****
TWCERT/CC 技術專欄
****

■ 無線網路

從早先的撥接, 到現在的 ADSL / Cable 寬頻上網, 網路已經成為許多人日常生活的一部份, 而無線上網正醞釀著下一波的潮流。無線上網的遠景是架構出一個無論何時何地都能快速連上網路, 不再侷限於家中、辦公室等等。無線網路正急速的成長, 相對的, 這項技術將成為另一個網路安全必須注意的環節。

早在 1999 年, IEEE 提出 802.11 無線區域網路標準(Wireless Local Area Networks), WLANs 因此誕生。 WLANs 目前適合用來建構中小型的區域網路, 例如家中、辦公室、圖書館等, 跟傳統的有線網路比起來節省了佈線的成本, 而且能更快速的架構起網路環境, 對於使用者本身而言, 方便的是使用者已經不再需要侷限於網路插座所在的位置, 可以隨意將支援無線網路的設備帶到任何可以存取無線網路的位置, 然後就可以使用網路。

雖然無線網路十分的方便, 但是在安全性上有其欠缺考量的地方, 其標準的安全機制具有嚴重的漏洞存在, 使得有心人士能非法存取無線網路, 使得在無線網路上傳輸的資料無法受到保障, 另一方面, 有心人士也可能使用您的無線網路來進行對外的一些攻擊行為, 這可能使您成為代罪羔羊。

無線網路安全弱點

雖然802.11b 有提供一些基本的安全機制, 但是這些都已經被證實有漏洞存在, 無法確保您的網路安全, 以下是一些關於這些安全機制潛在的問題：

Access Point (AP) 這個裝置通常會接上有線網路, 提供無線網路存取外界資訊, 每隔一定的時間會送出一個 'Beacon Frames' 內容包含有 relay information, timestamp, SSID (Service Set Identifier) 等, 因為這個特性讓無線網路設備不需要讓使用者設定 SSID 就能自行搜尋頻道找到合用的 SSID , 即能接上網路, 但是這也使得外界的人容易探測到無線網路的存在, 並取得一些像是 SSID 這類較為敏感的訊息。

AP 和無線網路裝置之間要做任何的連線, 必須要先經過一段協調過程, 這個過程稱為 'associating'。這個步驟完成後可以立即要求進行認證程序, 而這個步驟有兩個方式可以達成, 第一種是 open system authentication, 另一種為 shared key authentication。

預設的機制是 open system authentication, 使用這個機制的話任何人都可以透過AP進行連線, 不提供任何安全機制, 任何人只要有正確的 SSID 就可以透過 AP 進行網路的存取, 在這種狀況下等於是毫無保障可言。反之, 如果設定成 shared key authentitcation, AP 和使用者之間就會開始進行一段 Challenge-Response 的認證過程, client 必須先送一個 association requst 給 AP, AP 回應一個 128 bits 長度的 challenge text, 然後 client 使用 shared key 加密後返回, 如果返回後的加密字串正確無誤, AP 就會允許 client 建立連線。

這個方法的弱點在於使用明文傳輸 challenge text 以及加密過的 challenge text, 攻擊者使用竊聽的技巧來竊聽這整個過程, 就有辦法取得整個加密過程中三個變數中的兩個, 將其套入 RC4 的運算式中, 攻擊者就有辦法得到 shared key, 而且由於同一把 shared key 用於 shared key authentication 和之後的 WEP, 一旦這把 key 被破解, 接下來所有的通訊內容都有辦法被反解回明碼, 這將使得這項安全機制毫無保障可言。

Wired Equivalent Privacy (WEP) 預期提供一個跟使用有線網路一樣的安全等級, WEP 會加密每個封包, 然而其使用的加密法 RC4 有著先天的問題, 加上 WEP 後天的缺陷使得 WEP 變得毫無效力可言。RC4 一開始使用 40bits 的 WEP key 和 24bits 的亂數產生一個 Initialization Vector (IV) 來加密資料, 雖然監聽這個無線網路的攻擊者也能接收到這些資訊, 但是攻擊者無法得知加密前的 WEP key 是什麼, 因為沒有足夠的資訊去推論出來。

但是攻擊者可以使用 IV 先天上的數值限制來找出 WEP key, 由於 IV 中 random 數字的長度只有 24 bits , 就數學上來說 IV 只有 2^24 次方可能的值, 只要取得足夠的封包, 最後 IV 又會在資料流中開始重複的產生, 竊聽到這些加密的資料攻擊者很快就能取得用一個又一個用同樣的 IV 加密過的封包。 最後, 取得了足夠的資料作分析, 攻擊者就能取得 WEP key。

還有一種攻擊法是用某些基於部分的 IV 是所謂脆弱的 IV, 某些數字不適合用來當作和 WEB key 產生 IV, 一旦亂數產生這些數字, 用這些 IV 加密的封包就變得很容易破解, 而且攻擊者只要收集到足夠量的封包就一定能挑到用這些 IV 加密過的封包, 然後取得 WEP key。

另外一個 WEP 的問題是 key 的管理, 依照 802.11b 標準, 必須要把每一台無線網路設備設定好適當的 WEP key, 而當因為某些原因必須要改掉這個 key 時(例如這個 key 外流), 若只有一些設備的時候或許還好, 如果是大量的設備使用這個無線網路, 這就不是一

件容易的事情了。

如何保護無線網路

保護 SSID 是保護一個無線網路最基礎該作的事情，也是防護無線網路的第一個關卡，把 SSID 當作密碼來設定，不要使用容易猜到的字串，有些 AP 可以讓使用者取消 beacon frames，而讓要使用該 AP 的使用者自行設定 SSID，這是個基本的方法，設定上也很容易，只是當 SSID 更改時，使用該 SSID 的裝置也要跟著修改，這部分會比較麻煩。另外一種偏向實體的保護措施，比如說建築物內加裝遮蔽訊號的裝置，避免無線訊號外漏等等，讓外界的攻擊者無法探測到內部的無線網路。

另外也可以採用額外的機制來保護無線網路，例如說對 MAC address 進行過濾，但是要注意的是攻擊者也可以透過竊聽合法的 MAC address，進而將自己的 MAC address 修改成那些合法的 MAC address，如此就能存取這個無線網路，而且維護這個合法的 MAC address 清單也不是一件容易的工作。

另一種建議的方式是在 WLANs 上架設 VPN，透過 VPN 來建立一個安全的資料通道，如此可確保在網路上傳輸資料的隱密性，但是 VPN 無法保障在內部網路的安全性，攻擊者只要有辦法取得 WLANs 內合法的 IP，還是可以對其他 WLANs 內的電腦進行入侵，進而透過這些電腦取得對外界網路的存取權。

此外也可使用 802.1x 這項新標準，這是一項作身份認證以及管理金匙的一項標準，透過 802.1x 要使用 WLANs 的使用者都必須透過 AP 和認證伺服器認證通過後，才可進行連結，但是 802.1x 也存在一些漏洞，攻擊者可以進行 Man-In-The-Middle 或是 hijacking 攻擊。

總結

我們建議無線網路的管理者建立多層的安全防護機制，如此會大幅增加攻擊者突破無線網路安全的困難度，並注意一些關於無線網路安全的新技術，如 802.11i 以及 WEP2等。

無線網路發展至今，不論攻擊或是防禦，無線網路安全的技術也一直在進步，以上只是大略提供一些相關的資訊，無法作詳盡完整的描述，然而考量無線網路本身安全性問題的同時，也必須考慮在有線網路上遇到的安全問題，也會發生在無線網路上，例如 DoS，或是在 WLANs 上的電腦存有漏洞造成攻擊者入侵的機會等，這些問題也是破壞無線網路安全的因素之一，因此在架設無線網路上，網路管理者必須要更為全盤的考量，才不至於造成損失。

參考文件

IEEE
http://www.ieee.org/

(In)Security of the WEP algorithm
http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

IEEE 802.1X
http://standards.ieee.org/getieee802/download/802.1X-2001.pdf

Unofficial 802.11 Security Page
http://www.drizzle.com/~aboba/IEEE/

Wireless Security Blackpaper
http://www.arstechnica.com/paedia/w/wireless/security-1.html