從加密技術看無線網路安全

台灣思科系統提供/
企業事業群技術支援部經理 楊士逸

隨著無線網路的快速普及，企業也必須開始思考，如何能將現有的網路環境與無線網路更緊密地整合在一起。當企業著手部署無線網路時，通常最主要的考量即為無線環境的「安全性」，其中包含了兩個最重要的因素：「連線控制」與「資料保密」。連線控制在於確保機密性資料只能由被授權的使用者存取；而資料保密則關心透過無線網路傳遞的資料只能被特定使用者接收與解讀。

根據最近研究報告指出，目前業界廣泛使用的無線網路協定 802.11 標準－WEP（Wired Equivalent Privacy），被發現了幾處易受攻擊的弱點，其 RC4 加密演算法極可能透露了幾個金鑰的小片段，而未經授權的使用者便可利用這些片段，獲得一支存取無線網路所必須的金鑰（WEP Key）。

802.11 ≠安全

802.11 標準在連線控制方面，制定了兩種無線網路客戶端認證機制；包含開放式與共享金鑰式。除此之外，尚有兩種機制也常被採用，即為服務識別碼 SSID（Service Set Identifier）和 MAC 位址認證。有關這四種認證方法的原理與弱點分析，將在下面的文章中作進一步的說明。

至於資料保密的設計，802.11 標準則採用 WEP 加密法來保護無線網路基地台與客戶端網路介面間的資料安全。其加密方式為利用 40 位元或 128 位元長度的金鑰，透過 RC4 演算法對資料進行加密。

WEP 金鑰還可被視為一種控制存取的機制，當使用者缺少 WEP 金鑰時，將無法從無線網路存取點接收或傳送資料。

一、認識 802.11 認證機制

802.11 標準規格中所規定的認證方式，其認證對象為無線網路設備，而不是真正的使用者。此認證程序包含下列幾個步驟：

1. 客戶端對每一個頻道廣播探索要求（Probe Request）。
2. 服務範圍內之基地台傳送一個探索回應（Probe Response）的訊框到客戶端。

3. 客戶端選擇一個最適合的基地台，並傳送認證要求（Authentication Request）給該基地台。
4. 基地台傳送認證回應（Authentication Response）。
5. 當認證成功時，客戶端將會傳送一個連結要求（Association Request）的訊框給基地台。
6. 基地台傳送連結回應（Association Response）。
7. 客戶端可開始由基地台傳送與接收資料。

開放式認證

開放式認證本身是一種無效的認證演算法，如果沒有配合資料加密的技術，無線網路基地台將會准予任何來自客戶端的認證要求，亦即任何知道基地台 SSID 的客戶端裝置，都可以連線到此網路中。但若基地台使用了 WEP 資料加密，WEP 金鑰就成為了另一種存取控制機制。假設沒有 WEP 金鑰，客戶端就算是通過了認證，也無法傳送資料到基地台，更不用說將基地台傳送出來的資料解碼了。

共享金鑰式認證

共享金鑰式認證是 802.11 標準中的第二種認證模式，其要求客戶端先設定一個靜態的 WEP 金鑰，並且：

1. 客戶端將共享金鑰的認證要求（Authentication Request）傳送給基地台。
2. 基地台再傳送認證回應（Authentication Response），而其中包含了一個認證字串。
3. 客戶端使用其設定的 WEP 金鑰將該認證字串加密編碼，之後再傳送一個包含此加密資訊的認證要求（Authentication Request）給基地台。
4. 如果基地台可以成功地解密該資訊，且此資訊能與原傳送之認證字串相符合，則基地台將傳送連結回應（Association Response）並開放與該客戶端之連結。

服務識別碼 SSID

SSID 主要是用來劃分不同無線網路服務的區域，一般而言，客戶端需要設定適當的服務識別碼才能存取到無線網路。不過，SSID 並不提供任何資料保密的功能，也不完全提供客戶端連接到無線網路存取點的認證機制。

MAC 位址認證

MAC 位址認證並不包含於 802.11 標準中，但是有很多無線網路設備供應

商，包含 Cisco 在內都支援此法，其運作邏輯為基地台可針對事先設定好的 MAC 位址名單，或是透過認證伺服器來對客戶端進行認證；主要目的是加強開放式與共享金鑰式的認證機制，進一步限制未經過授權的客戶端裝置對網路進行存取的動作。

二、窺探認證機制的漏洞

開放式認證

如同前面所述，開放式認證本身並沒有辦法辨識要求授權的客戶端是否有效，因此若不搭配 WEP 加密技術，等於是對使用者主動敞開了一扇進入無線網路的大門。

共享金鑰式認證

當駭客對無線網路進行竊聽時，其可同時取得基地台傳送出的認證字串與客戶端回應的加密字串。根據 RC4 演算法，加密字串是由認證字串與 WEP 金鑰進行 XOR 運算所得的結果，因此，駭客也只要利用此運算法，便能輕易破解並獲得 WEP 金鑰。

就算駭客無法同時取得認證字串及客戶端回應的加密字串，目前 Internet 中隨手可得破解工具程式，即使經過 128 位元長度金鑰編碼的資料，都可在 15 分鐘內被破解。

服務識別碼 SSID

SSID 最初之用途並非在於安全方面，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，例如 Sniffer Pro，即可從資料封包中找出基地台的 SSID 來。

MAC 位址認證

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，取得一可用的 MAC 位址。

如何獲得更高的安全性？

在綜合上述四種認證制度的弱點分析後，Cisco 為了協助企業在無線網路建置時，能獲得更進一步的安全性，便採用了下列幾個技術，以彌補 802.11 的不足。分別為網路層的加密技術 IP Security（IPSec），以及基於相互認證、金鑰發送方式的 802.1x 標準。

IPSec

IPSec 是一種開放式的通訊協定，能確保私有資料在 IP 網路上傳送時的安全性。如要在無線網路環境中使用 IPSec，必須在每個無線網路客戶端安裝 IPSec，

並且在無線網路基地台和有線網路中間架設 VPN 閘道，而任何無線網路客戶端要傳送至有線網路的通訊，也都必須建立 IPSec 通道。

IPSec 使用 3DES 演算法，並利用 3 個不同的金鑰將資料加密三次，藉此確保資料的安全性。

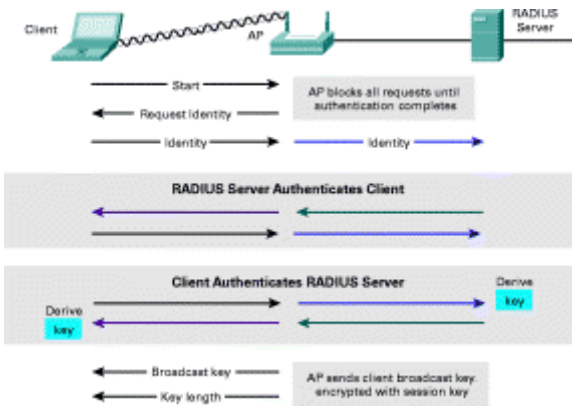
802.1x 與 EAP 標準

除了 IPSec 之外，Cisco 亦積極推動新一代的無線網路安全標準 IEEE 802.1x 與 EAP（Extensible Authentication Protocol；可擴充式驗證協定），讓企業可採用符合標準且能集中管理的安全性架構，來部署數千個使用者的無線網路環境。EAP 允許無線網路客戶端使用數種不同的認證方式，來與後端的認證伺服器如 RADIUS 溝通。而 802.1X 則是一種控制通訊埠為主的網路存取控制協定。

Cisco 符合 Wi-Fi（IEEE 802.11b）標準的 Aironet 系列無線網路產品則採用了 LEAP（Lightweight Extensible Authentication Protocol）技術，包括動態性地發給每個無線網路客戶端，每次連線階段之不同的 WEP 金鑰；其整合性的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，大大減少網路可受攻擊的範圍。如此不僅解除了前述 WEP 標準所受到的限制，企業更可藉由這些技術順利的部署其無線網路環境。

嚴謹的客戶端認證程序

依照 802.11 的認證程序，當基地台接受客戶端的連結後，即允許客戶端開始傳送資料。但 LEAP 會先強迫連線處於未授權模式，並只讓 802.1x 的資料通過，其它像 DHCP（Dynamic Host Configuration Protocol）、HTTP（Hypertext Transfer Protocol）、FTP（File Transfer Protocol）、SMTP（Simple Message Transfer Protocol）以及 POP3（Post Office Protocol 3）等通訊協定都將遭到限制。



當客戶端傳送 EAP-Start 封包時，即開始了 EAP 認證程序。基地台接著會傳送 EAP-Request Identity 身分需求封包給客戶端，並要求客戶端提供身分辨識的資訊。客戶端所回傳之 EAP-Response 封包與身分辨識資訊，將由部署於企業分公司的無線網路基地台，透過 WAN 將認證要求傳送回總公司的認證伺服器中，例如 ACS、Access Control Server 或是 RADIUS（Remote Access Dial-In User Service Server)。之後無線網路基地會根據認證伺服器的授權結果來開放或拒絕

客戶端的通訊連結。

除此之外，EAP 可設定為針對不同的使用者，或是不同的連線階段發給獨立的 WEP 金鑰，甚或是設定為每隔一段時間即自動更換金鑰，以避免金鑰被破解或是洩漏出去。

結論

如前言所述，無線網路可為使用者帶來高度的方便性與工作彈性，但使用無線網路傳輸資料，就如同使用廣播系統散播訊息一樣的「開放」。因此如何防止有心人士監「聽」到您的資料，便成了企業建置無線網路時最需關心的課題。雖然目前市場上遍佈著各式各樣的基地台與網路卡，要架設出一個無線網路環境並非難事，但如何能達到高安全的無線網路設定，或是選擇出支援高安全性標準的產品，絕對是值得企業者再多加研究與多付出一點耐心的。