Computer Network Laboratory

Wireless Authentication, Authorization and Accounting

Members 第10組

- B01501085 莊東諺：貢獻 1/6，架設實驗環境、連接 AP
- B03902087 周景軒：貢獻 1/6，架設實驗環境、整合實驗步驟、提供 Windows
- B03902023 尤沐惠：貢獻 1/6，架設實驗環境、撰寫 PHP
- B00401062 羅文斌：貢獻 1/6，架設實驗環境、整理結報
- B01902051 張君瑋：貢獻 1/6，架設實驗環境、蒐集結報資料
- B02501091 周宇霖：貢獻 1/6，架設實驗環境、蒐集結報資料

Problems

- WLAN Authentication Mechanism
- 網頁介面

References

1. Computer Networking： A Top-Down Approach 6th Edition
2. https://mjtoolbox.files.wordpress.com/2013/01/aes2.jpg
3. http://www.hsc.fr/ressources/articles/hakin9_wifi/hakin9_wifi_EN.pdf

WLAN Authentication Mechanism

1. **說明目前市面上對於無線區域網路所提出之認證機制其優缺點。**

   認證大致上可以分為兩大類：**無加密認證**、**加密認證**。其中無加密認證又分為**開放系統認證 (Open System. Authentication)**、**封閉系統認證 (Closed System Authentication)**，無加密認證的方式容易透過各種竊聽或嗅探取得 **SSID (Service Set ID)**，因此現今的認證機制主要都是採取加密認證，以下的報告也會針對加密認證進行討論。

   加密認證使用了 shared key 的概念，認證機制在過去近 20 年不斷推陳出新，shared key 其實就是一種為資料加密 (data encryption) 的演算法，以下包括了 WEP、WPA、WPA2。

   IEEE 在 1999 年提出了 802.11 Wired Equivalent Privacy (WEP)，其運作原理如第 2 題所述，其優缺點如下：

   - 優點：很早發展出來的一個加密機制，許多市面上的產品都可以支援此加密方式，在使用者正常使用的情況下，可以放心且廣泛地使用此加密方式。另外如果 shared key 本身的長度夠長，竊取重組的困難度就會提高，假使駭客無法在有效期間內破解，竊取就會失去時效性，而使得攻擊無效，如果又加上時常更換金鑰，可以達到更好的安全性。另外是此演算法相當容易，執行起來很有效率。
   - 缺點：WEP 使用同一把 shared key，加密前後的 data packet 透過無限網路四處廣播傳送，有心人士可以透過監聽將 data packet 的資訊重組回一個完整的鑰匙，最早開始有所謂 40 bytes 的 shared key，後來因為其安全漏洞太大，破解速度快，最後不得不將這個 shared key 的長度提高到 128 bytes，然而仍然無法有效抵擋有心人士的破解。另外一個缺點是，假使認證伺服器端想要更改 shared key，還必須手動調整所有 wireless client 的 shared key，使得頻繁更改金鑰變得相當麻煩複雜。

   WEP 的安全疑慮向來是為人詬病的地方，在 IEEE 還沒有提出新的標準前，企業界即努力發展新的加密方式以推廣自家的產品和無限網路的市場，其中最有名的就是 Wi-Fi Protected Access (WPA)，最先由 Wi-Fi Alliance 發展出來，最後也成功地將此演算法的精神納入 IEEE 802.11i 的標準內，優缺點如下：

   - 優點：改善 WEP 容易破解的缺點，使用了 Temporary Key Integrity Protocol (TKIP) 的方式，每一個封包皆有一個獨特的 encryption key 加密，因為金鑰是動態的更動，此機制大幅增強了安全性，另外 WPA 的設計也強調了與 WEP 的相容性，兩者基本上都使用了相同的 RC4 stream cipher，在使用和建置上面也相當容易。WEP 有分成個人版和企業版，來區分不同的使用需求。
   - 缺點：由於是新提出的機制，加上又被隨後崛起的 WPA2 取代，在市場上的使用率並不是太高，與舊版的作業系統也有相容性的問題。另外因為 WPA 的 overhead 相當大，使得 data packet 變大，延遲真正資料的傳遞速度。

   WPA2 與 IEEE 802.11i 相輔相成，WPA2 需要經過 Wi-Fi Alliance 檢驗，也是市面上將 IEEE 802.11i 實作地最完善的認證機制，其運作方式如第 3 題所述，優缺點如下：

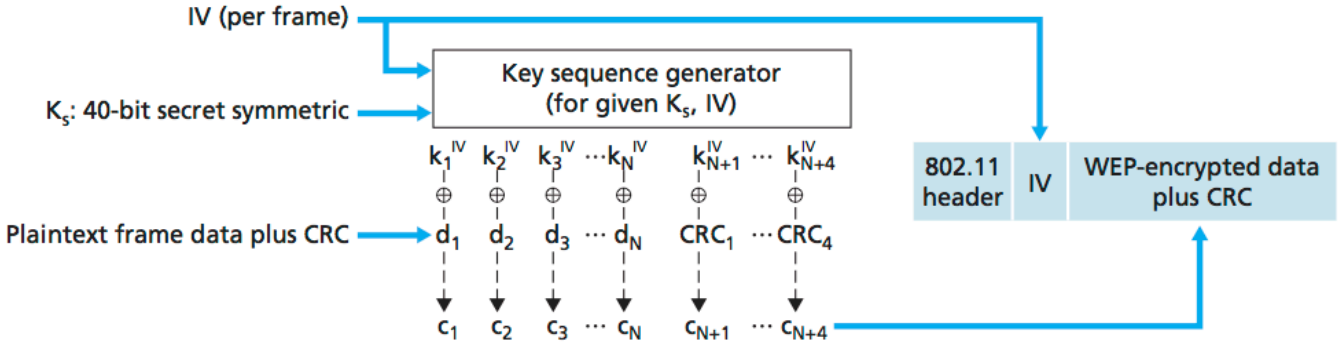
- 優點：為 WPA 的改善版，擺脫了過往 RC4 stream cipher 和 TKIP 的機制，WPA2 發展了新的演算法，稱為 Advanced Encryption Standard (AES) 和 Chaining Message Authentication Code Protocol (CCMP)，是目前市場上最好最安全的選擇之一。
- 缺點：為了提供良好的加密機制，有較高的運算需求，假使網路使用的負荷量過大，往往挑戰 authentication server 的運算處理能力，舊式的 AP 可能無法支援這個較新的技術，即使有支援，速度也會慢上許多。

2. **說明提出之認證機制的運作原理。**

WEP 包含了以下四個步驟：

1. Wireless client 對 AP 提出認證請求
2. AP 傳回 128 byte nonce value 作為 challenge text
3. Wireless client 使用一把與 AP 共享的金鑰 (shared key) 將 nonce 加密後回傳給 AP
4. AP 透過一把相同的金鑰將回傳的 data 解密，假使解密前後的 data 彼此吻合，wireless client 即通過了認證測試

WEP shared key 的運算方式如圖 [1] 所示，首先要透過一個 symmetric shared key (symmetric 暗示 authentication server 和 wireless client 的 key 相同) 產生所謂的 keystream，再加上 CRC，然後將每一個 data packet 與 keystream 的每一個 key 做 XOR 運算來為 data 做加密，若要解密，則使用相同的 key 再做一次 XOR 運算。



3. **說明對於所提出之認證機制其漏洞預防措施為何。**

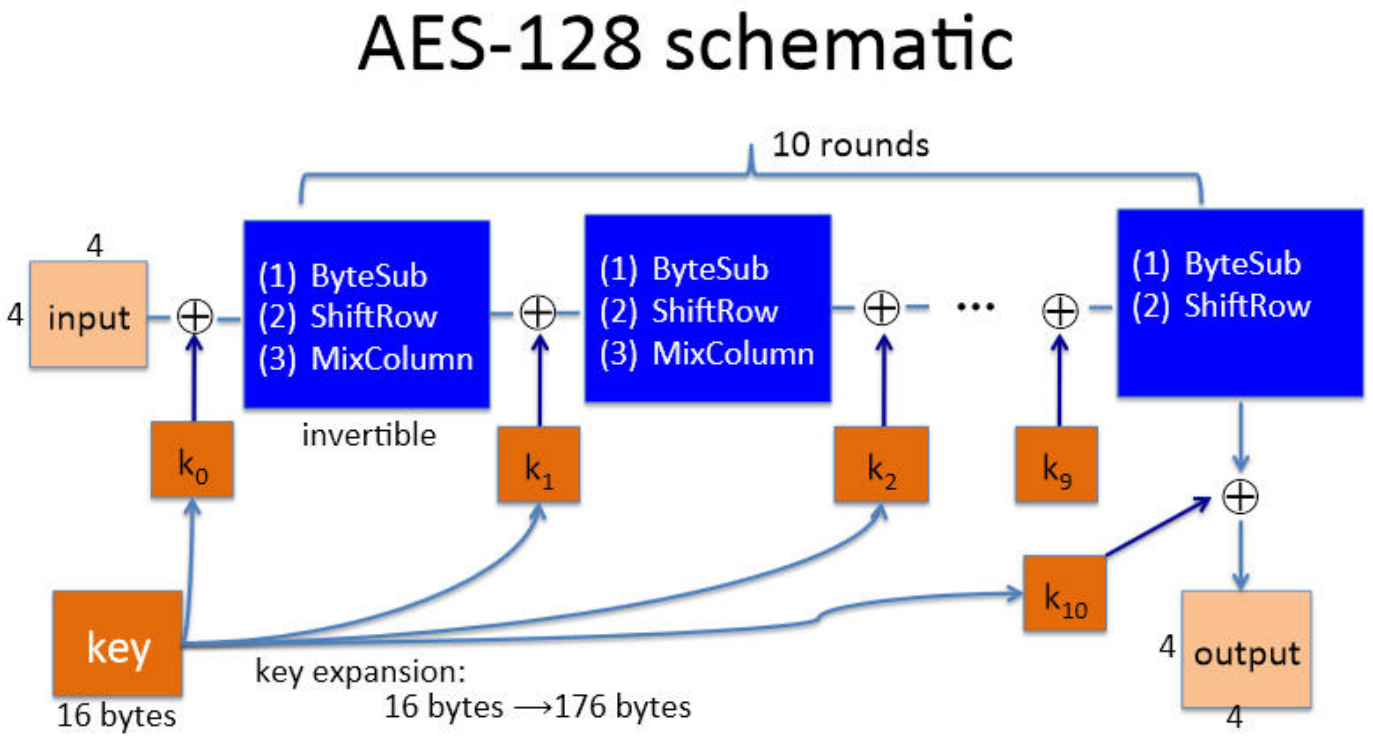
要破解 WEP 不是一件太困難的事情，有鑑於此，IEEE 在 2004 年又提出 802.11i，802.11i 的認證機制，算是相當一大部分解決了 WEP 的安全漏洞，也是目前所能提供的最佳方法，其中的 WPA2 更是將 802.11i 實作得相當完整，IEEE 802.11i 包含了 4 個步驟：

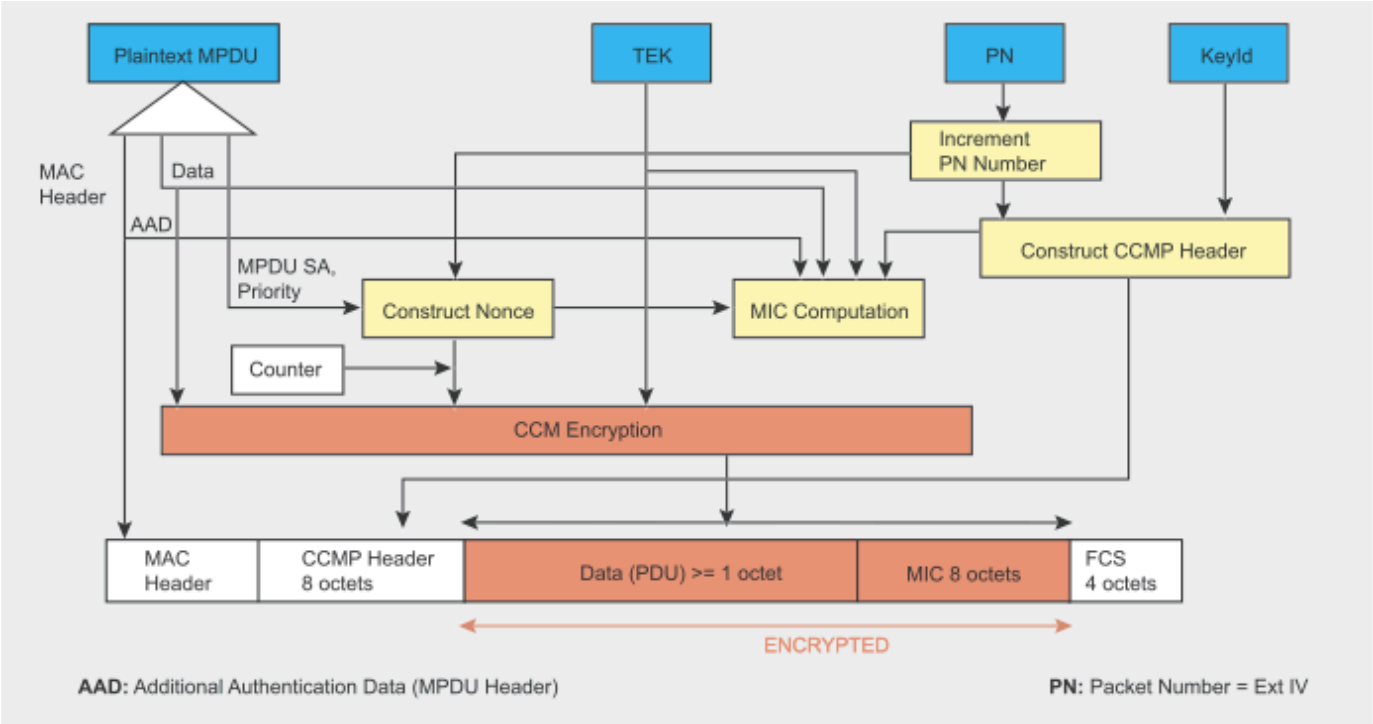
1. Discovery: AP 會對外開放服務，並顯示其認證機制，wireless client 可以透過機器搜尋到 AP 提供的服務與認證。
2. Mutual authentication and Master Key (MK) generation: AP 當作 wireless client 和 authentication server 的中繼站，**Extensible Authentication Protocol (EAP)** 定義了 end-to-end 訊息傳輸的格式，其中 EAP-TLS 的機制廣受使用，wireless client 和 authentication server 彼此交互認證，並產生一把只有彼此都知道的 **master key (MK)**.
3. Pairwise Master Key (PMK) generation: 透過 MK 產生第二把鑰匙 **pairwise master key (PMK)**，

authentication server 將此鑰匙的資訊傳送給 AP。

4. Temporal Key (TK) generation： 建立在 PMK 之上，wireless client 和 authentication server 可以針對不同的訊息傳遞和交易產生特定的 **temporal key (TK)** 再為 data 加密。

WPA2 能提供如此高的安全機制有賴於兩個技術，Advanced Encryption Standard (AES) 和 Chaining Message Authentication Code Protocol (CCMP)，其運算方式如下圖 [2] 所示。AES 有 3 種不同長度的鑰匙，128, 192 和 256 位元，搭配不同的加密 cycle，將 plain text 作 XOR 運算轉為 encrypted text。而 CCMP 只允許經過認證的使用者接收訊息，參考封包號碼和傳送 IP address 產生一個亂數，並使用 block chaining 的方式來確保 data 的完整性。





網頁介面

1. **說明使用之web介面技術。**

   基本上就是以php裡面支援sql的function，連上sql後，藉由讀取$_GET的參數以判斷要做什麼指令，此外也在計時，若滯留時間超過則timeout這樣。

2. **說明你們設計的網頁的運作方式。**

   首先先連上sql，接著判斷目前的頁面（是login還是register還是failed等等），若是login或register就會讀取輸入的帳號跟密碼，並連上sql 進行insert或是select的動作，藉此註冊或是取得登入者資料。