你的無線區域網路（wireless LAN: WLAN）安全嗎？

/台灣思科系統

由於WLAN**具有易安裝，以及提供企業內部隨處存取企業資源的上網能力等特性，因此使用數量日益增加；但令人驚訝的是，絕大多數的企業卻未啟動無線安全功能。根據**2001**年**4**月**27**日的華爾街日報（**Wall Street Journal**）報導，有兩位駭客開車進入矽谷，利用筆記型電腦和手提式天線竊聽每個沿途經過的網路，而根據這兩位駭客表示，財星五百大企業的外部周圍是最佳的竊聽點。**Cisco**無線網路事業部的軟體發展經理兼**IEEE 802.11**安全議題小組**(security task group)**主席**David Halasz**表示：『將無線傳輸技術加入網路之後，企業必須對安全和管理問題提高警覺，即使是在建築物之外或是鄰近某個員工的住家，依然可視為企業網路的一部份。而穩固的無線安全功能和簡易管理機制，則是將無線技術整合至企業網路架構的必備元素。』

根據加州大學柏克萊分校研究員的報告指出，即使企業確實啟動802.11**標準**WLAN**安全功能，也不表示無線電波是安全。這份報告不僅揭露靜態**WEP**標準的缺點，也不禁讓人質疑，這套標準為何會運用於所有的應用環境？換句話說，如果**WEP**成為全球標準之前已經被密碼專家檢驗過，許多可能的安全漏洞都應該已經被確實消除。事實上，網路界普遍認為保護**WLAN**網路安全唯一的方法就是採用虛擬私有網路（**Virtual Private Network**；**VPN**）技術，但卻需要額外的費用和管理。柏克萊分校的報告亦指出，截至目前並未發現任何一個現有商用化系統可支援此項技術的機制，而**VPN**技術確實可以有效保護無線通訊免於受到攻擊。

Cisco雖認同柏克萊分校的研究報告所提到關於靜態**802.11WEP**標準的弱點，但遺憾的是，柏克萊的研究人員並沒有發現到**Cisco Aironet**無線網路方案。**Cisco Aironet WLAN**在**802.11**架構中採用**IEEE 802.1x**初版標準的安全機制，而產品的安全機制則會提供動態、每個用戶和連線單獨的**WEP**密碼，因此可以解決此研究中所發現的許多問題，同時強化整體**802.11 WEP**加密機制的安全性。其中這些安全機制包括相互認證（**mutual authentication**）、安全鑰匙的產生**(secure key derivation)**、動態**WEP**加密鑰匙、重新認證（**re-authentication**）、初始向量的改變（**IV change**）。而企業所要做的就是將這些功能開啟，一切問題便能迎刃而解！

一、 相互認證

許多現有的產品都採用簡單、單向的認證機制。此機制會受到中間人攻擊法

（man-in-the-middle attack）的入侵，也就是駭客可以利用偽裝的裝置來攔截資訊，如接取點(Access Point)，並且由用戶端收集認證資料，接著複製或更動封包，最後再將這些封包當成是合法封包重新插入網路中。會有這樣的問題產生，主要是因為在無線網路中不可假設有任何安全疆域，而是必須確定用戶端和網路端接取點雙方的合法性，而相互認證是避免中間人攻擊法的唯一機制。

在Cisco Aironet無線網路解決方案中，Cisco參考延伸認證協定(Extensible Authentication Protocol；EAP)創造一種認證機制，稱為EAP-CiscoWireless或LEAP，其使用802.1x初版標準中以傳輸埠為控制單元的安全機制當作基礎，並針對WLAN環境作必要的修改。此外，LEAP具備提供Cisco Aironet用戶端網路卡和網路端RADIUS (Remote Authentication Dial-In User Service)伺服器間的相互認證功能。

二、認證和安全鑰匙的產生

第一代的802.11產品使用靜態WEP鑰匙以作為認證和加密之用，如此使得WLAN易於受到『密碼再度使用』攻擊法（password replay attack）的入侵。Cisco Aironet無線網路解決方案則是將認證和加密功能分開處理。在相互認證程序中，由於認證密碼本身不會在空中傳送，而檢查封包的內容則是隨機產生的，因此雙方共知的分享密碼會產生單獨回應對方送出檢查封包的資料，而回應封包的加密動作則會利用原始分享密碼，進行單方向的資料重新拼湊（hash）。而結合好的認證密碼選擇及變更策略，將可消除野蠻力量攻擊法(brute-force)的入侵。

單向交談鑰匙（session key）的產生是利用訊息摘錄5(Message Digest；MD5)演算法，將重新拼湊過的共享密碼和相互挑戰過程中的回應封包再進行一次單向資料重新拼湊，此方法可避免駭客利用攔截回應封包產生交談鑰匙的可能。無法解出單方向資料重新拼湊的內容，就如同無法將打散的雞蛋重新變回原來的模樣一般。而將隨機產生的挑戰-回應封包和鑰匙密碼的產生結合在一起的方法，可以確保在密碼過期或是漫遊之後，在每次重新認證時，都會讓交談鑰匙的內容有所更新。

三、動態WEP加密鑰匙

802.11標準中WEP加密鑰匙管理是交由製造商自行設計。多數第一代802.11產品採用單一、共享加密密碼，適用於同一網路中所有使用者，但這方法卻產生了一些問題，最明顯的危險就是，加密鑰匙可能會被偷竊、失竊或遺失的裝置卻遺留有這把加密鑰匙；第二個問題就是，WEP加密鑰匙的管理。

由於共享鑰匙使用靜態WEP標準，因此必須手動輸入每一個接取點和終端用戶裝置中，而這卻是一件相當費時的工作，尤其是如果網路管理者必須每次都

為整個網路新輸入加密鑰匙、或是處理終端用戶的裝置遺失時，這問題顯得更為嚴重，尤其當有數以千計的用戶時，這方法更是不可行！為了解決此一問題，Cisco在其無線網路解決方案中採用動態安全機制，一旦登入系統並通過認證，整個連線過程中的加密鑰匙就會自動產生。

四、重新認證策略

WLAN通常會受到『流量注入』攻擊法（traffic-injection attack）入侵，意即駭客發現到預期中的資料格式時會將自己的封包插入企業區域網路中。雖然標準的802.11WEP制訂抵擋『流量注入』攻擊法和『統計』攻擊法（statistical attack）機制，但是靜態WEP方法並無法正確的抵擋攻擊。

串流式加密法(Stream Cipher)會將較短的加密鑰匙延展成為無限長、近似亂碼的一長串密碼流。傳送端會將長串密碼流和原始資料（plaintext）經過XOR運算後產生加密資料（ciphertext），而接收方也會因為用了相同的加密鑰匙而產生一樣的長串密碼流，因此攻擊者可利用攔截資訊流(intercepting traffic)、更動位元(flipping bits)、將修改過封包加入網路的方法來攻擊此一漏洞，如果攻擊者攔截到兩份使用相同長串密碼和初始向量處理過的加密文件，則可利用『統計』攻擊法將原始資料加以還原。

為了防止上述的駭客攻擊，Cisco Aironet無線網路解決方案則加入讓網路管理者可以制訂和集中化管理連線中途的重新認證策略，如每30分鐘進行一次（這是在24位元初始向量的整體重複週期時間之內）。由於此方法主要是破壞駭客利用攔截、中斷傳輸、和破解連線認證鑰匙以登入網路的能力，因此可大幅減少主動攻擊法的有效區間。

五、初始向量的改變

802.11 WEP標準提供搭配初始向量（IV）數值的整體檢查法（integrity check），以確認每個封包標頭正確性的功能。然而，由於IV欄位的長度僅有24個位元，任何單一連線只要維持約五個小時以上，IV欄位的數值就必須重複使用。當有多個連線透過單一接取點在通訊時，IV數值會發生重疊現象，如此則增加攔截到兩份使用相同加密鑰匙的加密文件的可能性，也為表列式攻擊法（table-based attack）提供一個攻擊起點；經過解讀少數封包的原始文件後，攻擊者就可以建立一個解密表，由使用中的IV數值產生RC4加密鑰匙流，藉此對資料流中其它封包進行解碼，若再經過長時間的運算，攻擊者就可以建立起IV和加密鑰匙流的數值表。

Cisco Aironet 802.1x無線網路解決方案，藉由改變每個封包的IV數值以解決這個問題，而駭客就只能找到毫無規則可循的一串數字而已；同時每個連線的IV

數值都是隨機產生，而不是每次都是使用相同的數值。結合上述重新認證機制，改變IV數值讓駭客難以採用表列式攻擊法。

六、CRC-32 檢查加總（Checksum）

802.11標準的整體檢查功能容易受到攻擊，因為其採用線性的CRC-32檢查加總法，只要更動資料中的位元就有可能計算出兩個CRC數值之間的不同。不管是802.1x或是現有的802.11標準都沒有為這問題提出解決方法。

由於駭客可以修改封包內容，更動位元產生CRC數值，如此這些封包就變成合法的封包；此外，他們亦可模擬已知協定的行為來修改封包。而解決此問題的唯一途徑，就是每個封包都進行整體檢查。Cisco在未來產品中將加入此項功能，同時推動標準的後續演進。

制訂標準促進互通安全性

Cisco目前正和其它公司共同為WLAN網路，以發展一套可互通的安全架構而努力。在IEEE 802.1x的基礎上，Cisco、Microsoft和其它公司一起向IEEE 802.11標準組織提出一套基本的安全架構。依據一些標準，如EAP和RADIUS，802.1x為802.11提供一個具有彈性的架構，可以支援多種的認證機制，包括生物檢查法（biometrics）、文件證明法和單次密碼認證法。然而，為了要完全解決無線通訊環境的特殊問題，如相互認證、多人環境下密碼再度使用的保護等，這些認證機制必須要從原有應用於傳統有線網路或是撥接網路的架構中再做些改進。

結論：沒有單一的安全機制可以解決所有問題

保護WLAN網路安全只是整體企業安全架構的一環，安全專家建議企業應該在網路中架設多層的防衛機制以消除威脅，而其它安全元件包括防火牆、入侵偵測系統(intrusion detection systems)和網路區段分隔。Cisco的802.1x無線安全產品確實消除多數由靜態WEP標準所衍生的威脅。Cisco除了提出Aironet無線網路解決方案，以保護企業組織免於受到大部分的攻擊外，Cisco亦和合作夥伴共同參與標準組織的運作，努力解決剩餘的問題。

人們現在正開始利用筆記型電腦和PDA享受無線IP傳輸所帶來的自由，預估從現在開始的一年後，可能再也無法買到一台主機板上沒有內建無線連線功能的筆記型電腦或PDA了！未來，一旦802.11網路卡成為攜帶式電腦的基本配備後，人們將可以走到任何地方，隨時保持連線狀態，而這也正是無線網路的最終目標！