾訪客時，只要訪客能夠說出想要訪問的對象，就放行。在這種認證方法下又分為兩種認證方式：開放系統認證 (Open System Authentication) 與封閉系統認證 (Closed System Authentication)。

開放系統認證：

在開放系統認證的模式下存取點會對空白的 SSID (null SSID)作出回

應，回應的內容則是該存取點的 SSID，這也就是在 Windows XP 下一但啟動無線網路時，會出現的“可使用網路”清單的工作原理。

在這種認證方式下任何人都可以取得 SSID 並且與存取點進行連線，因此這種做法與大樓警衛後方就是該大樓公司行號的列表一樣，如果有心人士想要滲透進入，只需要看一眼列表報知警衛，便可暢通無阻；可以說是完全沒有任何安全防護的認證方式。

封閉系統認證：

在這種認證方式下，存取點將不對 null SSID 回應，使用者必須提供正確的 SSID 才能與該存取點進行連線。

這種方式乍看之下應該足夠安全，因為這種認證方式如同一般的密碼認證，必須要得知密碼才能進入系統。但是由於無線網路的特性，無法控制訊息的傳播方向（它是以無線廣播的方式傳送資料），因此攻擊者可以利用網路嗅探 (sniffing) 的方式取得 SSID，進而使用無線網路。

這種方式如同要通過大樓警衛的詢問時，偷聽前幾個人的回答而依樣畫葫蘆，藉以欺騙警衛以達到滲透的目的。

加密認證

加密認證使用分享金鑰(或稱為挑戰與回應)的方式進行身分認證，在 802.11b 認證方式中使用 WEP 密鑰作為我們的分享金鑰。

這個認證方式主要流程如下圖 6，大致有四個階段，整個認證過程以 RC4 加密方式為基礎。

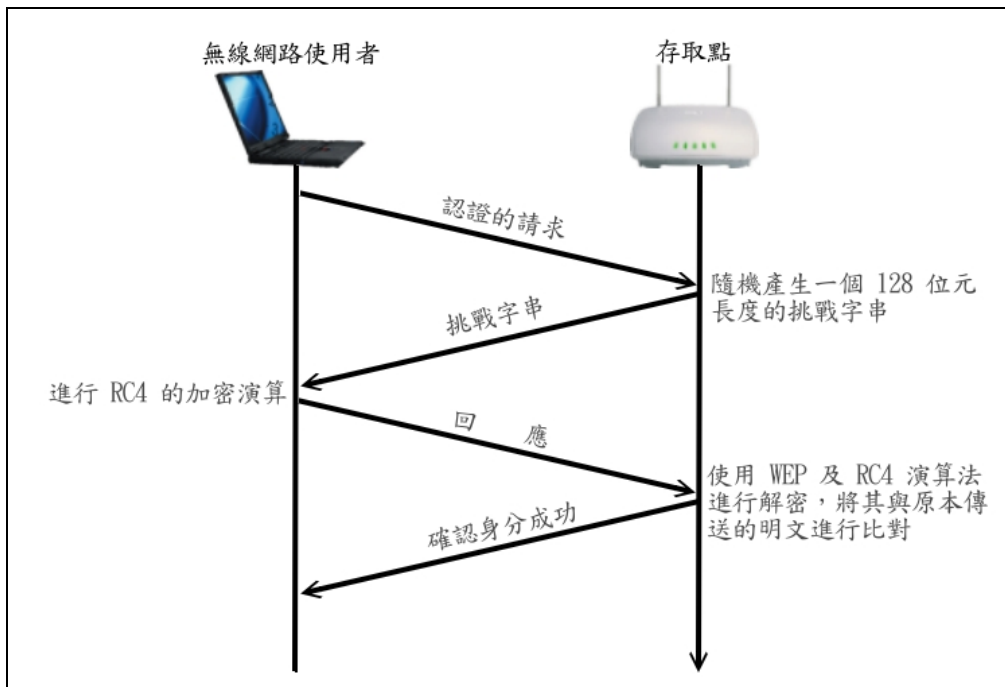


圖 6 、 Challenge-Response 使用者認證模式

1. 無線網路使用者 (Wireless Station, 或稱為 STA) 對存取點 (AP) 提出認證的請求。
2. AP 收到請求後產生一個 128 位元長度的挑戰字串 (Challenge Text)。
3. AP 將步驟二中產生的字串傳送給 STA，等待 STA 傳送加密後的結果。
4. STA 收到這個挑戰字串後，使用 WEP 密鑰進行 RC4 的加密演算。
5. STA 將字串加密後的密文回傳給 AP。
6. AP 收到加密後的密文，使用 WEP 及 RC4 演算法進行解密，將其與原本傳送的明文進行比對。如果解密後的結果與明文挑戰字串符合則表示通過驗證；如不符合則表示對方無法提供正確的 WEP 密鑰，無法通過驗證。
7. 依照步驟六中獲得的結果決定接受或拒絕該 STA 的連線請求。

一個簡化過的認證模式如下圖 7 所示：

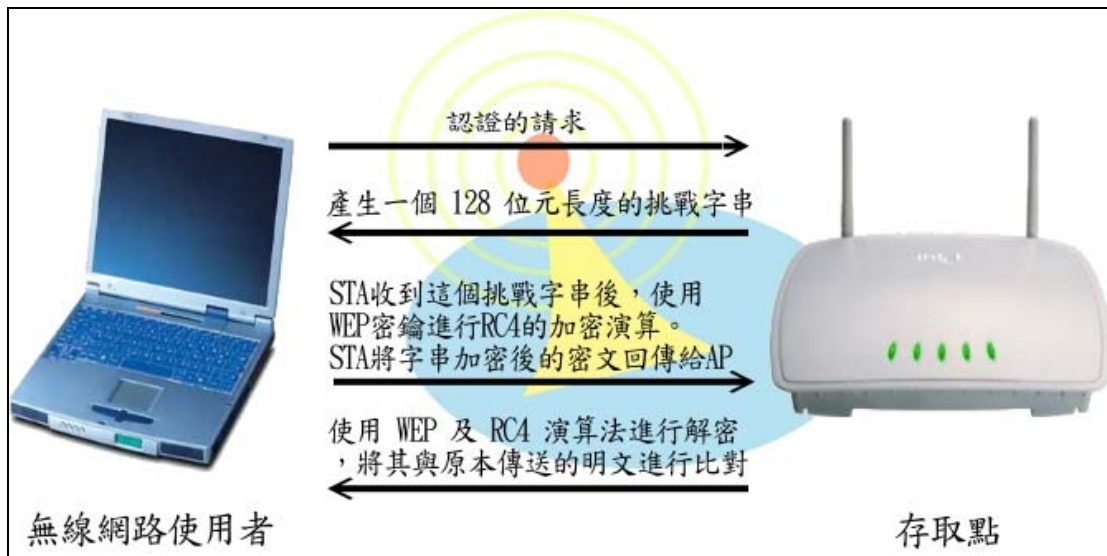


圖 7、簡化後的挑戰-回應認證模式

資料保密

由於無線網路通訊是以無線電廣播的方式進行訊號的傳遞，較一般的網路更容易遭受資料的竊聽，為此 IEEE 設計了一個加解密的機制，期望無線網路使用者能獲得與一般有線網路同等的私密性；這個加解密機制稱為 WEP (Wired Equivalent Privacy)。

根據 802.11-1999 的標準，WEP 的設計是為了要滿足以下幾個條件：

1. 這個系統要夠強韌足以抵擋暴力或字典攻擊法。
2. 這個系統必須要提供自我同步 (Self-synchronizing) 的特性，即使在惡劣的傳輸情況下，依然要能夠完成保護資料的動作。
3. 這個系統必須要有效率，可以用硬體或是軟體來實現。
4. 這個系統最好是可出口的。由於美國對加解密技術有出口管制，因此希望 WEP 能夠符合可出口的條件。
5. 這個系統是非必要的。意即使用者可以選擇用或不用 WEP。

WEP 基本上是一個對稱式加解密系統 (Symmetric Cryptography System)，亦即加密與解密是用同樣一個密鑰，原始密鑰的長度是 40 bits 或 104 bits。WEP 使用 RC4 PRNG (虛擬亂數產生器) 的演算法來產生實際加解密的密鑰，然後用 XOR 演算法作資料加解密的動作，以配合無線網路封包多變的資料長度。整個 WEP 的運作流程可以參考圖 8 以及以

下說明。

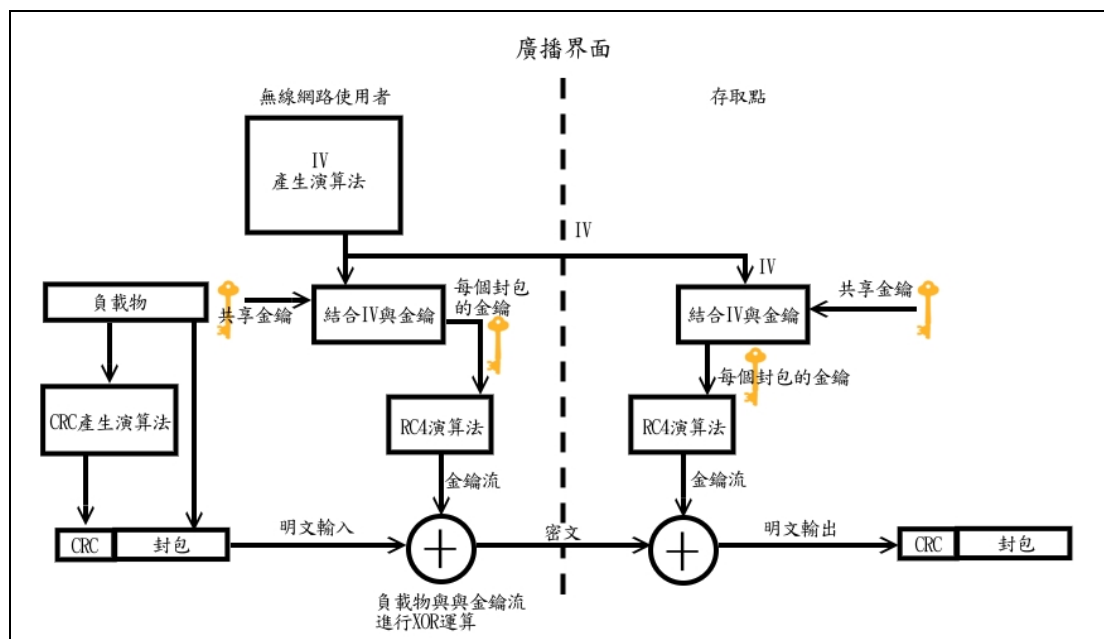


圖 8 、WEP 加密流程 (資料來源：NIST)

WEP 加密需要的相關資訊

1. 由於 WEP 採用的加密方式為對稱金鑰加密方式，因此資料收送端必須持有相同的密鑰，根據 802.11b 的標準，這個金鑰長度可以為 40 bits 或是 128 bits。
2. 雙方使用相同的加解密演算法，在此使用的是 RC4 演算法與 XOR 演算法。
3. 由於在加解密過程中為了避免固定金鑰 (static key) 的使用容易遭受破解，因此加入了一個 24 bits 長度的初始向量 (Initial Vector, IV)，藉此打亂加密金鑰的組合。

WEP 加密流程

1. 發送端將封包的負載物 (payload)進行 CRC 的運算產生完整性檢核碼，並附於該封包中。
2. 發送端使用 IV 產生的演算法取得一個 IV。
3. 發送端將 IV 以及密鑰進行 RC4 PRNG 運算取得一個加密金鑰。
4. 利用此加密金鑰將步驟 1 所得到的封包進行 XOR 運算加密，獲得一密文資料，並將 24 bit 長度的 IV 附於本資料中。

5. 將密文資料透過無線網路傳送給接收端。

WEP 解密流程

1. 取得附於封包中的 IV。
2. 將取得的 IV 與密鑰進行 RC4 PRNG 運算取得對該封包進行加密的金鑰。
3. 將該封包資料透過步驟二所獲得的加密金鑰進行 XOR 運算還原，便可取得明文資料，
4. 進行 CRC 完整性確認。

資料完整性確認

在 IEEE 802 系列的網路通訊協定中通常都使用 CRC 的方式作為資料完整性的確認，這種方式可以有效的防止資料傳輸過程中受到電氣因素或其他不明因素的干擾，透過一個單方向的雜湊函數 (one-way hash function) 進行資料完整性的確認。接收方可以將所接收到的負載資料 (payload) 透過同樣的函數進行運算，得出的數值與乙太網路封包中存放的 CRC 值進行比對，若數值相同則確認資料的完整。

但是在網路安全的領域中所謂的資料完整性確認隱含著在資料收送兩端之間的通訊是無法被竄改的，一般的明文通訊極為容易遭受第三者介入 (man-in-the-middle)或是通訊劫奪 (session-hijacking)的攻擊法破解。而 802.11b 則嘗試使用 WEP 的加密方式來進行資料的完整性確認。

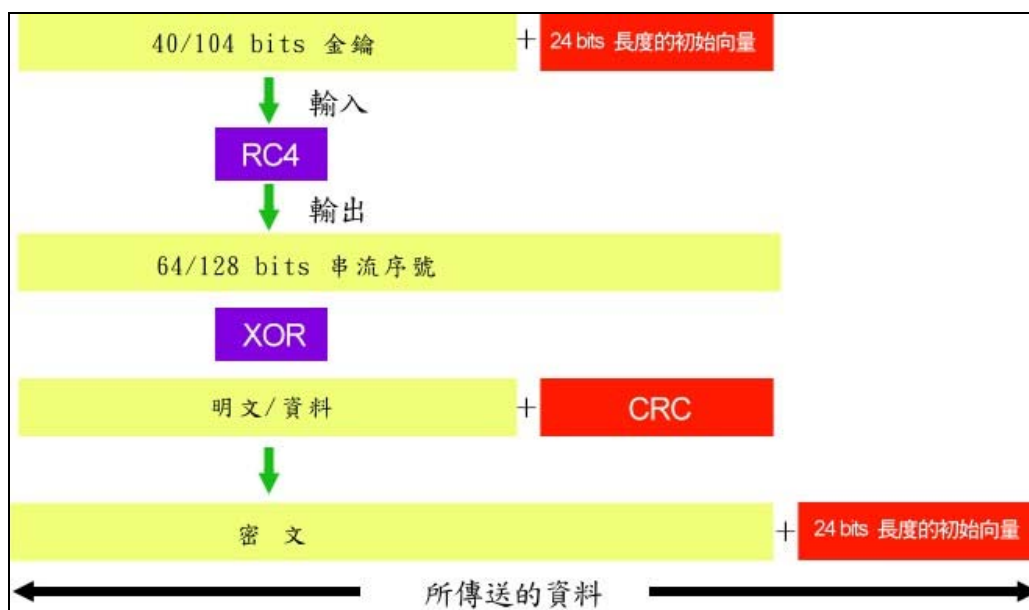


圖 9、WEP 用於資料完整性確認

資料來源：802.11, 802.1x, and Wireless Security, J. Philip Craiger

關於 WEP 的動作原理我們已在上一節中詳述，在此我們不再贅述。

802.11 安全認證措施與威脅

802.11 認證措施分類

802.11 安全防護及認證的相關措施大致可以分為使用加密方式的挑戰與回應 (Challenge-Response) 認證方式以及不使用加密的開放式系統認證 (Open-System Authentication) 與封閉式系統認證 (Closed-System Authentication) 幾種主要的方式，如下圖 10 所示。

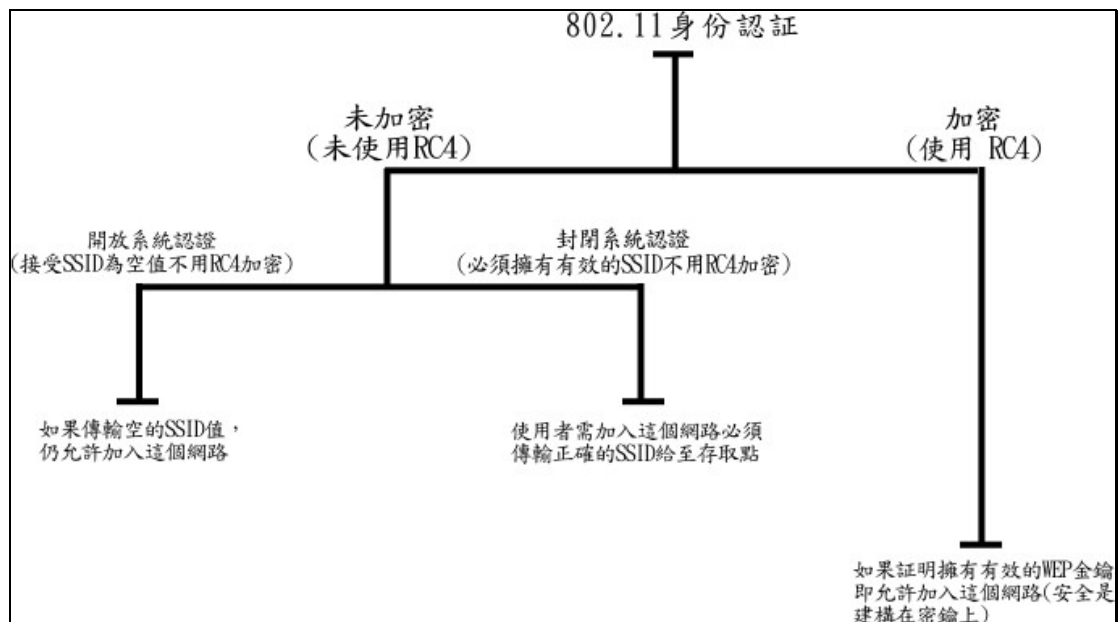


圖 10、802.11b 認證模式(資料來源：NIST)

未使用加密安全措施的無線網路如開放式系統認證以及封閉式系統認證都將遭受網路竊聽的攻擊，其中開放式系統認證由於將本身的 SSID 洩漏，使得入侵者能夠不需任何工具輕易地竊取網路資源。

使用加密安全措施的無線網路則由於 WEP (Wire Equivalent Privacy) 先天設計上的某些缺失，而被破解；我們將對破解的方式及工具進行詳細的介紹。

此外在設備出廠時的一些內定設定值往往因為使用者的疏失而未加更動，使得入侵者能夠獲得無線網路存取點 (Access Point, AP) 的控制權——根據 Eric Smith 與 Drew Fahey 今年度進行的一項研究顯示，有 30.8% 的人使用無線網路存取點時完全沒有更改系統的出廠設定，只有 28.5% 的人啟動了 WEP 來保護網路通訊內容；在本文中我們也將針對常見的設定缺失進行介紹。

在本文的下一個章節我們將對這些安全措施的弱點進行分析；但是首先我們先針對網路系統的攻擊行為進行分類與介紹。

網路攻擊的分類

根據一般的網路安全實務經驗，針對網路通訊內容的攻擊可粗分為主動式攻擊(Active Attack)以及被動式攻擊(Passive Attack)兩大類型。

所謂的被動式攻擊意指入侵者(非法)取得資訊資產的存取權限，但是並未對其內容進行竄改。主要的攻擊方式有以下兩種：

1. 竊聽 (Eavesdropping)：竊聽是指入侵者針對檔案或通訊內容進行監控。最常見的例子是於影片中時常出現的電話監聽與網路監聽等等。
2. 通訊分析 (Traffic Analysis)：流量分析是針對網路通訊的流量、內容、以及行為等等進行分析，透過通訊內容或者流量的分析可以獲得目標網路可觀的資料，如：伺服器位址、通訊模式等等。

所謂的主動式攻擊意指入侵者針對檔案或通訊內容進行偽造或修改，可能為以下四種攻擊型式之一或是採取混合方式進行：

1. 偽裝 (Masquerade)：偽裝是指攻擊者欺騙認證系統，非法取用系統資源。例如利用社交工程法騙取，或者利用網路竊聽的方式取得密碼後登入系統。
2. 重播 (Replay)：重播是指攻擊者將從網路上截取的某些通訊內容(如認證資訊)重新發送，以欺騙伺服器認證機制。常見的實例如早期 Windows 網路芳鄰採用雜湊方式 (Hash Function) 進行密碼的加密，入侵者若能截取獲得編碼後的密碼內容，可以利用重送一次的方式取得系統登入的授權。
3. 訊息竄改 (Message Modification)：訊息竄改指攻擊者針對網路通訊的內容進行刪增或者更動。通訊劫奪(Session Hijacking)利用 TCP/IP 網路通訊的弱點，搶奪合法使用者的通訊頻道，進而獲得系統的操作權限，這種方式為訊息竄改的一個實例。
4. 服務阻絕 (Denial of Service)：服務阻絕大概是大家最耳熟能詳的攻擊方式，攻擊者透過各種可能的方法 (ICMP flooding、SYN Flooding、Mail Bomb)等等方式使得使用者與管理者無法取得系統資源及服務。

網路攻擊的分類方式如下圖 11 所示。

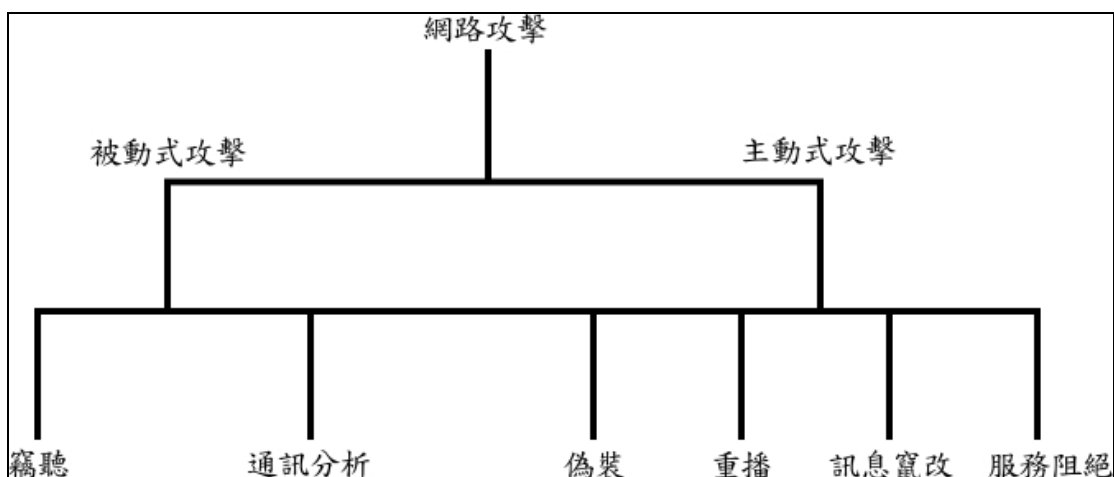


圖 11、網路攻擊的分類方式(資料來源：NIST)

802.11 安全措施相關弱點分析

802.11 無線網路的安全問題大致可分為三大類：

1. 無線通訊的特性

由於無線網路先天設計便是以無線電技術為基礎，使得攻擊者得以無線電波涵蓋的範圍內進行通訊內容的監聽。如果使用者未將傳送的資訊適當的進行加密，則入侵者很容易的便可以竊取所有的通訊內容。

另外由於無線通訊只要電波收訊範圍內即可使用，也造成了管控上的大麻煩，管理者無法完全的進行存取控制。

2. WEP 設計的錯誤

在 802.11 的標準中訂定了 WEP 的標準，希望透過這種加密技術能讓使用獲得更好的資料安全性，但是由於某些設計及實作上的錯誤使得 WEP 所獲得的效果並無法百分之百保證資料內容的機密性。

此外由於設計協定時沒有考慮金鑰管理的問題，因此如果你有一個很大的無線區域網路的話，金鑰的修改及配送會是一個很大的管理問題。

3. 設備安全管理措施不當

所有的網路設備出廠時都有一些預設的設定值，許多的管理者與使用者將網路設備當成家電般的隨插即用 (Plug and Play)，沒有更改系統內定的相關管理資訊；這些缺失可能造成攻擊者反客為主，獲得設備的管理權限，「幫助」管理者進行網路的管理。

無線網路重要的安全問題整理如下表：

網路管理者未設定安全相關功能	無線網路設備出場時的預設值大多沒有啟動安全相關的功能。雖然有些無線網路安全功能有已知的漏洞，但是這些安全相關的功能多少還是可以提高入侵難度。
IV (啟始向量) 長度太短或是常為固定值	24-bit 長度的 IVs 造成加密用的密鑰有重複使用的機會。當密鑰要重複時，一定程度的攻擊者可能加以利用並破解加密的保護。
加解密用的密鑰長度太短	40-bit 長度的密鑰已經不敷使用了。104 bits 長度的密鑰應該是最低要求。密鑰的長度越長，攻擊者用暴力搜尋法找到密鑰的難度就越高。
缺乏適當的密鑰管理機制	一個系統的安全有時候維繫在密鑰的安全程度上。若沒有適當的密鑰管理機制能減少密鑰被竊取的可能性以及定期自動更換密鑰的機制，密鑰可能成為整個無線區網中最脆弱的地方。

<p>RC4 密鑰產生演算法有弱點，並且 WEP 使用 RC4 的方法也不正確。</p>	<p>24 bit 長度的 IV 加上 RC4 密鑰產生演算法的弱點導致攻擊者可以有效地從收集到的資訊裡找出密鑰。RC4 大部份其他的應用都沒有這類的問題，因為那些應用不會將密鑰的部份內容公開以及不會每個封包都重新計算一次密鑰。這類攻擊需要對 WEP 及 RC4 有較深入了解的攻擊者。</p>
<p>封包完整性的保護很弱</p>	<p>CRC32 以及其他的線性方程式並不適用於提供密碼學上資料完整性的保護工作。使用這類線性方程式並不能提高惡意竊改資料的門檻。要完善地保護資料完整性需要依靠一些密碼學裡的方法，使用 CRC32 等非密碼學的方法通常無法達到保護資料完整性的目標。</p>
<p>沒有使用者身份認證機制；僅有簡易的 SSID (服務域名) 辨識。</p>	<p>須要身分認證的系統若建構於無線區網之上將會造成更多的弱點。</p>
<p>設備認證方式採用 challenge-response (挑戰與回應) 方法。</p>	<p>單向的挑戰與回應認證方式會遭受“Man-In-The-Middle”方式的攻擊。雙向認證方式可互相確認使用者以及無線區網的身分。</p>
<p>無線區網通訊協定設計缺陷</p>	<p>無線區網通訊協定再設計上有缺陷導致惡意攻擊者除了可以進行實體層的阻絕服務攻擊以外還可執行資料鏈結層的阻絕服務攻擊。</p>
<p>無線區網設備安全問題</p>	<p>無線區網設備包括 Access Point (存取點) 以及 Client (使用者端)。兩者都有很多的安全問題導致攻擊者有機可趁直接攻擊無線區網設備以取得控制權。</p>

表 2、無線網路重要的安全問題

以下我們將根據表 2 裡面所列出來的安全問題一一加以解說。首先從介紹各種認證方式所產生的網路安全弱點及攻擊方式開始。

未使用加密認證方式相關弱點與攻擊

由於無線通訊的訊號是四面八方傳遞的特性，使得在無線網路上監聽(或稱竊聽，Sniffing)的問題特別的嚴重，我們建議您參閱網路設備的操作手冊，除非您的網路存取點不支援 WEP 加密通訊，或是有設備之間 WEP 互通的連接問題，否則我們強烈建議您將存取點的 WEP 功能開啟。如果您所使用的產品有提供非標準的安全保護，我們也建議您在不影響設備運作情況下適當將這些額外的安全保護功能開啟。

網路監聽

網路監聽是常常出現的攻擊方式之一，由於乙太網路的設計是以共享通訊頻道 (Shared Communication Channel) 的方式進行的，所以在同一個資料匯流排 (Bus) 之下的網路節點可以接受到其他節點的通訊資料。在一般的 802.3

乙太網路上，可以利用特殊程式將乙太網路卡設定為雜湊模式 (Promiscuous Mode)，如此一來便可以擷取網路上所有的封包進行分析。一般來說這類程式通稱為 Sniffer，原本設計的目的在於方便網路管理者進行網路流量的分析與除錯；但是也有某些 Sniffer 是專門設計來竊取密碼或者進行通訊內容的監控。

在 802.11 無線網路上則可以將某些無線網卡設定成 Monitor mode (監聽模式) 藉以進行網路的監聽，茲收錄相關類似程式如下表：

軟體名稱	功能簡介	網址
Airopeek	商業軟體，價值約 \$3,800 美金，圖形化使用者介面，多種有用的通訊協定分析工具以及過濾工具 (filters)，可以在 win 2000 及 XP 上執行，支援多張無線網卡，並且即將推出對 802.11a 的支援。	http://www.wildpackets.com/
Sniffer Pro Wireless	商業軟體，價值約 \$8,000 美金。圖形化使用者介面，多種分析及過濾工具內建，可以在 win 2000 上執行，支援較少無線網卡，目前尚無計劃提出對 802.11a 的支援。	http://www.sniffer.com/products/sniffer-wireless/default.asp?A=5
Observer	商業軟體，價值約 \$3,800 美金，圖形化使用者介面，多種分析及過濾工具內建，同一軟體也可用於監聽乙太網路。可在 win2000 及 XP 上執行，支援多張無線網卡，計劃推出對 802.11a 的支援。	http://www.networkinstruments.com/
Airmagnet	商業軟體，價值約 \$3,000 美金，圖形化使用者介面，多種分析及過濾工具內建。只能在 WinCE 上執行，因此需要配合 PocketPC.	http://www.airmagnet.com/
Mognet	開放原始碼軟體，以 Java 撰寫。圖形化使用者介面，提供基本的分析工具追蹤無線基台以及分析網路資料量，提供基本的監聽以及追蹤無線網路基台與使用者的功能。主要在 Linux 上執行。	http://chocobospore.org/mognet/
Prismdump	免費軟體，以 C 語言撰寫，主要執行於 Linux 並且已經被移植到 BSD 上。類似 tcpdump 的工具但是針對 IEEE 802.11b 無線網路。	http://www.guerrilla.net/software/linux/80211/tools-prismdump_2000_1122.tgz
Kismet	開放原始碼軟體，主要執行於 Linux 作業系統上，文字式介面。提供無線基台追蹤以及網路資料量分析等簡單的功能。	http://www.kismetwireless.net/

表 3、無線網路監聽程式列表

攻擊者使用這些程式可監聽未使用加密的所有通訊內容；某些監聽軟體甚至可以將通訊的內容以模擬終端機的形式展現，也就是您的 telnet 視窗中看到什麼，監聽的人士便可以看到一模一樣的內容。

開放式系統認證及相關攻擊

在開放式系統認證的方式下，如果將無線網卡要加入的服務域名設定成“ANY”，此時無線網卡就會發出訊號詢問週遭是否有無線網路存取點的存在，若存取點被設定為對此類詢問有所反應，則此存取點就會送出回應給此無線網路卡，而此回應就包含 SSID。

利用這個原理，我們可以撰寫一個程式不斷的對週遭進行廣播，送出這種請求，進而獲得一個可用網路的列表；在網路上可以找到很多相關的程式可以進行無線網路存取點的掃描。有許多的存取點可以配合全球衛星定位系統 (GPS) 紀錄無線網路存取點所在經緯度，以方便繪製可用無線網路分布圖；表 4 為相關程式列表：

軟體名稱	功能簡介	軟體平台	網址
Netstumbler	支援全球定位系統，圖形介面，能偵測基台信號強度與相關資料。	Windows	http://www.netstumbler.com/
Wavelan-tools	能偵測基台信號強度與相關資料，圖形介面。	Linux/Unix	http://sourceforge.net/projects/wavelan-tools/
Dstumbler (bsd-airtools)	支援全球定位系統，能偵測基台信號強度與相關資料，文字式圖形介面。	*BSD/Linux	http://www.dachb0den.com/projects/bsd-airtools.html
airosniff	偵測基台信號強度與有無 WEP 機制，文字介面。	*BSD	http://www.graviton.net/bind/airosniff/
Airtraf	偵測基台信號強度與相關資料，文字式圖形介面，具備簡易入侵偵測功能。	Unix	http://sourceforge.net/projects/airtraf/
Wavemon	偵測基台與無線區網使用者的信號強度與相關資料，文字圖形介面。	Linux	http://www.jm-music.de/projects.html
Network Monitor	偵測基台與無線區網使用者的信號強度與相關資料，圖形介面，作業系統附屬程式。	WinXP and .Net server	Part of .Net server MMC add-in.
Wellenreiter	偵測基台與無線區網使用者的信號強度與相關資料，圖形介面。	Linux,*BSD (written in GTK+Perl)	http://www.remote-exploit.org/
iStumbler	支援全球定位系統，圖形介面，能偵測基台信號強度與相關資料。附原	MacOS X10.2	http://homepage.mac.com/alfwatt/istumbler/

始碼。		
Apscan	偵測基台信號強度與相關資料，圖形介面。	MacOS X http://homepage.mac.com/typexi/Personal1.html

表 4、無線網路掃描程式列表

利用這些掃描程式進行無線網路存取點掃描在駭客圈中是常見的休閒娛樂，這些人可以利用一台筆記型電腦配合無線網卡以及掃描程式，加上高功率的天線駕車在市區內掃描可用的無線網路，配合全球衛星定位系統標記出所有可用的無線網路。這種行為稱為 War Driving，有些人則選擇在可用無線網路的附近人行道上畫上標記以提醒同好，這種方式則稱為 War Chalking。

在網際網路上有許多類似 Wardriving 計畫的網頁，例如網路上某位有閒的仁兄便針對舊金山灣區的可用無線網路進行掃描，並且放在網頁上供人參考；Pete's Demo Wardriving Maps(<http://www.dis.org/wl/maps/>) 便是這位仁兄的大作。

在網路上類似的計畫非常的多，透過適當的關鍵字便可以取得許多地區的無線網路分布圖。

封閉式系統認證及相關攻擊

既然使用開放式系統認證那麼危險，也許您會這麼覺得：「既然如此，我把認證方式設定為封閉式系統認證，不要讓我的存取點對 ANY 的要求回應就好了，我的 SSID 取的奇怪一點、不好猜一點，駭客就猜不出來了！」

這句話只對了一半——因為有心的攻擊者不需要用猜的，用竊聽的就可以了。攻擊者可以監聽附近無線網路的通訊內容，這些通訊內容包含兩種重要的封包讓攻擊者可以取得服務域名。

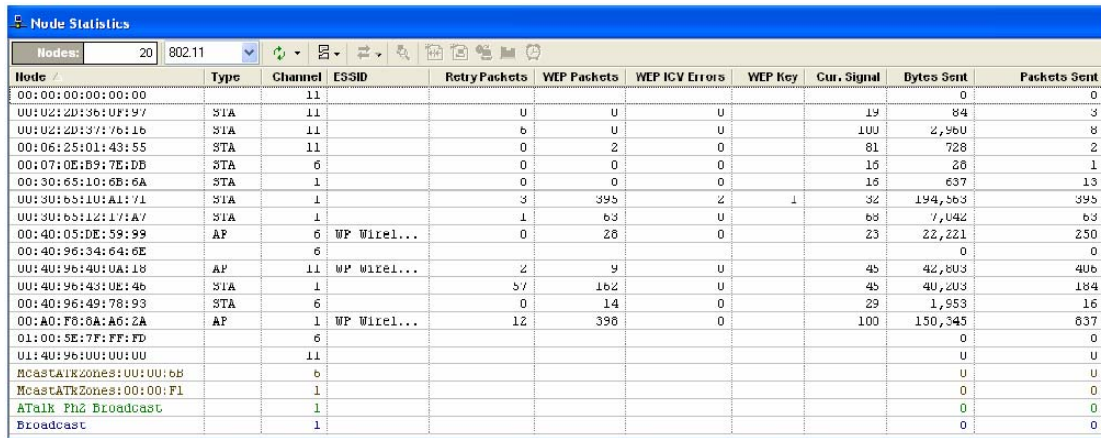
首先，存取點會定時發出一種標誌訊框 (Beacon Frame) 告知無線區網的使用者這個存取點的存在，在這訊息封包裡其中一項資訊就是服務域名(SSID)。

另外，在一個使用者能正式加入無線區網之前，無線網卡會送出“探測請求”(Probe Request)的封包以確定附近有存取點存在。這個封包就包含了此電腦要加入的無線區網的服務域名。

這兩種資訊都是在沒有任何加密系統保護下傳遞。因此若攻擊者可以在無線區網訊號範圍內監聽到這些消息，攻擊者就可以取得服務域名的相關資訊。在取得 SSID 之後，攻擊者只要將這個 SSID 填入系統設定內，便可以使用該存取點上網。

下圖為 Airopeek 監控週遭無線網路通訊內容是所發現的無線網附存取點

(AP) 與無線網路工作站 (STA) 的實例。



Node	Type	Channel	ESSID	Retry Packets	WEP Packets	WEP ICV Errors	WEP Key	Cur. Signal	Bytes Sent	Packets Sent
00:00:00:00:00:00		11							0	0
UU:U2:2D:36:UF:97	STA	11		0	0	0		19	84	3
UU:U2:2D:37:7b:1b	STA	11		6	0	0		100	2,960	8
00:06:25:01:43:55	STA	11		0	2	0		81	728	2
00:07:0E:B9:7E:DB	STA	6		0	0	0		15	28	1
00:30:65:10:6B:6A	STA	1		0	0	0		16	637	13
UU:3U:65:1U:Al:71	STA	1		3	395	2	1	32	194,563	395
UU:3U:65:12:17:A7	STA	1		1	63	0		63	7,042	63
00:40:05:DE:59:99	AP	6	WP Wirel...	0	26	0		23	22,221	250
00:40:96:34:64:6E		6							0	0
UU:4U:96:4U:UA:18	AP	11	WP Wirel...	2	9	0		45	42,803	406
UU:4U:96:43:UE:4b	STA	1		57	162	0		45	40,203	184
00:40:96:49:78:93	STA	6		0	14	0		29	1,953	16
00:A0:F6:8A:A6:2A	AP	1	WP Wirel...	12	396	0		100	150,345	837
01:00:5E:7F:FD		6							0	0
U1:4U:96:UU:UU:UU		11							0	0
HcastATKZones:UU:UU:6B		6							0	0
HcastATKZones:00:00:F1		1							0	0
ATalk Ph2 Broadcast		1							0	0
Broadcast		1							0	0

圖 12 、Airopeek 探測週遭網路節點狀況實例

因為無線網路極容易遭受竊聽及盜用，我們強烈建議您使用加密的方式進行無線網路通訊以及身分認證。值得一提的是，有些管理員除了原本的認證方法外還會加上 MAC address 過濾的功能充當另一種身分認證方法。這種方法最大的問題就是 802.11 並未提供資料鏈結層加密的功能，因此所有的 MAC Address 都可以經由無線網路竊聽程式得到，因此這樣的身分認證方法可說幾乎形同虛設。

使用加密認證相關弱點與攻擊

如前所述，此種認證方法主要是使用於 WEP 的模式，在此模式下無線網路使用者 (Station) 與基台 (Access Point) 已透過其他的方式預先配給 WEP 所用的密鑰。然後兩者透過所謂的“挑戰與回應”(Challenge-Response) 的方法交換認證訊息。無線網路使用者先送出使用密鑰分享認證的要求給基台，基台回應給使用者一個接受此認證方法的訊息，此訊息中並包含一個 128bits 的亂數作為挑戰用訊息。使用者收到此訊息後，以預知的密鑰將此亂數加密並送回給基台驗證。基台驗證結果後決定此使用者是否通過。聰明的讀者此時可能已經發現這個認證方法存在一個可能的問題。此問題就出在基台回應給使用者挑戰用的訊息時並未加密，因此一個監聽無線網路的攻擊者就可以同時獲得未加密的原文與加密後的密文。這些資料非常有助於解密分析 (Cryptanalysis)，可以幫助攻擊者找出可能的密鑰或是解開其他加密過的封包。

因為這個認證方法依賴 WEP，因此在接下來的段落裡面，我們將會介紹三種關於 WEP 比較常見並且較具破壞力的攻擊方法。

第一種攻擊方法是採用窮舉或是字典式攻擊法去猜出使用者所選擇的密

鑰。第二種攻擊方法是在不知道密鑰的情況下利用 IV 被重複使用的問題來反向解出特定加密封包。第三種攻擊方法則是利用 RC4 決定密鑰演算法的漏洞，尋找具有特別特徵 IV 的封包，在收及足夠多資料後反向解出使用者所選的密鑰。

窮舉及字典攻擊法

所謂窮舉或字典式攻擊法指的是靠電腦的運算能力在有限的密鑰空間內將使用者所選的密鑰找出來。Tim Newsham 在這方面提出理論以及實作找出 WEP 亂數產生器的漏洞，並且成功地縮小有效密鑰空間 (Effective Key Space)，達成可以在極短時間內用強大的運算能力找到長度為 40 bits 的密鑰。Ian Goldberg 以及 UC Berkeley 的研究者也提出如何實行字典攻擊法以達成即時 (real-time) 解開加密後的無線區網資料封包。

窮舉攻擊法

管理者在選擇 WEP 所用的密鑰時，通常會用自選密碼當作密鑰，這個自選密碼會再透過一個亂數產生器產生真正用來加密的密鑰。Tim Newsham 發現這個亂數產生器所產生出來的亂數有瑕疵，這些瑕疵包括：

1. 管理者所輸入的字串會被映射到 32 bits 的空間 (原本的字串長度可以達到 40 bits)。
2. 映射結果每個位元組的第一個位元通常為 0，這又減少了 4 bits 的空間。
3. 用來作為亂數產生器的種子 (seeds) 每 2^{24} 次就會循環一次。

這樣的結果造成整個密鑰的可能性從 2^{40} 種可能減少到 2^{21} 可能性。對於使用窮舉攻擊法的攻擊者來說，卻是一個再好不過的消息了。Tim Newsham 的工具可以在幾分鐘之內反解找出 40bits 長度的使用者密鑰。不過對於 104bits 長度的使用者密鑰還是很難在可接受的時間內找到。

字典攻擊法

從 WEP 的運作原理可以看出，最終用來加密資料的密鑰是由使用者原先設定的密鑰以及一個三位元組長度的亂數所產生的。由於使用者原先設定的密鑰不變，而三位元組的長度大概只提供 2^{24} 種可能性。所以 Ian Goldberg 以及 UC Berkeley 的幾位研究者提出了字典攻擊法的可能性。所謂的字典攻擊法指的是攻擊者將所有可能的 IV 以及相對應的密鑰建成一個表(即字典)，如

此一來以後只要發現同樣的 IV，攻擊者即可馬上找出相對應的密鑰並且將加密後的密文解密。此攻擊的困難點在於攻擊者如何建立此字典。有幾個可行的方法包括攻擊者傳送已知內容的電子郵件，並且攔截接收此電子郵件的交通以建立字典，另外，攻擊者也可以藉由自己以太網路端傳送 ICMP 封包至無線網路端並且監聽無線網路的交通。

一旦攻擊者能成功地建立此字典，被當成目標的無線網路就等於沒有任何保護，攻擊者可以即時反解出經過 WEP 加密後的原文。

已知或猜測原文攻擊法

此攻擊法是利用一些已知或是可猜測的原始資料以及 WEP 重複利用 IV 的弱點來解出其他加密封包的密文。此攻擊方法首見於 Ian Goldberg 以及 UC Berkeley 研究人員的論文，Jesse Walker 也曾提出類似的攻擊方法。

首先我們先回顧一下 WEP 的工作原理：

WEP 基本上是一個對稱式加解密系統 (Symmetric Cryptography System)，亦即加密與解密是用同樣一個密鑰，原始密鑰的長度是 40 bits 或 104 bits。WEP 使用 RC4 PRNG (虛擬亂數產生器) 的演算法來產生實際加解密的密鑰，然後用 XOR 演算法作資料加解密的動作，以配合無線網路封包多變的資料長度。整個 WEP 的運作流程可以參考圖 13，至於詳細的說明請回顧本文資料保密的段落：

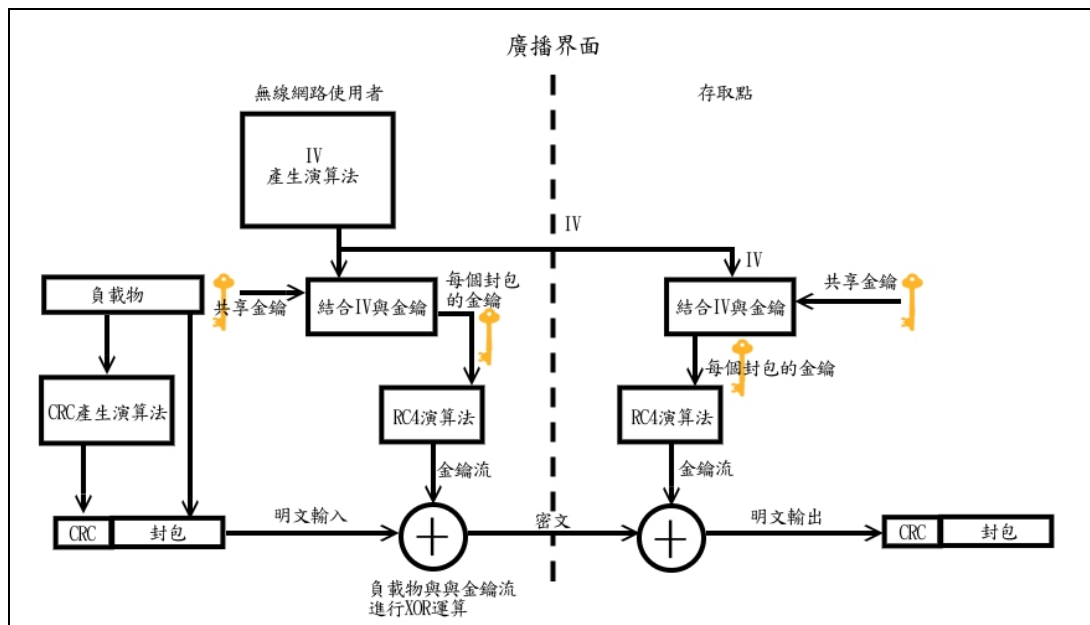


圖 13 、WEP 加密流程 (資料來源：NIST)

由於在 WEP 加密的方法中雙方的密鑰是共享的，透過一個 24 bit 長度的 IV (Initial Vector) 來共同產生真正用來加密的密鑰串流，所有的內容與這個密鑰串流進行 XOR 運算，變成密文後發送。

由於 IV 的長度過小，加上在某些系統的實作上不是使用亂數產生 IV 而使用循序方式產生 IV，因此我們可以發現一個事實：IV 總有一天會發生重複使用的問題。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。

此方法的原理是收集使用相同 IV 的封包，並且利用 XOR 運算的特性來反解出部分的資料。如同上一個攻擊方法，WEP 加密用的密鑰是靠使用者事先輸入的密鑰以及一個三位元組長度的 IV 來決定。由於使用者事先輸入的密鑰不會改變，因此一但攻擊者發現兩個或以上的封包具有相同的 IV 就可以確定這些封包是用同樣的資料串流進行加密。而 XOR 運算有一個特點，假設有兩個未加密的原文 P1 和 P2，兩者都用相同的密鑰 K 經過 XOR 運算後加密產生密文 C1 和 C2，則以下的數學運算式成立：

$$C1 \text{ XOR } C2 = (P1 \text{ XOR } K) \text{ XOR } (P2 \text{ XOR } K) = P1 \text{ XOR } P2$$

因此，如果攻擊者能夠猜到或知道 P1 的內容，並且攻擊者也截獲 C1 及 C2，則攻擊者可以輕鬆反解出 P2 以獲得另一個原文。事先猜到 P1 的內容除了如前一個字典攻擊法中所描述的以外，由於 TCP/IP 通訊協定中有許多的封包內容是可以預測的，我們可以考慮將常見的 TCP/IP 封包交通內容加以分析，把不變的部分找出來建立字典，然後再實行此攻擊。

密鑰弱點攻擊法

Scott Fluhrer, Itsik Mantin 以及 Adi Shamir 共同發現在 RC4 用來產生密鑰的演算法裡面的弱點，只要找到符合特定特徵的 IV，並且收集足夠多的資料樣本，就可以反推出使用者所指定的密鑰。

根據此篇論文，RC4 用來產生密鑰的演算法有數學上的漏洞，演算法產生密鑰時所作的運算有部分會仍然出現在最後所產生的密鑰裡，這類的密鑰在密碼學上稱為“弱密鑰”(Weak Key)。因此，只要攻擊者能收集到越多符合特定

特徵的資訊，找出原來使用者指定的密鑰的可能性就越高。

目前網路上有最少兩個工具—WEPCrack 與 airtsnort 可以用來進行此項攻擊。兩者的使用方法都是由攻擊者先進行網路交通的監聽，並且收集具有弱密鑰特徵的封包，之後就可以利用上述兩個程式將 WEP 密鑰在數分鐘的時間內反解出來。

此攻擊需要很大量符合特徵的封包—攻擊者往往需要監聽上百萬個 WEP 加密過的封包才能找到足夠符合特徵的樣本來破解密鑰。依照目標區網的網路通訊量的不同，要收集到這個數量的樣本需時可能少則一個晚上，多則長達數週才可完成。但是攻擊一但成功，原本的密鑰便不再具有保護的作用。

網路設備相關弱點

無線網路設備出廠時與其他的網路設備相同，有各種不同的管理介面例如，telnet, FTP, TFTP, WWW or SNMP。這些管理介面也會有一些預設的內定值如管理密碼等等，許多的管理者與使用者將網路設備當成家電般的隨插即用 (Plug and Play)，沒有更改系統內定的相關管理資訊；這些缺失可能造成攻擊者反客為主，獲得設備的管理權限，「幫助」管理者進行網路的管理。由於無線區網設備推陳出新，加上品牌以及產品眾多，因此這裡並沒有窮舉所有已知及未知的安全問題，但是重點在於管理者在採購無線網路相關設備時應該注意這些設備本身的安全議題以避免採購之後造成的困擾。

本節將介紹在無線網路設備常見的缺失，內容如下：

Telnet 管理介面

許多無線區網存取點都有提供 Telnet 為管理介面之一。優點是方便，簡單。可以用各種連接方式 (透過乙太網路或是 null modem) 來管理存取點。Telnet 服務最大的漏洞就是一切資料都未經過加密。因此攻擊者可能在公司的內部網路竊聽到管理者密碼並且加以利用。除此之外，已知 Cisco 無線區網基台的 Telnet 管理介面有阻絕服務式的漏洞，只要送出過長的字串可以導致無線區網基台自動重新開機。管理者需要將韌體升級到 11.21 以上的版本才能解決此問題。

TFTP 管理介面

Trivial File Transfer Protocol 是一個簡易的檔案傳輸協定。它的優點是方便好用，它的缺點是幾乎沒有安全性可言。只要知道檔案名稱及位置，不需任何使用者身份認證即可透過網路將檔案抓下來。因為 TFTP 的方便性，很多網路設備如路由器、交換器或硬體防火牆等都利用 TFTP 來傳遞設備所使用的設定資料。但是也因此產生許多安全問題。在無線區網存取點裡最有名的例子就是 D-Link 的 DWL 900 AP 存取點。這個存取點上有個手冊裡面沒有提到的 TFTP 伺服器存在，使用者或攻擊者可以從這個存取點上抓取所有的設定資料，包括 MAC Address 過濾器內容、管理者密碼、WEP 密鑰以及其他相關設定資料。由於 TFTP 不需要是先經過身分認證，因此任何人都可以抓取這些相關的設定資料。

WWW 管理介面

WWW 管理介面容許管理者直接透過瀏覽器管理遠端的網路設備。因為是圖形化介面又方便易用，所以許多管理者或是家庭使用者都會偏好使用 WWW 管理介面。WWW 管理介面的問題主要有下列幾種：

1. 出廠預設密碼未更改。許多的管理者沒有設定 WWW 管理介面的密碼，導致產品出廠預設的密碼仍然可用。此時攻擊者便有機可趁。
2. WWW 管理介面安全漏洞。各家產品所用的管理介面有不同的安全漏洞。Cisco 曾經有的漏洞是在 WWW 管理介面被管理者關掉後，攻擊者仍然能夠透過這個管理介面來做管理的動作。另一個較著名的漏洞則是 Linksys 的無線路由器，其 WWW 管理介面要求使用者身份認證，但是只要在預存取的檔案名稱後面加上“.xml”即可省略身分認證的步驟直接執行所有管理功能。

由於一般無線網路存取點都會被設定為內定的路由器，或者是每個存取點都有出廠預設的 IP 位置。因此攻擊者在使用 DHCP 取得 IP 位址後便可以開啟瀏覽器連線到路由器的 IP 位址上進行「管理」，或者是針對 WWW 管理介面的弱點進行攻擊。

SNMP 管理介面

Simple Network Management Protocol (SNMP) 也是方便網路管理者進行設備管理的一個協定，要利用此協定管理網路設備需要使用 SNMP 瀏覽管

理軟體。而 SNMP 這個通訊協定的認證依賴於 SNMP 社群字串(SNMP Community String)，這個字串相當於是使用者通行密碼一樣。

通常網路設備中有兩個預設的字串，一個供讀取資料使用，一個則具有存寫資料的權限。有經驗的網管都知道這兩個預設值；透過 SNMP 瀏覽管理軟體，如果設備所用的密碼還是出廠值的話，便可以進行設備組態的變更及設定。幾乎所有無線區網設備都具有 SNMP 管理介面。目前此方面已知的漏洞包括有下列幾項：

1. 預設管理密碼。如前所述，很多管理者常常忽略了更改管理密碼出廠預設值的重要性，如果這件事情被忽略，有時候可能造成重大的安全損失。
2. 資料外洩問題。有一些無線區網存取點的 SNMP 管理介面設計有問題，造成資料外洩的漏洞。這些資料可能包括管理者所用的密碼、WEP 密鑰、MAC 位置列表或者是 community string。
3. 非正規 SNMP 管理介面：SNMP 通常都使用 UDP 這個通訊協定以及通訊埠 161。如果有另一個 SNMP 管理介面使用通訊埠 27155，並且沒有紀錄在使用者手冊上的話那這等同於是後門一樣。此情況已經真實發生在所有由 Global Sun Tech 公司代工的無線區網存取點上。這個後門基本上暴露了所有關於此無線區網存取點的秘密資料。

預設管理密碼

許多的人都沒有修改預設的管理密碼，這些出廠的預設密碼都會詳細的寫在手冊之中。每一家廠牌的預設管理密碼都不同，但是如果沒有修改的話對於這些設備熟悉的攻擊者很容易就猜到你設備的密碼，並取得管理權。

緩衝區溢位攻擊

不要以為緩衝區溢位攻擊 (Buffer overflow) 只有在 IIS 上看得到，事實上無線區網存取點也是緩衝區溢位攻擊的受害者之一。緩衝區溢位攻擊常見的結果有三種，第一種是達成遠端控制的效果，攻擊者可以藉此漏洞來執行程式控制遠端設備。第二種是阻絕服務式的效果，攻擊者可能把此設備所提供的服務中斷。第三種則是無法預料的結果，意即結果可能是第一個或第二個，但是攻擊者無法預料。

目前已知最起碼 LinkSys 的一些無線區網路由器有緩衝區溢位的漏洞並且可能容許攻擊者執行任意程式碼，而 Buffalo 的無線區網存取器的漏洞則是

會導致阻絕服務的效果。由此可知緩衝區溢位攻擊也成為無線區網存取點漏洞的重點之一。

用戶端安全問題

本段落提了很多關於無線區網存取點的安全問題，但是並不代表無線區網用戶端就可以高枕無憂。因為在無線區網用戶端也存在幾個安全問題值得注意並且加以防範的。這些問題包括：

1. 用戶端密鑰儲存問題
2. 以偽造存取點攻擊用戶端

以下就分段一一說明。

用戶端密鑰儲存問題

既然 WEP 是使用對稱式加密系統，那麼用戶端的密鑰是如何儲存或管理呢？有一些無線網路卡是將 WEP 用的密鑰儲存在韌體裡面，可是有一些無線網路卡是將密鑰儲存在作業系統的 Registry 值裡面，然後僅僅將 WEP 密鑰做一些簡單的加密保護而已。目前網路上有公開的工具可以讓人輕鬆破解 Lucent/Orinoco 卡儲存在 Registry 裡面的 WEP 密鑰。

以偽造存取點攻擊用戶端

無線網路裡用戶端跟存取點之間的連線建立靠的第一個條件是服務域名 (SSID)。那麼如果今天同時有兩個無線區網存取點同時使用同樣的服務域名，那麼用戶端該跟哪一個建立連線？考慮預設的狀況下，用戶端會跟訊號較強的存取點建立連線。

利用這種原理，一個惡意的攻擊者可以偽造存取點騙取不知情的用戶端連線後從偽造存取點端對用戶端發動攻擊，因為很多用戶端電腦的保護可能不若其他重要電腦的保護來得完善，因此攻擊者可能利用一些常見的漏洞對無線區網用戶端進行攻擊並植入後門或木馬程式等等日後伺機破壞。這種攻擊尤其容易在公共場合例如咖啡館或是其他提供公共無線上網的場所。

其他的攻擊方式

前面提到目前已知的許多無線區網安全問題，從使用者身份認證、WEP 安全問題到無線區網設備漏洞。本段落將介紹幾個比較不常見或是攻擊難度高的安全漏洞。這些安全問題包括阻絕服務式攻擊與 Man-In-The-Middle 攻擊。

阻絕服務式攻擊

在無線區網中，Denial of Service (阻絕服務式攻擊) 可以用很多種方式達成。包括用實際的無線電訊號干擾 (2.4 Ghz 的室內無線電話即可)，實際破壞無線網路存取點的天線等方法。不過這裡要介紹的是因為無線區網通訊協定設計不良所導致的阻絕服務式攻擊。

由於無線區網不依靠實體佈線來傳輸資料，那麼無線區網要怎麼樣來維持存取點與用戶端之間的虛擬網路線呢？答案是無線區網存取點會與用戶端靠幾個特殊的管理封包來建立連結 (Association)。建立這個虛擬線路主要有兩大步驟，第一個是先做身分認證的動作 (Authentication)，第二個就是建立連結 (Association) 的動作。那既然有建立的動作就會有相對應的解除動作。在無線區網所用的通訊協定裡這兩個動作靠的是 Deauthentication 與 Disassociation 兩個封包。

設計者在設計這樣的通訊協定時並未將身分認證機制加進這些管理虛擬線路的封包裡面。這樣造成的問題是任何人都可以替無線區網存取點偽造這些管理封包然後切斷任意無線區網用戶端的連線。造成無線區網用戶端無法享有一個穩定的連線。同時這個設計缺陷也導致了我們接下來要提的 MITM 攻擊。

中間人(MITM)攻擊

Man-In-The-Middle (中間人) 攻擊方法是攻擊者處於無線區網用戶端與存取點中間，攔截兩者的通訊，並同時偽裝成無線區網存取點與用戶端的角色讓受到攻擊的用戶端與存取點在不知情的情況下繼續原有的通訊。

上一段提到無線區網通訊協定的設計瑕疵導致阻絕服務式攻擊。同樣的設計缺陷也可以讓攻擊者施行 MITM 的攻擊。首先攻擊者將無線區網用戶端的連線中斷，在用戶端嘗試再次連接存取點的時候攻擊者偽裝成存取點並同時對



台灣電腦網路危機處理暨協調中心(TWCERT/CC)

E-mail: twcert@cert.org.tw

Tel : 07-5250211

Fax : 07-5250212

Tel : 02-23563303

Fax : 02-23924082

原有的存取點偽裝成用戶端，此時攻擊者已成為中間代理者的角色，所有通訊都會經過這個攻擊者，而攻擊者可以任意更改這些通訊的內容。

增進無線網路安全的方法

很幸運的，除了在那些如山高又讓人困惑的管理文件以外，對於無線網路的管理者而言的確有一些技巧可以有效的增進網路的安全性。即便有許多問題是出自於整體協定設計的疏忽、是先天體質的問題，但是「有燒香、有保佑」—有這麼多不設防的無線網路基地台可以利用，那些以掃描為樂的駭客們願意花時間心血來專門搞破壞的可能性會大大的降低；如果您真的覺得在您網路中的資料重要到你不願意冒任何一絲的暴露風險，那麼您一開始就不應該考慮使用無線網路。無論如何，任何網路設備都有一定的風險，只要能保持『防禦縱深』的原則，就能夠合理地降低風險並與企業目標達到平衡。

以下我們針對各種可能的技術方案進行探討：

修改預設的設定

您可以想像得到機器出廠以後有多少的預設值需要更動嗎？這些預設值往往是入侵者可以運用的資訊，而且這些嘗試通常都是您的網路陷入入侵者手中的第一個警訊以及防禦的第一道防線。

預設的密碼

不論是無線網路基地台或者是其他的電腦設備，出廠時都預設了管理所需的密碼—有些廠商使用空字串作為密碼，有些使用簡單的字串如“admin”、“administrator”等等；這些密碼都可以在說明書中找到，並適用於同廠牌所有的設備。其他廠商的做法則是將密碼設成與設備流水號相同，不論如何，為了認證使用者的權限，這些設備必須設定密碼以確定使用者權限。

然而使用者在使用這些網路設備時往往沒有修改內定的密碼，使得有心人士很容易的可以取得這些設備的管理權限。我們建議您應該更改設備的管理密碼，使用至少八碼的密碼並且夾雜特殊符號，避免使用英文姓名或是出生年月日，才能有效保護設備的安全性。

大部分的系統都至少有 telnet 管理介面、Web 管理介面以及廠商專屬管理軟體等等不同的管理方式，請注意這些介面的密碼通用情形並且重設管理密碼。

預設的 SNMP 社群碼

絕大部分的網路設備都支援 SNMP (Simple Network Management Protocol) 網路管理協定，這個協定允許管理軟體遠端擷取網路設備的資料並且加以分析，甚至可提供管理軟體更動網路設備的設定值。

在 SNMP 網路管理協定中透過 SNMP 社群碼 (SNMP Community String) 來識別使用者權限，通常廠商出廠預設值為 “public” 與 “private”，擁有不同的管理權限。

如果您的網路設備支援 SNMP 網路管理協定的話(請參考網路設備的手冊)請您修改預設的 SNMP 社群碼，如果可能的話設定存取列表 (Access Control List) 限定可存取 SNMP 資訊的 IP 位址。

最省事的方式是：如果你不確定是否需要這項功能的話，關掉它，同時並確定設備上沒有其他在非標準通訊埠上執行的 SNMP 管理介面。

預設的 SSID

通常在無線網路基地台出廠時為了方便使用者使用，都採取開放式系統認證的方式為預設組態，使用者只要將網卡插上就可以馬上找到基地台並且建立連線。此外，各家廠商的預設 SSID 諸如 Cisco 的 “tsunami”、D-Link 的 “Default” 等等視廠商的喜好而有所不同。

如果您的無線網路不提供給非特定的大眾使用的話，建議將認證方式修改為不廣播 SSID 的封閉系統認證方式 (Closed-system Authentication)；為了避免他人的誤用，例如有人家中用同型的無線網路基地台預設值而不小心使用到您的網路，建議同時修改預設的 SSID。

預設的通訊頻道

預設的通訊頻道對於網路安全的威脅並不大，但是它可能導致您與您的鄰居的無線網路基地台彼此爭奪通訊頻道，而造成服務阻絕的狀態 (DOS, Denial of Service)。

造成這個狀況的原因是由於無線通訊設備有其分配的頻帶，這些頻帶在 802.11b 網路裡面被切為幾個通訊頻道，如果發生頻道衝突的情形會造成衝突的這些網路基地台發生通訊異常。但是，同一廠牌的出廠預設值往往相同，所以我們必須將通訊頻道調開以避免通訊頻道衝突的狀況發生。

修改網路設計

DHCP 伺服器的使用

DHCP (Dynamic Host Configuration Protocol)是一項非常方便的服務，只要網路服務提供者提供這項服務，網路的使用者便可以讓自己的電腦自動的取得 IP 位址、子網路遮罩、預設閘道器、網路名稱伺服器以及其他的一些額外資訊。換一個角度來說，未授權的使用者也不需要對您的網路組態下太多的功夫，只要如法炮製也可以自動的連線到您的無線網路上。

如果您的無線網路規模不大，可以考慮用靜態的 IP 配置來進行管理；如此可避免 DHCP 伺服器洩漏網路設定相關的參數。這種方法會犧牲一些無線網路的方便特性，如無線網路漫遊以及 Ad hoc 資源分享等等，並不適用於大型的網路。此外，如果碰到真正有心的入侵者使用監聽器 (sniffer) 分析無線網路流量，這項防護便會失效。

使用適當的加密技術

WEP 加密協定有一些先天設計上的問題，這些問題可能導致在無線網路上傳輸的資料洩漏；但是選用較長的金鑰的確有助於資料的保密。建議您使用網路設備可以使用的最長金鑰，一般可以選擇的選項有：不加密 (Disable WEP)、40-bit WEP 以及 104-bit WEP 三種方式。

使用 WEP 需要注意：

1. 網路產品的相容性問題

有些產品在採用 WEP 相連時會有不相容的狀況產生，造成無法連線。

2. 傳輸速率可能下降

由於加解密都需要使用系統的資源，尤其在基地台端要應付所有的用戶端的解密，因此在使用 WEP 時可能遇到傳輸速率下降的問題。

3. 基地台加密功能限制

許多系列產品在外觀上與控制軟體上都採用相同的設計，僅僅在無線網路基地台的網路卡上有所不同；因此需要注意基地台最大支援到多少 bit 的 WEP 金鑰長度。

此外需要注意的是，將加密金鑰加長雖然有助於資料的保密，但是有些攻擊方式是與金鑰長度無關，建議您若情況許可，最好能定期更改 WEP 金鑰。另外如果廠商有提供非 IEEE 標準的加密功能，最好是測試過相容性與安全性後再使用。

網路卡號管理

大部分的無線網路基地台都可以設定僅僅接受某些卡號的連線，網路卡必須先由管理者註冊後方可使用該無線網路基地台。

使用這種管理方式可以有效阻擋未授權的使用—即使對方知道您的 SSID 以及 WEP 密碼，只要卡號沒有出現在名單中就無法使用無線網路。

這種方式的問題在於，網路卡卡號是可以偽造的！！有心人士可以利用監聽程式監聽無線網路的流量，找出可以連線的卡號並利用這些卡號上網。

防火牆區隔網段

許多的無線網路使用者直接將無線網路基地台放置在公司內部網路方便大家使用，這是一個相當危險的組態方式。由於無線網路很難進行使用者的控管授權，一般建議將透過無線網路連上的主機均視為不信任的主機。無線網路的管理應該比照其他遠端連接網路 (remote access network) 例如撥接網路，的管理方式來管理。

因此，建議將無線網路利用防火牆隔離成一個網路區段，對於由無線網路進入公司內部使用資源的行為進行控管，同時應視公司安全政策，調整無線網路隔離區段可使用的公司內外網路資源。

802.1x 使用者認證

IEEE 802.1x 於 2001 年七月獲 IEEE 核可，是目前無線網路上最理想的身分認證與密鑰管理協定。透過 802.1x 能將無法通過認證的使用者隔絕於網路之外，使其無法利用任何網路資源。目前生產的無線網路基地台已有越來越多支援 802.1x。但在使用者方面，除 Windows XP 支援 802.1x 外，其餘作業系統目前均無提供，需要外掛程式支援。

在 802.1x 架構下有幾個主要的角色：

Authenticator :

要求並且接受未受信任端網路節點的認證請求的實體。

Supplicant :

請求網路存取權，並且需接受 Authenticator 的認證稽核。

Port Access Entity(PAE) :

具有存取埠的一個實體，具有 Authenticator, Supplicant 或兩者的功能。

Authentication Server :

對 Authenticator 提供身分認證服務的實體，可能與 Authenticator 存在同一主機內，但大多數的狀況下是一台獨立的伺服器。

其角色分工如下圖所示。

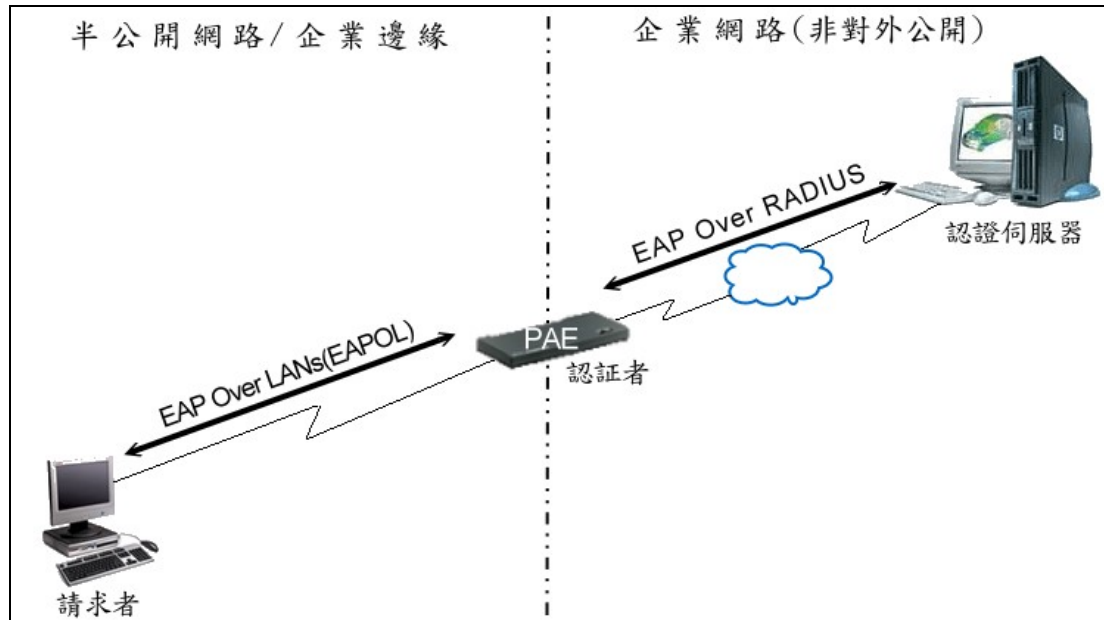


圖 14、802.1x 網路拓譜

802.1x 身分認證可以分為幾個大階段：

1. Supplicant 向 Authenticator 提示身分

這個階段中 Supplicant 向 Authenticator 提出連線要求，Authenticator

此時會向 Supplicant 要求提示身分，Supplicant 將身分交與 Authenticator。

2.Authenticator 向 Authentication Server 要求使用權

這個階段中 Authenticator 確認 Supplicant 的身分後，向 Authentication Server 提出身分認證的要求。

3. Authntication Server 提出挑戰/回應要求

Authentication Server 收到要求後，提出一個挑戰給 Authenticator，Authenticator 轉交給 Supplicant；Supplicant 根據這個挑戰字串提出相對應的回應交予 Authenticator，再轉至 Authentication Server。

4.Authentication Server 接受/拒絕認證請求

Authentication Server 根據 Supplicant 的回應，決定是否接受認證的請求。

詳細的流程如下圖所示：

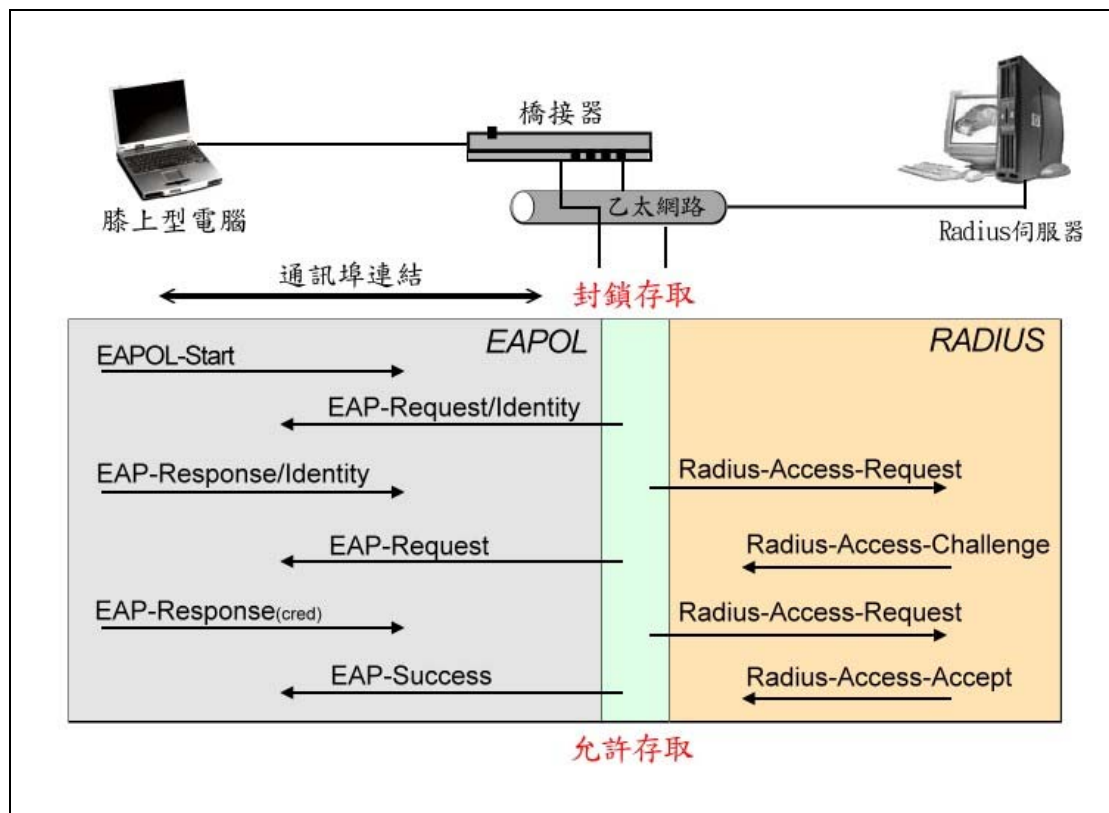


圖 15、802.1x 應用於 802.11 網路

資料來源：Bernard Aboba, Wireless LANs: The 802.1X Revolution

802.1x 可以有效的補強 802.11 無線網路對於使用者認證缺乏彈性的缺點，對於存取的控制以及個體的身分確認提供一個有效可行的方案。但是要確記如果未使用雙向認證 (Mutual Authentication) 的方式 (例如用戶端身分憑證或智慧卡)，則即使使用了 802.1x 還是可能遭受 MITM 的中間人攔截攻擊。而若使用 802.1x 與 WEP，則利用 802.1x 自動定期更新 WEP 密鑰的功能也是保護無線區網的重要一環。

VPN 的使用

由於 802.11 網路的使用者身份辨識及授權有許多的風險存在，一般均建議將其隔離於防火牆的特殊網段內；此外為了補強 WEP 的弱點以及加強使用者認證功能，於是將 VPN 與 802.11 網路整合成為一個實務上相當可行且有效的解決方案。

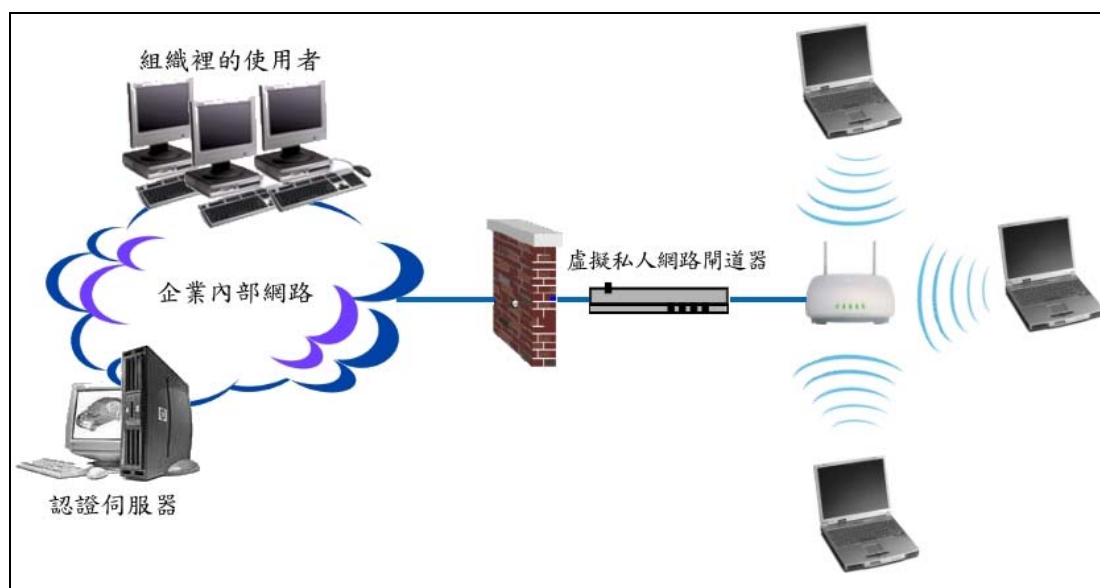


圖 16、VPN 應用於無線網路

在這種架構上所有的無線網路工作站 (STA)需要先行與 VPN 開道器進行身分確認，並且建立一個加密的連線。VPN 的身分認證方式較 802.11 網路更加的完善與多樣化，例如支援動態密碼及其他生物辨識技術，足以有效識別使用者身份；而 VPN 內建的加解密功能相較於 WEP 更加的具有彈性，可以抽換不同的加解密模組。

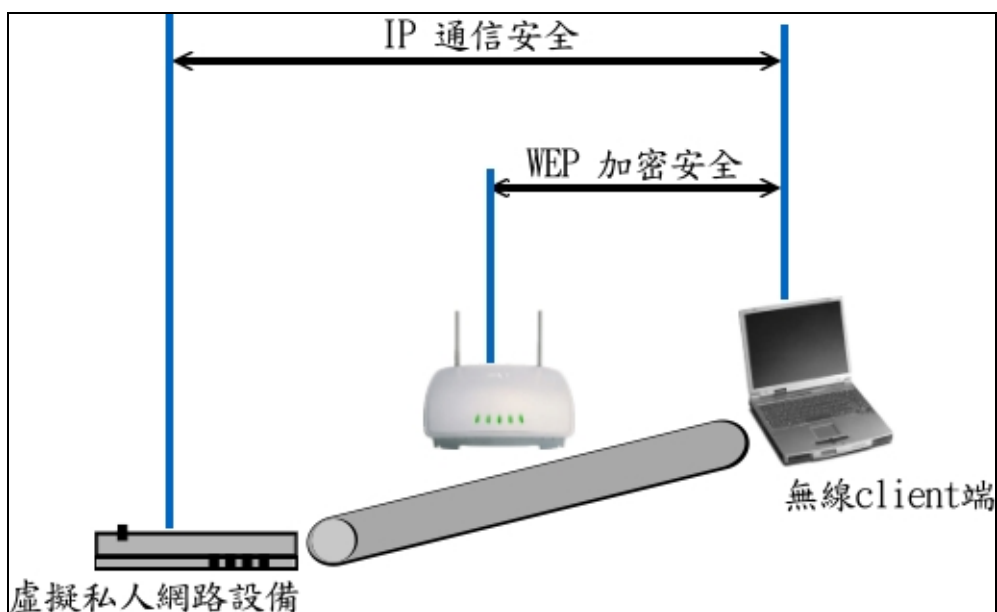


圖 17、VPN 與 WEP 安全的關係

如此解決了 802.11 使用上主要的問題,也是目前已知較完善的解決方案。

相關管理措施

除了技術管理以外，對於無線網路相關的管理措施也可有效提升組織內部網路之安全性，相關管理措施分述如下。

制定無線網路安全政策

授權無線網路使用

組織或機關必須制定無線網路使用之授權標準，包括可使用無線網路人員授權方法以及無線網路實體使用範圍，例如僅能於會議室中使用無線網路、僅有取得相關主管授權者可使用無線網路等。

此外由於無線網路容易遭受竊聽破解，因此必須針對無線網路上傳輸之資料機密等級進行規範，嚴格執行。

確認無線網路活動範圍

組織或機關必須針對內部資訊財產進行標記，限制無線網路可存取之資訊資產內容及範圍，以免遭受入侵造成損失。

確認無線網路相關安全操作標準

對於無線網路安全所必須遵守之安全控制明定管理條文，並列出使用無線網路之各種狀況所需符合之安全標準，例如加密機制的使用、安全控管方式等等。

確認無線網路管理權責

組織或機關必須確認無線網路設置、設定及管理之管理權責，並依照管理規定，定期稽核清查。

無線網路設備清查

無線網路基地台清查

無線網路基地台清查目的在於防止公司內部網路私設未經核准之無線網路基地台，確認各基地台皆依照公司安全政策正確地組態，以預防未經授權之人員盜用網路資源。

本方法可以找出公司內部未經授權裝置的基地台，避免未經授權之存取內部網路資源，此外清查基地台可以找出內部偽裝之無線網路，有效避免中間人 (MITM) 攻擊。

無線計算設備清查

無線計算設備機動性極高，通常是個人數位助理 (PDA)、筆記型電腦等等移動式計算設備，因此也較容易遺失或者失竊。

由於失竊的無線計算設備上可能儲存有重要的資訊，例如 WEP 加密金鑰、內部通訊 SSID 列表等等，而且極可能可以直接使用內部無線網路，因此無線計算設備的遺失可能造成極大的安全威脅，因此應定期清查內部之無線計算設備。

無線網路安全應變與稽核

無線網路安全應變機制

組織或機關必須明定無線網路安全通報及應變機制，例如無線計算設備失竊或遺失時之處理準則、遭受入侵時之通報及處理方式等。

無線網路安全稽核

組織或機關必須定期對內部無線網路安全狀況進行安全稽核，包括弱點掃描以及其他管理稽核。

結論

企業在導入無線網路前需參考組織之安全政策，評估無線網路所傳輸資料之敏感性以及資料完整性需求，在安全性、方便性以及成本之間評估取得其平衡點。

在使用無線網路時應先修改無線網路基地台之設定，避免使用原廠的預設設定值；並且參考組織內之資訊系統安全政策調整網路組態設計，視需要導入 802.1x 使用者認證機制或者 VPN 來加強無線網路安全性。

由於無線網路的存取控制機制不甚完善，我們建議在使用無線網路時應先了解無線網路基地台所提供的種種安全認證機制以及其弱點，並且採取相對應的安全防護措施。本文針對無線網路的認證措施及安全措施，以及這些措施中存在的弱點進行詳細的介紹，並且對於網管人員在技術上可行的修正提出可行的解決方案。

參考資料

1. IEEE 802.11-1999 Standard
2. J. Philip Craiger , 802.11, 802.1x, and Wireless Security
SANS Reading Room
3. Jorgen Ellingson , Layers One & Two of 802.11 WLAN Security
SANS Reading Room
4. Tom Karygiannis, Les Owens,
DRAFT: Wireless Network Security 802.11, Bluetooth™ and Handheld Devices
<http://csrc.nist.gov/publications/drafts/draft-sp800-48.pdf>
5. Nikita Borisov, Ian Goldberg, David Wagner, “Intercepting Mobile Communications: The Insecurity of 802.11”
<http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>
6. Jesse Walker, “Unsafe at any key size: An Analysis on WEP Encapsulation”
<http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip>
7. “Your Wireless Network has No Clothes”,
<http://www.cs.umd.edu/~waa/wireless.pdf>
8. Arunesh Mishra and William Arbaugh, “An Initial Security Analysis of the IEEE 802.1X Standard”, <http://www.cs.umd.edu/~waa/1x.pdf>
9. Tim Newsham’s web page about WEP problems:
<http://www.lava.net/~newsham/wlan/>
10. Adam Stubblefield, John Ioannidis, and Aviel Rubin, “Using the Fluhrer, Mantin, and Shamir Attack to Break WEP”,
http://www.cs.rice.edu/~astubble/wep_attack.pdf
11. David Hulton, “Practical Exploitation of RC4 Weaknesses in WEP Environments”, <http://www.dachb0den.com/projects/bsd-airtools.html>
12. Wireless Sniffers List:
<http://www.personaltelco.net/index.cgi/WirelessSniffers>
13. IEEE 802.1X
<http://standards.ieee.org/getieee802/download/802.1X-2001.pdf>
14. Enterprise Deployment of IEEE 802.11 Using Windows XP and Windows 2000 Internet Authentication Service,
<http://www.microsoft.com/windowsxp/pro/techinfo/deployment/wireless/default.asp>



15. HOWTO on EAP/TLS authentication between FreeRADIUS and XSupplicant, <http://www.missl.cs.umd.edu/wireless/eaptls/?tag=missl3>
16. HOWTO: EAP-TLS Setup for FreeRADIUS and Windows XP Supplicant, <http://www.denobula.com/EAPTLS.pdf>
17. Unofficial 802.11 Security Page, <http://www.drizzle.com/~aboba/IEEE/>
18. Wireless LAN 802.11b Security FAQ, http://www.iss.net/wireless/WLAN_FAQ.php

作者介紹

林秉忠

畢業於中央大學資管系及中山大學資管所，於 1997 年協助陳年興教授成立台灣電腦危機處理中心。曾任台灣電腦網路危機處理中心技術組研究員兼任執行秘書，對於電腦網路、主機管理以及網路安全相關議題具有十年以上之實務經驗，並取得 CISSP 專業認證資格；專長為風險評估、電腦網路技術稽核、入侵事件調查處理以及滲透測試等。

曾於 2001 年七月美國拉斯維加斯舉行之國際駭客年會 DefCon 9 主持會議並發表論文，著有 2000 年台灣地區網站安全調查報告以及 2001 年台灣地區網站安全調查報告，為目前各界引用網路安全現況數據之重要來源。

陳彥銘

陳彥銘目前在 Foundstone 資訊安全公司擔任資深顧問。他的專長在無線網路安全、Web 應用程式安全測試、產品安全測試、入侵偵測系統與攻擊滲透測試。他在管理 Unix 與各種相關網際網路服務有四年多的經驗，並且對於無線網路、密碼學、入侵預防、電子投票與網路存活方面有豐富的知識與研究。他同時也是多本暢銷書的作者群之一。這些書包括：Hacking Exposed 3rd ed., Hacking Exposed for Web application 以及 Windows XP Security。

他同時也是各種會議的常客，除了擔任 Ultimate Hacking 系列課程講師以外，他曾擔任 Global Knowledge Webinar 的講師以及 MISTI 資訊安全會議的講師。他的文章曾發表在 SysAdmin, UnixReview, DevX, PCWeek 以及網路通訊雜誌。今年六月到九月間他才剛在網路通訊雜誌上發表一系列關於無線網路安全一題的文章。

在加入 Foundstone 之前，他曾在卡內基美隆 (CMU) 的 CyberSecurity 中心擔任研究人員，從事與 Agent-based 入侵偵測系統相關研究。他也曾參與開放軟體“snort”的相關發展，開發了分析事件的相關工具。他在 CMU 的碩士論文是與分析財務金融網路存活能力為主題。

陳彥銘由國立中央大學數學系畢業，並取得卡內基美隆 (CMU) 資訊網路科學碩士。他擁有的專業證照包括 CISSP 與 MCSE。