Module 14:無線網路安全

學習目的

- 本模組介紹無線網路可能遭遇的攻擊，無線網路802.1x標準，WEP安全技術及風險與組織如何架設、管理一個具安全性的無線網路。
- 本章利用四個小節介紹
  (1) 無線網路技術:包括WLAN 標準、傳輸安全技術及身份認證
  (2) 無線網路安全問題:包括WLAN偵測、竊聽及攻擊
  (3) 架設安全無線網路:考慮存取點安全、傳輸安全、客戶端安全及伺服端安全，透過原理解說，提供同學對無線網路安全有一整體性的認識。
  (4) 專案實作: 實際以無線網卡及無線基地台(AP)建置一無線網路環境。
- 建議14-1~14-3使用三個鐘點教授， 14-4專題實現作可作為學生的homework

Module 14:大綱

Module 14-1: 無線網路技術(*)

Module 14-2: 認識無線網路的安全問題(**)

Module 14-3: 架設安全的無線網路(*)

Module 14-4 專案實作(*)

附錄一:IEEE802.11標準

ul

* 初級(basic):基礎性教材內容
** 中級(moderate):教師依據學生的吸收情況，選擇性介紹本節的內容
*** 高級(advanced):適用於深入研究的內容

u1

* 初級(basic):基礎性教材

**中級(moderate):教師依據學生的吸收情況，選擇性介紹本節的內容

***高級(moderate):適用於深入研究的內容

user, 2007/2/14

Module 14-1: 無線網路技術

14-1 無線網路技術

- 1997 年6 月IEEE802.11 正式公告，將無線區域網路以乙太網路(Ethernet)為基礎作為標準，使用2.4GHz 頻段定義介質存取層和實體層之功能規範。
- 實體層要求DSSS (Direct Sequence Spread Spectrum,直接序列展頻) 產品之資料傳輸速率2Mbps，而FHSS (Frequency-Hopping Spread Spectrum,跳頻式展頻)產品之資料傳輸速率1Mbps。
- IEEE802.11 促成了區域網路不只在軟體上能擴展至Internet，且在硬體上亦將朝向「無線」之方向發展。

14-1 無線網路技術

- IEEE802.11標準歷經七年方始制定完竣，其功能在於：
  - 確保使用技術之成熟穩定性,該項標準之委員會係由來自全球40 個知名廠商共同研究，彙整所有之技術並經投票後決定。
  - 解決相容性問題，原先DSSS、FHSS及IR (Infrared,紅外線) 等三種技術，其產品間僅能同類間相通，而802.11 則解決其相互間不相容之問題。
  - 無線網路之優勢包括安裝程序簡易，省卻網路之佈線工程，可漫遊，亦不必更動現有網路架構和可跨越數棟大樓之傳輸能力，具有替代T1 專線之功能，解決區域網路受限於100 公尺及佈線死角之問題外，更把網路之應用延伸到室外。

14-1 無線網路技術

- IEEE 802.11 指的是電子電機工程師協會（Institute of Electrical and Electronics Engineers ，IEEE）這個國際組織所於1997 年制定出來的一套在無線區域網路環境下作業的一個通訊協定標準
- 目前無線區域網路都是遵循IEEE802.11標準在運作，由於已不敷使用
  - 於1999 年制定IEEE802.11b(頻道為2.4GMHZ 速度11M bps) ，及IEEE802.11a (頻道為5GMHZ 速度54M bps)
  - 2003 年制定IEEE802.11g(頻道為2.4GMHZ 速度54M bps)

14-1 無線網路技術

- 802.11 是一項被設計用來進行長距離或高速數據資料傳輸的技術，資料傳輸也具有全方位的傳輸特性，即沒有所謂角度或方向性的限制，並且能夠穿透障礙物而完成資料傳輸的工作，非常適合在辦公室的環境下使用。

- 只需在公司內部架設一個無線橋接器（Access Point），則在其有效發射範圍內，就可以跟裝有無線網路卡的電腦達到網路連線的目的。

- 這對於用在一般上網、資料傳輸工作來講，其實已綽綽有餘，而且對行動式的工作者來說，也能解決傳統有線網路環境下的限制。

14-1 無線網路技術

- 802.11 極適合用於在原有的有線區域網路（LAN）下作延伸的佈局，亦或是完全取代現有的有線區域網路，因其可架構出與有線區域網路完全相同的功能。

14-1 無線網路技術

三種規格的差異性：

	802.11b	802.11a	802.11g
使用頻譜	2.4 GHz	5 GHz	2.4 GHz
傳輸速率	11 Mbps	54 Mbps	54 Mbps
傳輸距離	115 ft	22 ft	42 ft

14-1 無線網路技術

- 802.11a其傳輸速率最高可達54Mbps，但因其為受管制的5GHz頻譜及其傳輸距離較802.11b的115ft來得短(802.11a為22ft)，若要將其使用率提高，在實質面上是比較困難的，但也因為5GHz這頻譜波段比較不易受到干擾，所以相較之下802.11a仍具有其優勢。
- 802.11g的傳輸速率和802.11a一樣為54Mbps，而其波段與802.11b同為2.4GHz，使用2.4GHz波段不需要經過申請相當的方便；在相容性上，802.11g與802.11b是可相互相容的，這讓企業在建制新通訊標準時可大幅的減少相關成本。
- 相同的54 Mbps傳輸速率，802.11g的傳輸距離比802.11a更遠，因此兩相比較下802.11g極具優勢。

14-1 目前的無線網路技術

- 本節的內容如下：

  Module 14-1-1: 標準架構

  Module 14-1-2: 傳輸安全

  Module 14-1-3: 身份認證的改進

14-1 目前的無線網路技術

- 上述所提的標準(802.11x)允許工作站和無線存取點之間，使用高達11~54Mbps的傳輸速度建立連線，接著再和有線LAN或其他工作站連線（詳見圖14-1）。
- 無線區域網路標準最主要是做為連線時的身份認證資訊的交換和資訊加密。

註:在這裡所說的802.11X，泛指802.11b、802.11a、802.11g 、802.11n等802.11系列標準。

14-1 認識目前的無線網路技術

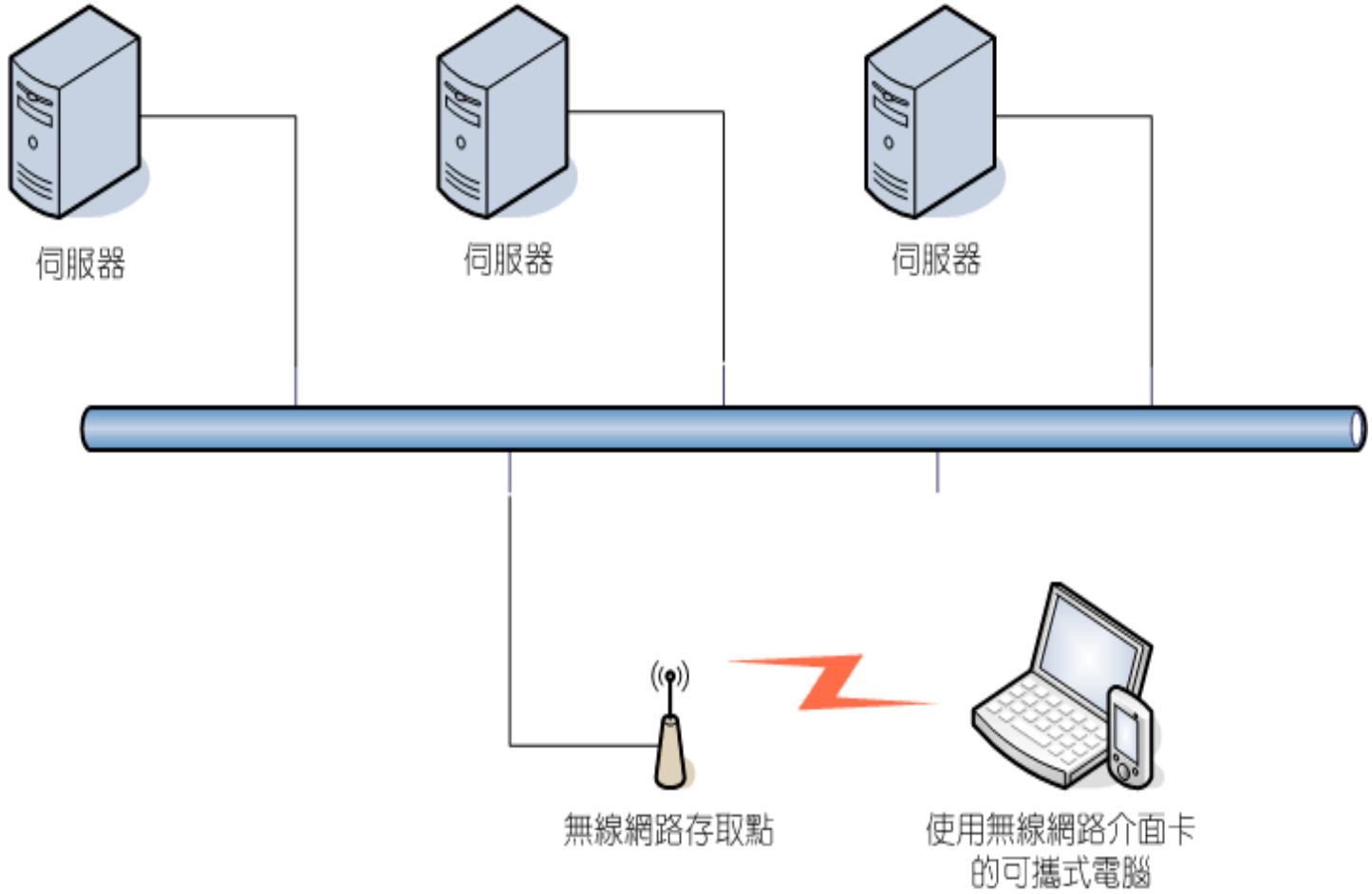

圖14-1 典型的無線網路架構

返回

Module 14-1-1: 標準架構

14-1-1 標準架構

- 為了讓組織更有效地使用無線區域網路（wireless LAN，WLAN），無線信號的涵蓋範圍必須完整地涵蓋員工或訪客放置電腦的區域。
- 室內：
  - 典型的802.11x WLAN有效涵蓋範圍大約是150英尺。
- 室外：
  - 涵蓋範圍大約可達1500英尺。

14-1-1 標準架構

- 無線區域網路可以依照網路通訊拓樸區分成兩種：
  - 簡易模式(Ad hoc Mode)
  - 基礎建設模式(Infrastructure Mode)
- 簡易模式的存取方式不需要透過存取點（access point，AP），而是採用點對點(peer-to-peer)的傳輸方式(詳見圖14-2)。
- 基礎建設模式則是透過存取點(AP)來將所有的用戶連結，資料由類似乙太網路(Ethernet)中集線器(Hub)的中繼站(Relay)來接送(詳見圖14-3)。以下介紹基礎建設模式。

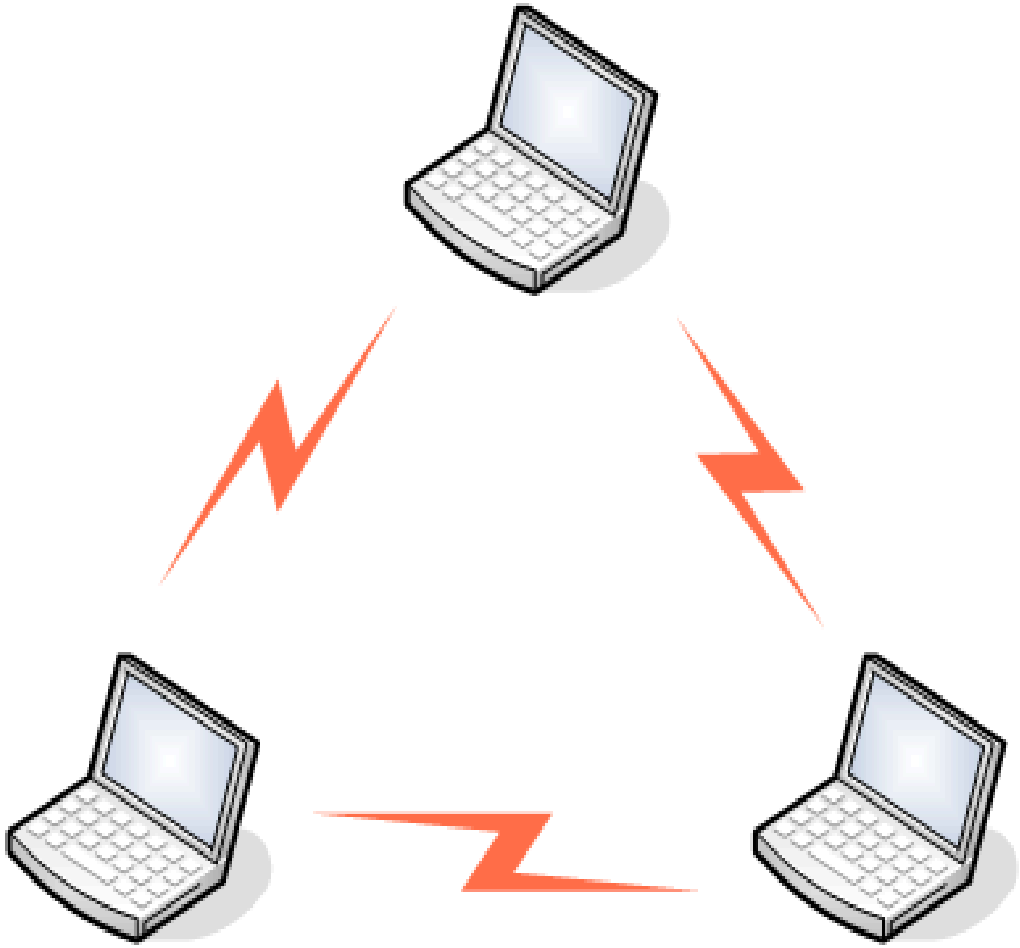

圖14-2 無線區域網路-簡易模式

返回

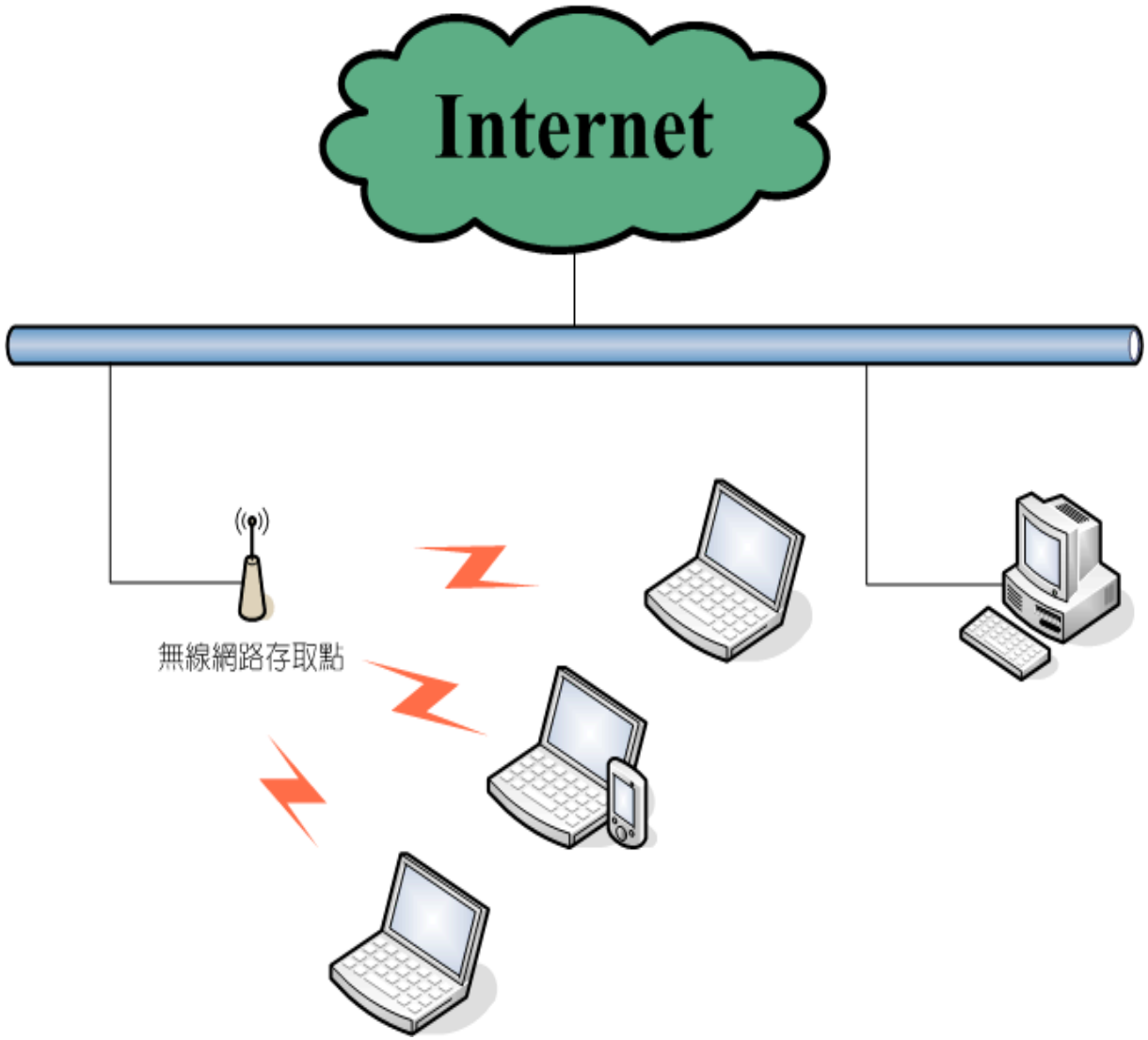

圖14-3 無線區域網路-基礎建設模式

返回

14-1-1 標準架構

- 基礎建設模式運作
  - 存取點必須在AP的涵蓋範圍內。
  - 在無線網路的架構中，一般都會含有提供IP位址的DHCP (Dynamic Host Configuration Protocol)伺服器，以及其他讓工作站可以連結上網路通訊所需的資訊。
  - 這些資訊架構允許可攜式電腦隨意漫遊且無須特別留意，也照樣可以在WLAN進行溝通。

Module 14-1-2: 傳輸安全

14-1-2 傳輸安全

- 由於WLAN是以無線電訊號做為傳送和接收資訊的媒介，所以只要位於訊號範圍內的工作站皆可接收到信號，因此，傳輸安全對整個系統的安全格外顯得重要。
- 在工作站和AP之間，如果沒有適當的機制來保護資訊的機密性和完整性，將會產生資訊是否遭到侵害、入侵者是否已經偽裝成工作站或AP等疑慮。
- 802.11x標準在透過WLAN傳送資訊時，將以有線設備隱私（Wired Equipment Privacy，WEP）協定來確保資料傳送封包的安全。

14-1-2 傳輸安全

- WEP三種基本的服務如下：
  - 身份認證
  - 機密性
  - 完整性

身份認證

- 802.11 安全防護及認證的相關措施可分為使用加密方式的挑戰與回應 (Challenge-Response) 認證方式，例如AP使用RC4演算法加密方法及使用交互換認證的挑戰／回應系統（詳見圖14-4）。
  - 使用者先送出使用身份認證的要求給基台，在使用開放式身份認證系統的過程中，工作站是以服務辨識碼(SSID)或MAC位址做為與AP初始交換的身份認證回應。
  - 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。
  - 基台驗證結果判斷是否為合法使用者，並決定是否讓使用者連結進入網路。

身份認證—服務辨識器

- 服務辨識器（Service Set Identifier，SSID）是一種做為網路名稱的32位元組字串。
- 工作站和AP都必須擁有相同的SSID才能順利地連結。
- 如果工作站若沒有適當的SSID，也就無法順利地連結進入網路。
- SSID是透過許多AP進行廣播，當SSID 在傳送時，其資料是沒有經過加密的文字型態，因此只要透過無線網路分析器，即可從資料封包中找出基地台的SSID 。
- 雖然某些AP可以將預設的SSID廣播予以關閉，但忽略了傳輸安全機制，駭客依然可利用流量監聽的方式判斷出SSID。

身份認證—MAC位址

- 某些AP允許工作站使用MAC位址做為身份認證的方式，在這種組態類型之中，AP設定成只能和預設認可的MAC位址進行通訊。
- AP認可的合法MAC位址，是經由管理員將認可的MAC位址加入到設備的存取列表(ACLs)之中。
- 802.11 標準中要求MAC 位址以不加密的字元傳送，因此駭客可直接經由監聽無線網路，取得一合法的MAC 位址。

身份認證

- 如果入侵者經由監聽網路訊息流量取得已經授權的SSID 或MAC位址，並將自己的系統設備設定為此合法的MAC位址，那麼入侵者也可以和AP進行通訊。

身份認證

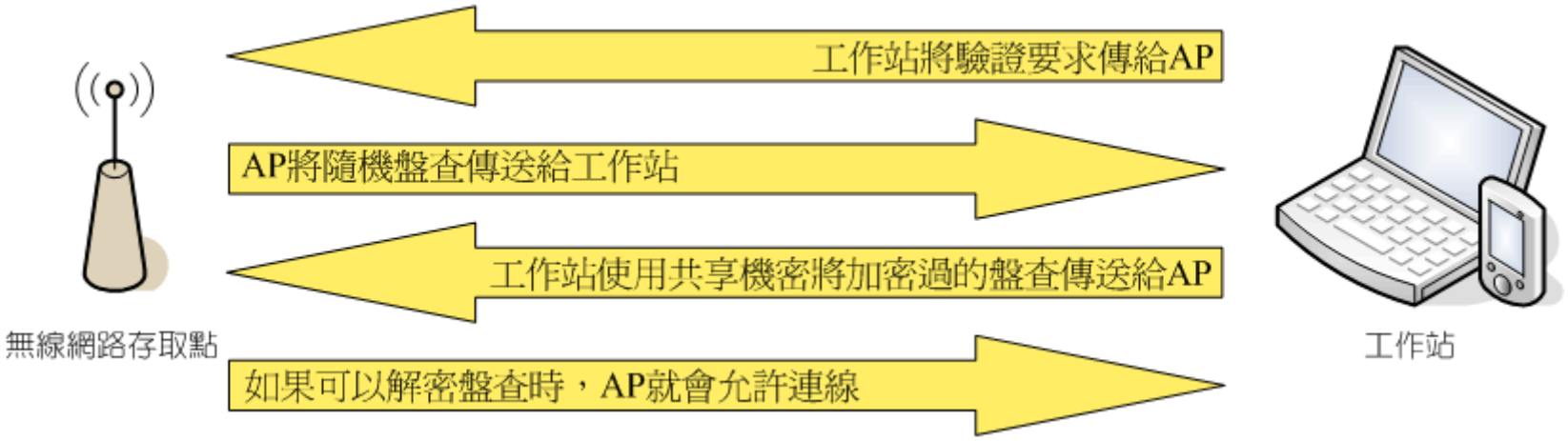

圖14-4 WEP交換身份認證

返回

身份認證的問題

- WEP身份認證服務只能提供AP單向認證工作站的身份，它並不提供雙方相互認證的機制，所以工作站也無法證明AP的真實身份。
- 此外，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。

身份認證的問題

- WEP身份認證的過程中，可能會遭到中間人(man-in-middle)或攔截攻擊(interception)(詳見圖14-5)。

802.1X連接埠型的網路存取控制

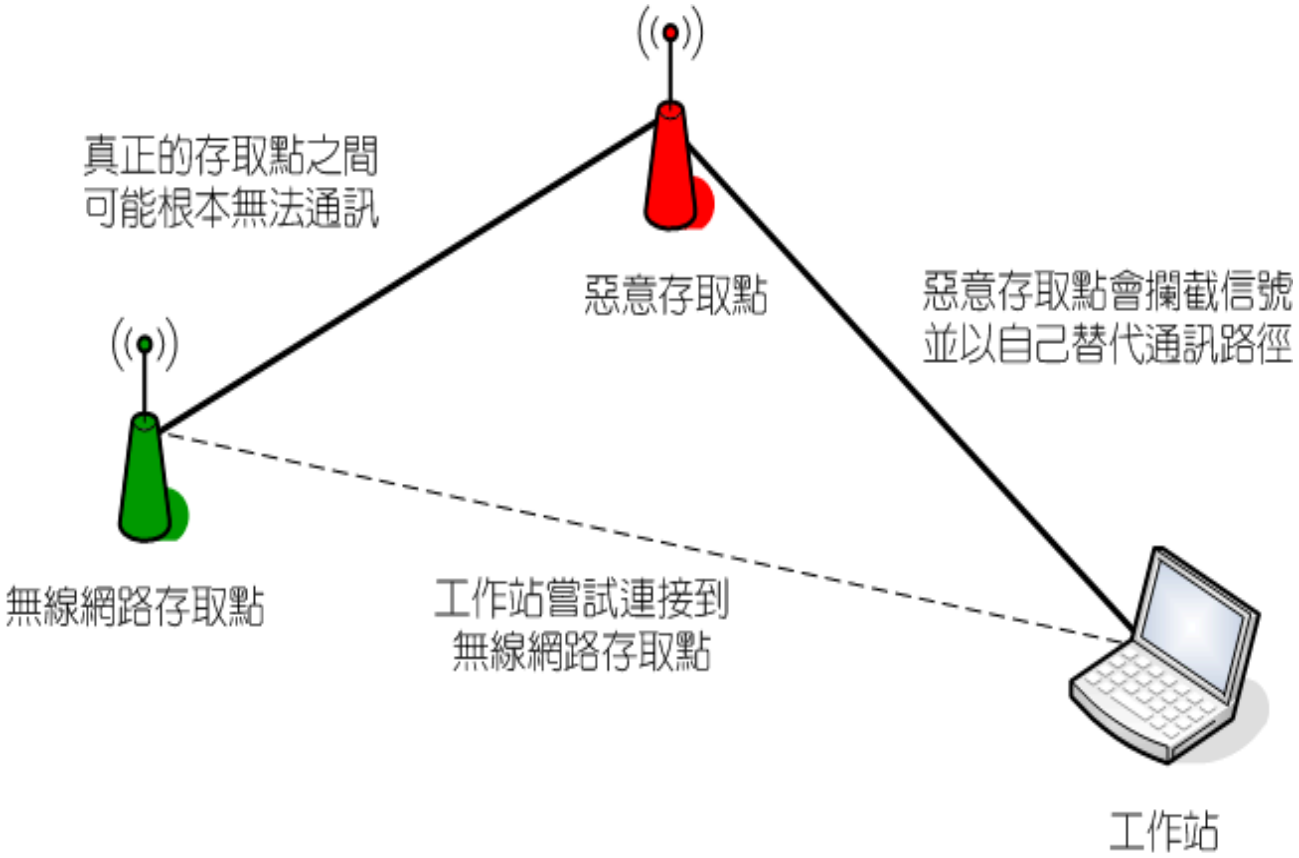

圖14-5 針對WEP的中間人攻擊

機密性

- WEP 加密採用RC4演算法，雙方的密鑰是共享的，透過一個 24 bit 長度的初始向量IV (initialization Vector)，結合 40位元或104位元的密鑰來共同產生真正用來加密的密鑰串流，所有的傳輸內容與這個密鑰串流進行XOR 運算，轉換成密文後發送。

- 此一加密機制可以用來保護所有的協定標頭(header)資訊，以及802.11x協定層以上的資料（也就是2層以上的資料）。

機密性

- WEP並未指定金鑰管理機制，也就是說使用相同的私密金鑰來進行加解密， 沒有提供私密金鑰的定期更換或變更功能。
- WEP 運用802.11x標準，預計提供與纜線傳輸同等級的安全性，但在2001年學者Scott Fluhrer, Itsik Mantin 及 Adi Shamir [2]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。

註: 某些設備供應廠商已經採用階段性變更WEP金鑰的標準機制，但是這些機制都是標準以外的機制。

機密性的安全問題

- 根據Scott Fluhrer學者們的論文，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，有部分仍會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)。
- 攻擊者若能收集到越多符合特定特徵的資訊，找出原來使用者指定之密鑰的可能性就越高。

機密性的安全問題

- RC4演算法中的IV，間接的透露出密鑰的資訊；駭客可利用破解工具予以分析，在有效訊息封包數量足夠的情況下，快則在數十分鐘內即可將密鑰反解出來。

- 破解WEP的工具程式
  - WEPCrack，網址是 http://sourceforge.net/projects/wepcrack/
  - AirSnort ，網址是 http://airsnort.shmoo.com/

完整性

- WEP協定規格會針對每一個傳送的封包完整性做檢查。
- 完整性檢查是採用32位元循環冗餘檢查（cyclic redundancy check，CRC）。
- 在每一個封包加密之前會先使用CRC予以計算，之後再將資料和加密過的CRC相加並傳送給目標接收者。
- 雖然CRC並不是安全密碼(採用安全雜湊函數更佳)，但仍然受到RC4加密的保護。如果加密系統相當牢靠，或許也不至於造成嚴重的問題。

完整性

- RC4演算法可能導致WEP協定中封包的完整性遭到竄改，更顯現出CRC對資訊完整性保護的重要性。
- 只要WEP協定採用適當宜牢靠的加密系統機制，就不會產生封包完整性的問題（甚至單純使用CRC檢查），也可以做為保護資訊，避免遭受未經授權的第三者竄改的機密性服務。

Module 14-1-3: 身份認證安全的改進

身份認證安全的改進

- WEP只能提供簡單型式的AP認證工作站身份，單向認證機制。
- Cisco 積極推動新一代的無線網路安全標準，建議組織採用802.1X的可擴充式驗證協定 (Extensible Authentication Protocol, EAP)[3,5]，透過認證伺服器（Authenticator server）讓企業可採用符合標準且能集中管理的安全性架構，以用來部署數千個使用者的無線網路環境。(詳見圖14-6)
- EAP 允許無線網路客戶端使用數種不同的認證方式，與後端的認證伺服器如RADIUS 溝通。

802.1X連接埠型的網路存取控制

- 802.1X是一種控制通訊埠為主的網路存取控制協定。
- 802.1x協定主要是提供一般性的網路存取身份認證機制，且可廣泛地提供下列網路的身份認證：
  - 乙太網路(802.3)
  - 記號環(802.5)
  - WLAN (802.11)

802.1X連接埠型的網路存取控制

- 以下介紹802.1x協定

請求端（Supplicant）

– 是以用來尋找存取的實體。在WLAN的架構中，工作站就是扮演這種角色。

認證端（Authenticator）：

– 這是一種用來找尋其他認證實體(認證伺服器)的網路設備。在WLAN的架構中，可利用AP來擔任這項類似看門警衛的工作。

認證伺服器（Authenticator server）：

– 此為 認證服務的來源。802.1x允許中控化的管理機制，所以也有可能是RADIUS伺服器來扮演這種角色。

網路存取點：

– 工作站連結到網路的連接點。在實體環境中，是由交換式集線器或共享式集線器的連接埠扮演這個角色。在無線網路的環境中，是由工作站和AP共同扮演這個角色。

802.1X連接埠型的網路存取控制

連接埠存取實體（Port access entity，PAE）：

- PAE是一種執行認證協定的流程，認證端和需求端都具有PAE流程。

802.1X連接埠型的網路存取控制

- EAP應用於802.1x的認證協定架構如圖14-6，其提供比WEP更為牢靠的認證機制；如果在此機制下能夠結合RADIUS伺服器，則可達成中控式管理使用者的目標。
- 相互認證是屬於802.1x的選項，但是許多系統都將這個選項設定成預設值，因此也就有可能遭到攔截攻擊。
- 故唯有AP及工作站緊密地結合，802.1x才能夠正常地發揮作用，也就是說，若802.1x未能發揮作用，或許在認證發生之前，工作站就已經連線到無線網路了。

802.1x應用於無線網路的存取控制

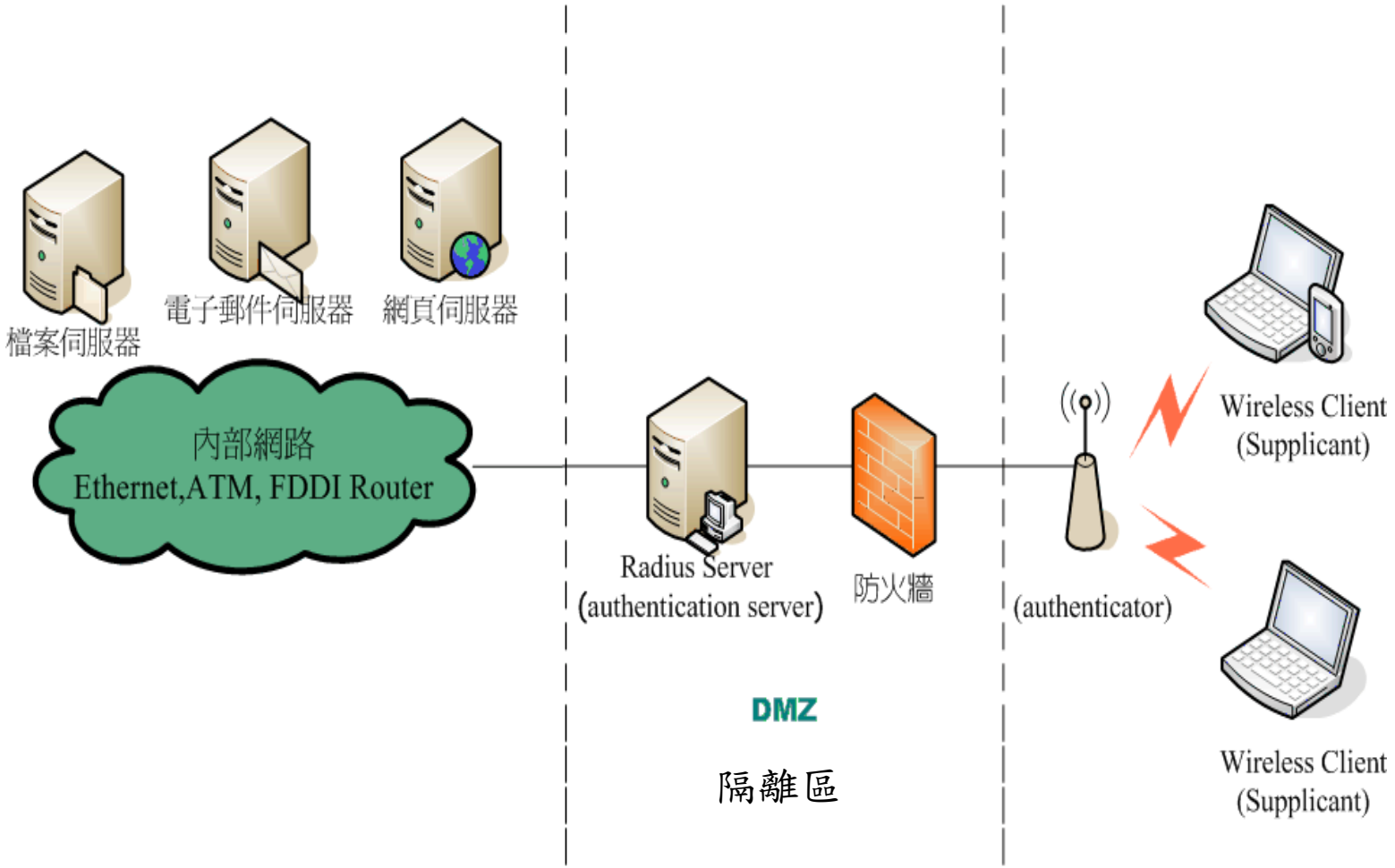

圖14-6 EAP認證協定架構

返回

802.1X連接埠型的網路存取控制(**)

- 802.1x/ EAP支援多種認證協定，如MD5、TLS、TTLS、LEAP及PEAP等 。
- 其中EAP-MD5是一種簡單且容易實現的方式，是屬於單向且一次性認證（開始進行交談時），故容易遭到中間人攻擊或攔截攻擊。
- 改進的方法:
  - EAP-TLS (rfc2716)為微軟所發展，亦為IETF(Internet Engineering Task Force)所認可，提供Pre-session的動態交換WEP密鑰， 且supplicant與authentication server進行雙方認證，可大幅降低中間人攻擊或攔截攻擊。

802.1X連接埠型的網路存取控制(**)

- 輕量型可擴充式驗證協定 (Lightweight Extensible Authentication Protocol, LEAP)：由Cisco所發展之技術，使用動態性地將每次連線階段所使用的不同WEP 金鑰，發給每個無線網路客戶端，其整合網路登入認證機制亦加強了WEP 標準的安全性，有效降低駭客對於金鑰的預測機率，大大減少網路可能受到攻擊的範圍。
- 被保護的延伸性認證協定 (Protected EAP, PEAP)：將身份認證分為二階段，首先藉由TLS的加密通道，讓工作站對認證伺服器做認證，之後再以不同的EAP身份驗證方法去驗證工站作的身份。

Module 14-2: 認識無線網路的安全問題

14-2 無線網路的安全問題

802.11 無線網路的安全問題大致可分為大類：

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以適當的機制進行加密，則入侵者很容易的便可以竊取所有的通訊內容。
- 另外，由於無線通訊只要位於電波收訊範圍內即可使用，也造成了管控上的問題， 管理者無法完全的存取監控。

14-2 無線網路的安全問題

2.WEP 設計問題

- 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者獲得更好的資料安全性。
- 但是由於某些設計及實作上的欠缺考量，使得 WEP 無法保證資料內容的機密性。
- 設計協定時沒有考慮金鑰管理的問題， 因此如果要管理一個很大的無線區域網路的話，金鑰的更換及配送將會是一個重要的管理問題。

14-2 無線網路的安全問題

3. 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，以致於駭客可經由原廠的設定資訊進行攻擊。
   - 這些缺失可能造成攻擊者反客為主，獲得設備的管理權限，造成安全的威脅。

14-2無線網路的安全問題

以下介紹攻擊者可能的攻擊程序及其法律問題

Module 14-2-1: 偵測WLAN

Module 14-2-2: 竊聽

Module 14-2-3: 發起攻擊

Module 14-2-4: 可能的法律問題

14-2-1 偵測WLAN

- 入侵者偵測WLAN非常容易，目前也已經出現許多這種類型的工具程式。
  - NetStumbler是一種在Windows系統執行的工具程式，且可使用全球定位系統（Global Positioning System，GPS）接收器測探WLAN。（http://www.netstumbler.com/）
  - 這個工具程式可以辨識WLAN使用的SSID，甚至也可以辨識WEP。

14-2-1 偵測WLAN

- Kismet是另外一種工具程式，也同樣可以辨識和AP交談中的工作站，以及這些設備的MAC位址。（http://www.kismetwireless.net/）
- 具有外部天線的可攜式電腦，也可用來找尋鄰近地區或都會區的無線網路，並試著去認證是否可以存取該WLAN。
- 帶著可攜式電腦繞著建築物轉一圈，偵測是否有無線網路訊號，此做法同樣是偵測WLAN的好方法。

14-2-1 偵測WLAN

- 入侵者可能不需要使用外部天線，不過外部天線可以提高這些工具程式的偵測範圍。

14-2-2 竊聽

- 當入侵者完成WLAN偵測，並取得SSID或MAC資訊，則可連接上組織內部網路。

- 入侵者有可能藉由將車輛停放在目標建築物的停車場(某種有效距離範圍內)，進而連接上組織的WLAN(詳見圖14-7)。

14-2-2 竊聽

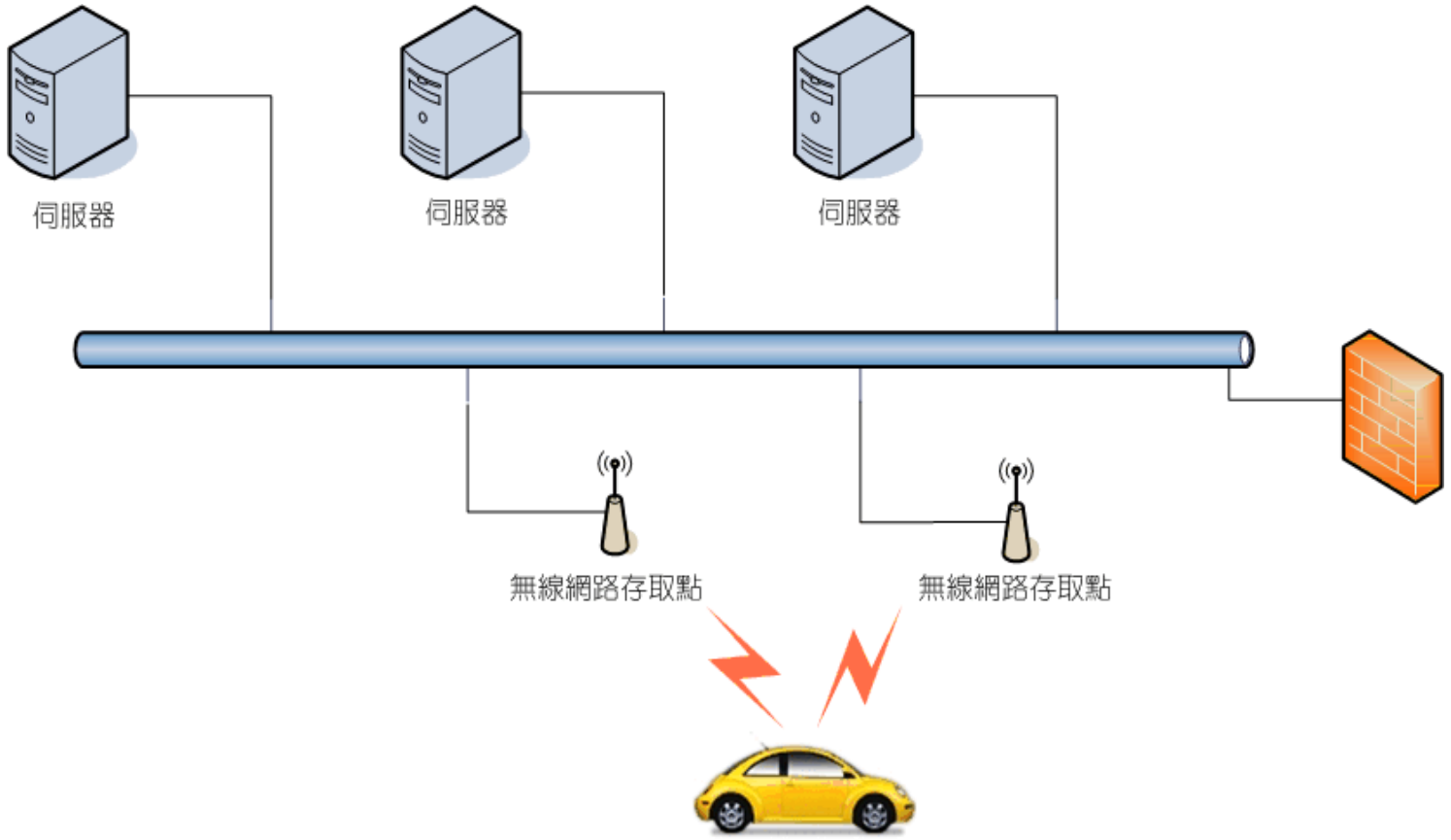

圖14-7 竊聽WLAN

14-2-2 竊聽

- 部署無線網路的組織，須面對無法避免的竊聽攻擊類型。在非常繁忙的網路上，入侵者運用竊聽工具程式，只需要一點點時間即可利用被動式監聽網路擷取所需的資料封包數量，並分析判斷出加密私鑰。
- 無線網路管理組織一般無法察覺被動式竊聽攻擊。

14-2-2 竊聽

- 網路上常用的兩項工具 - WEPCrack 與 AirSnort 可以用來進行此項竊聽。
- 兩者的使用方法都是由入侵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, Scott Fluhrer, Itsik Mantin 及 Adi Shamir等研究人員的論文。
  - Nikita Borisov, Ian Goldberg, David Wagner: Intercepting mobile communications: the insecurity of 802.11. MOBICOM 2001: PP. 180-189

14-2-3 發起攻擊

- 當入侵者完成WLAN竊聽後，隨之反解出來的密鑰將被用來更進一步收集、解析網路上的通訊資料。
- 後續攻擊行為可包括：
  - 蒐集網路重要資訊
  - 竊取電腦內部資料
  - 佔領此一據點，繼續監聽此網路的其他電腦，再佔領此一網路
  - 以此網路為基地去攻擊其他網路

14-2-3 發起攻擊

- 故入侵者可直接攻擊組織的內部，或控管此入侵的系統，並利用連線攻擊其他組織(詳見圖14-8)。
- 如果可以偵測到入侵者，這個問題就會變成『入侵者從哪裡闖入』？或許可以追查到入侵者的IP位址來源，但是這個IP位址也可能只是跳板。
- 入侵者可能出現於無線網路系統範圍之內的任何地點，故組織須測量並管制無線網路的運作範圍，避免外人不當存取 。

14-2-3 發起攻擊

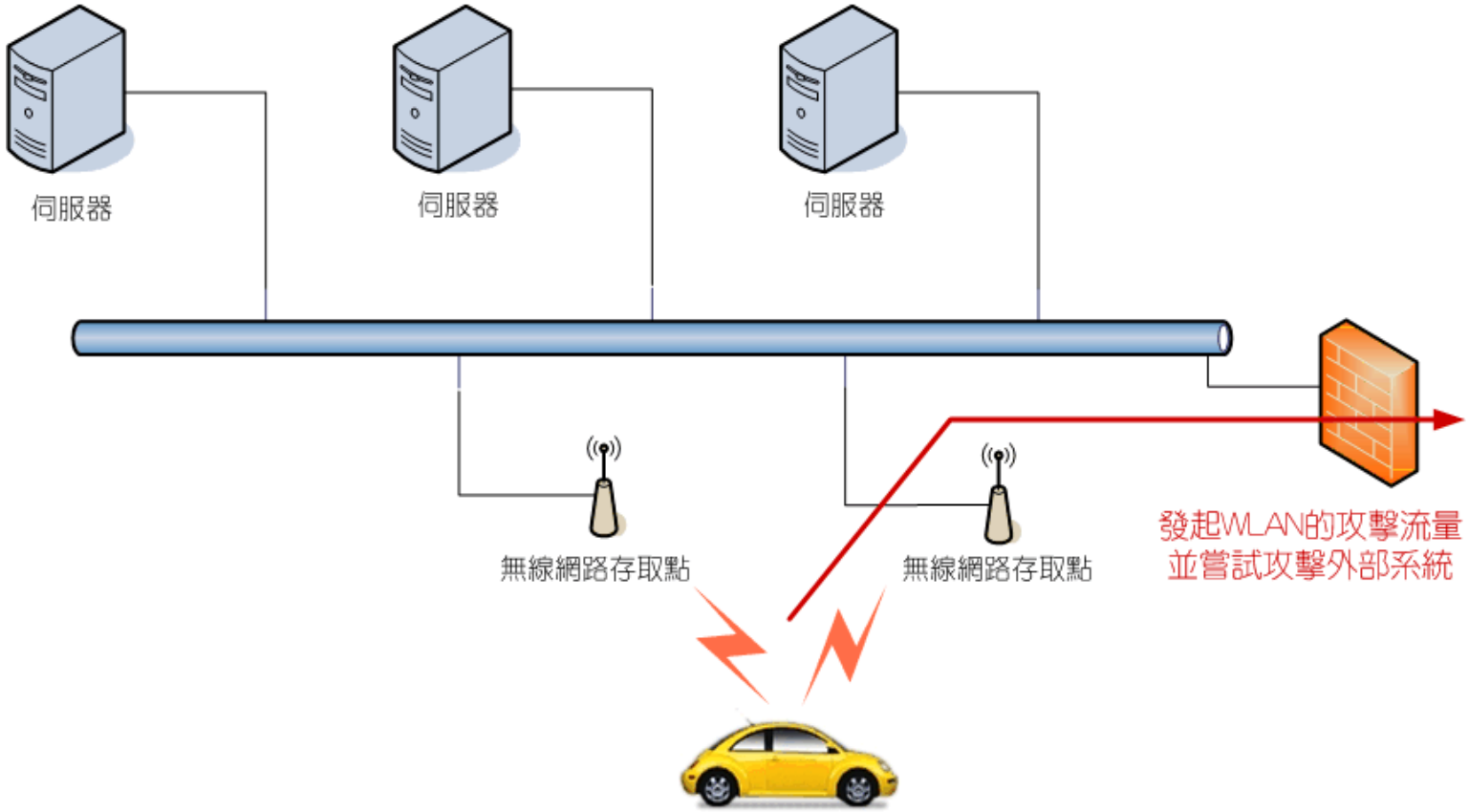

圖14-8 利用WLAN存取並攻擊外部站台

返回

14-2-4 可能的法律問題

- 如果入侵者獲取組織內部網路的存取權，隨之而來的法律問題變成了組織必須面對的另一種風險。
- 組織需面對機密資訊保護與控管流程的問題來提出解決方案。
- 如果入侵者利用組織的WLAN成功地攻擊其他組織，WLAN的擁有人是否應該負責所有的損害？

Module 14-3: 架設安全的無線網路

14-3 架設安全無線網路

- 在架設WLAN之前，務必要先進行需求分析、風險分析和威脅分析，待完整地評估每一個項目的風險後再依計劃執行。
- 組織應該重視可能導入的風險，除此之外也應該為此建立防範措施。
- 如果組織選擇架設無線網路，也應該要建置可以降低組織風險的安全措施，下列內容都是可以用來協助處理風險的安全措施。

14-3 架設安全無線網路

Module 14-3-1: 存取點安全

Module 14-3-2: 傳輸安全

Module 14-3-3: 工作站安全

Module 14-3-4: 站台安全

14-3-1 存取點安全

存取點安全管理

- 設定安全組態的存取點(Access Point, AP)，是架設無線網路的重要起點

- AP必須要設定WEP金鑰，而且也應該要確保不容易為駭客猜到金鑰，雖然無法完全的防範金鑰遭到破解，但是相對的也會提高破解的困難度。

- 以MAC位址作為合法工作站的判斷要項。

- 兩項認證的機制雖然會增加整個管理專案的工作量，不過卻可以協助限制攻擊者對某些AP的偵測。

14-3-1 存取點安全

- 若AP的廣播SSID功能可關閉則關，不然盡可能選用不會廣播SSID 的AP 。
- 目前市場上大多數的AP，都已經提供管理介面，這些管理介面可能是Web介面或SNMP介面。
- 盡可能使用HTTPS的加密管道來管理AP，並使用牢靠的密碼來防範入侵者。
- 最後必須思考的項目就是架設AP的地點。

14-3-1 存取點安全

- 無線網路的訊號涵蓋範圍非常廣闊，有效訊號距離可能會擴及建築物的其他樓層、停車場，或是外部的人行步道，造成無線網路管理上的漏洞。

- 盡量的規劃AP的架設地點，使其訊號涵蓋範圍限制在組織的設施內。

- 要完全地限制信號的涵蓋範圍似乎是不可能，不過也要盡可能地嘗試，且不要讓信號涵蓋範圍擴散到不容易掌控的區域。如果可以做到限制不能從某些步行區域、人行道、停車場等，使用無線網路卡存取到組織的WLAN時， 則可大幅的降低被攻擊成功的機率。

14-3-2 傳輸安全

傳輸安全管理

- 找出一個WEP補強的方法
- 首先將WLAN視為不能完全信任或不信任的網段時，用保護遠端員工存取內部系統的方式來保護WLAN
  - 例如以Ipsec進行原始資料加密後再傳送
  - 大多數的VPN(Virtual Private Network,虛擬私有網路)都是採用非常牢靠的演算法，且沒有類似WEP的缺陷，故WLAN可結合虛擬私有網路(VPN) ，傳輸的資料一律進行加密與身份認證(詳見圖14-9)。
  - 將WLAN放在防火牆或其他存取設備的後方，且同時使用VPN即可解決很多有關WLAN存取安全的問題。

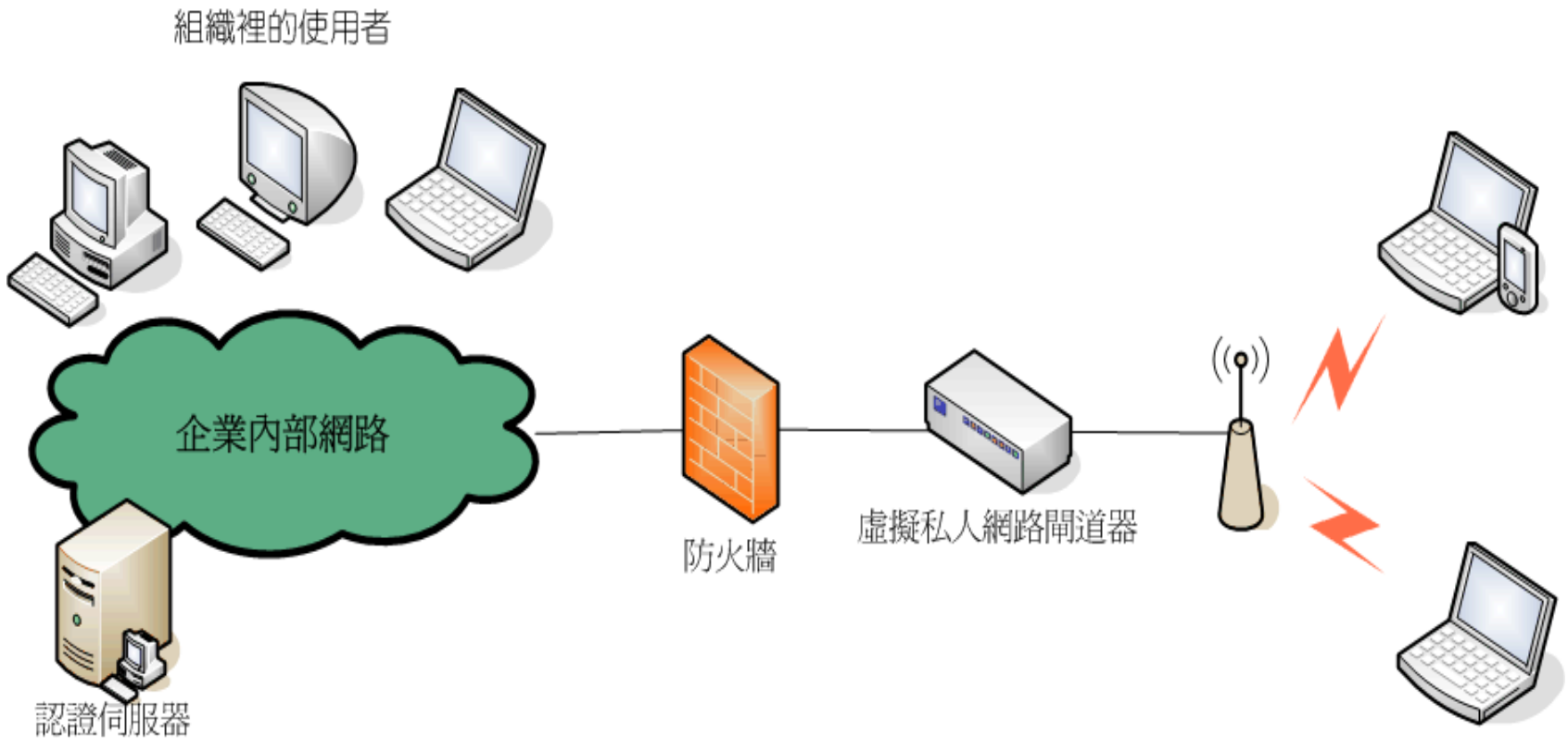

圖 14-9 VPN應用於無線網路

返回

14-3-3 工作站安全

工作站安全管理

- 如果入侵者得以存取WLAN，那麼入侵者即可使用sniffer辨識其他工作站， 進而攻擊WLAN的工作站。
- 保護WLAN工作站的方式和一般桌上型系統一樣，應該要安裝個人防火牆並適時的進行作業系統修補。
- WLAN工作站須安裝掃毒軟體，以找出入侵者所安裝的後門及木馬程式。
- 若作業處於高風險的環境中， 則WLAN工作站也須定期透過Nmap或Nessus進行弱點掃瞄， 找出系統的漏洞。

14-3-4 站台安全

站台安全管理

- 不能允許WLAN工作站存取內部機密系統: 如果管理者將WLAN視為不完全信任或不信任的網路時，就沒有任何理由要將WLAN架設在內部網路上。

- 防火牆加以區隔: 將WLAN架設在它們獨立的網段上，且在WLAN網段和內部網路之間，安裝某種類型的防火牆加以區隔。

14-3-4 站台安全

- 以IDS偵測: 在這些獨立WLAN網段中，也應該架設用來偵測未獲授權訪客的入侵偵測系統，以發現入侵者的攻擊行為。
- 定期評估無線網路的安全: 非法或未經授權的安裝與使用AP都是組織必須重視的問題，因為任何人都可能以低價的方式購得AP，並安裝在網路上，故組織應該定期在自己的內部網路上，執行無線網路安全評估。

※未來發展趨勢與研發議題

- 802.11n通訊規格與硬體實做
- WiMAX無線網路通訊技術
- 無線感測網路(Wireless Sensor Networks)
- AES結合TKIP(Temporal Key Integrity Protocol)的網路通訊加密技術

習題

習題一

- 請簡述無線區域網路中簡易模式(Ad hoc Mode)與基礎建設模式(Infrastructure Mode)的差別。

習題二

- 請說明服務辨識器（Service Set Identifier，SSID）為何？以及其運作上有何缺點？

習題三

- 試以圖解並說明WEP加密機制的運作流程。

習題四

- 請解釋何為弱密鑰？

習題五

- 請以三項服務構面(身份認證、機密性、完整性)簡要說明WEP機制。

Module 14-4: 專案實作

14-4-1 專案目的

- 應用Windows XP系統平台。
- 安裝無線網卡及無線基地台。
- 設定連結資訊。
- 以圖文解說，實際操作方式，引導同學建置出一無線網路環境。

14-4-2 專案摘要

- 本專案範例中用的無線網卡是以LEMEL(LM-WLB600I)為例。
- 本專案範例中的無線基地台(AP)是以ZyXEL(G-500)為例。
- 不同品牌的無線基地台，其管理設定介面的預設IP位址及密碼會不同，請參考其使用說明書。
- 務必更改無線基地台預設的管理設定介面登入密碼，以防有心人士對連線設定的竄改。

附錄一:IEEE802.11標準[7]

- 1997 年首次公開的IEEE802.11 無線區網路標準，主要是在規範無線區域網路環境的通訊協定，對於實體層(Physical Layer)及Mac (Media access control sub layer)亦規範之。而Mac 層規範了各種不同的實體層，以因應將來的情況未來的技術方向。
- 此項標準有三個主要部份，第一部份為Power saving function，第二部份訂定相關的PHY 規格，第三部份定義為了未來技術的擴充性，都提供多重速率(Multiple Rates)的功能。
- 無線區域網路的基本結構IEEE802.11 Mac 的基本存取方式稱為CSMA/CA (Carrier Sense Multiple Access with collision Avoidance)，與乙太網路所用的CSMA/CD (Collision Detection)不同。

附錄一:IEEE802.11標準(續)

- 在IEEE802.11 中感測載波的方式有兩種，第一是資料感測目前是否在傳送，再加上優先權的觀念。第二是虛擬的感測載波，告知多久的時間要傳資料，以防止網路上封包的碰撞，在此架構提供300 米的範圍，可有1Mbps 到 2Mbps 的傳輸速率。
- 國際電子電機學會於1999 年9月再度發表IEEE 802.11b 高速無線區網路標準，將原來無線網路的傳輸速度至 11Mbps。
- 在IEEE 802.11 中傳輸模式包含兩種，分別是紅外線(Infrared)及微波展頻(Spread Spectrum)兩種
  - 紅外線有其距離及阻隔的先天限制，已甚少使用
  - 此微波為無線區網路之主流，目前大部份產品都使用UHF二個波段及微波900Mhz、2.4ghz、5.7Ghz 等。

附錄一:IEEE802.11標準

微波展頻技術

- 微波展頻技術又分成兩部份：直接序列展頻DSSS (Direct Sequence Spread Spectrum)及跳頻展頻FHSS (Frequency Hopping Spread Spectrum)。
- 直接序列展頻發射頻率以較有規則性的、成序列性的在該寬波段內，以展開碼(Spread Code)的方式傳資料，目前在無線網路上，是使用ll 位元的展開碼將原來的無線電波訊號展開11 倍後再傳送。
- 跳頻展頻則是利用窄頻載波在不同的頻道間，以協定的頻道跳躍順序來傳送訊號，依FCC 規定跳頻使用的頻道數，至少為75 個，比DSSS 直接序列展頻來得多。

附錄一:IEEE802.11標準

- FHSS 有複雜的跳頻及同步協定，相對於DSSS 有較佳之保密性，在複雜的環境下，會產生多重路徑(Multi-path)問題，FHSS 有跳頻優良的性能，可克服此多重路徑的問題
- 在小區域，大量存取需求需要數量多的收發器同時存在時，FHSS 有較大的頻道可分配（至少75 頻道），並且允許在小區域架設多數量之收發器Access Point，而不會造成微波碰撞，降低性能。
- 反之DSSS 的相對頻道較少（11 頻道），允許重復涵蓋的只有3 個頻道，因此在小區域架設多數量之收發器有其限制，相關位置亦有其限制，增加了不少在配置上的困難。

參考文獻

1. Network Security — A Beginner'Guide by Eric Maiwald.
2. Scott R. Fluhrer, Itsik Mantin, Adi Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4". Selected Areas in Cryptography 2001: pp1–24.
3. 無線區域網路技術白皮書,D-Link技術團隊編著
4. 詹俊韋,無線區域網路資源動態分配之效能研究,國立中央大學碩士論文, 民92。
5. 涂世雄, 徐敬堯, "應用EAP-TLS 與 X.509 實現 WLAN (IEEE 802.1X) 之全域認證研究", 中原大學電機工程研究所, 碩士論文, 民91。

參考文獻

6. 謝續平, 網路安全概要2005教材, 交通大學, 民國九十四年, http://dsns.csie.nctu.edu.tw/course/intro~securit/2005/。
7. 葉義雄、胡家棟, “A SSO Service of integrating SAML and EAP-SIM Authentication, and Its Security Consideration”, 國立交通大學資訊工程系所,碩士論文,民93 。
8. 林文修,輔仁大學資訊管理系,資料通訊與網路課程資料。http://cyber.im.fju.edu.tw/