無線網路安全技術之分析與偵測分析系統之設計與實現

戴志坤　　楊中皇
高雄師範大學資訊教育研究所
tai.tomy@gmail.com　chyang@computer.org

摘要

無線區域網路的安全技術主要根據 IEEE 工作小組 TGi（Task Group i）所制定的 WLAN（Wireless LAN）所使用的安全技術 WEP（Wireless Equivalent Protocol）為主，但由於缺乏金鑰交換及認證的技術，已被證實有高度的安全問題，於是 IEEE 及 Wi-Fi 聯盟之後陸續制定了 802.1x、WPA、802.11i 等技術來解決金鑰交換及認證的問題，但其中還是存在一些安全上的顧慮，本論文針對無線區域網路的各項技術分析其可能存在的安全性問題及可能的解決方法，最後根據無線網路安全問題利用 Borland C++設計並實做一安全偵測分析系統，提供管理者在分析安全問題上的一個參考工具。

關鍵詞：無線區域網路、WEP、802.1x、WPA、802.11i

Abstract

Wireless Local Area Network（WLAN）are increasing in popularity. In order to provide secure data communication over wireless link, the 802.11 Task Group i（TGi） proposed the Wired Equivalent Privacy（WEP）to encrypt the data stream and authenticate the wireless device. However, lacking technology of the key exchanging and authentication, WEP has been verified that there are some high security problems. Then IEEE and Wi-Fi alliance made 802.11i、802.1x and WPA to solve these problems, but there are still some among them. The paper addresses possible security problems analysis of these new wireless technology and possible solution. Finally utilize Borland C ++ to design and make a wireless detect and analysis safely system that offer administrators a safe and managerial reference tool .

Keywords: WLAN 、WEP、802.1x、WPA、802.11i

1. 前言

由於無線區域網路不像有線網路需要較高的佈線技術及經費花費，又具有高度的移動性，使無線網路的應用越來越普及，但因傳播訊息的方法採取的是廣播的方式，容易遭受攻擊，而使得資料的機密性（Confidentiality）、完整性（Integrity）、有效性（Availability）受到威脅，如 FMS Attack[11]，利用未加密的 IV 以及其建置的缺失來達到破解加密金鑰的目的，WEP 的安全性已遭瓦解，所幸 WPA、802.1x 到 802.11i 新技術的出現，解決了部份固定金鑰及認證的問題，但新技術在安全上也受到嚴格的考驗，如 WPA 也已經遭到嚴重威脅[8]，WPA 的威脅主要是由於一般人無法記憶太長的密碼，其利用擷取到的交握（handshake）的封包與字典檔作比對，只要有豐富的字典檔，就有可能破解 PSK（Pre-Share Key），同樣的 802.1x 和 802.11i 同樣都有一些安全上的一些疑慮和問題值得我們去研究與探討。

2. 文獻探討

2.1 WEP

早期的無線網路 802.11 是透過 WEP(Wired Equivalent Private)和固定的 WEP Key 機制來做為加密的依據，其最主要是透過 RC4 並配合 40bits 和 104bits 兩種不同的長度的 Wep Key 來做加密，最後採用 24bit 的初始向量（IV）附加在加密資料上。WEP 加密法的缺點有以下幾點

1. 固定的 WEP Key，IV 值太小。
2. 沒有金鑰管理、交換機制。
3. 加密演算法 RC4 是個不安全的演算法[11]。
4. CRC Checkcum 訊息完整檢查碼（ICV）是不安全的，容易遭受到第三者的篡改。

2.2 WEP 破解

2.2.1 暴力攻擊 (Brute-Force Attack)

Tim Newsham發現亂數產生器的瑕疵[7]，將密鑰的可能性從2^{24}降到2^{21}，利用此法破解金鑰長度為40bit的金鑰，不過對於104bit長度較大的金鑰就很難於短時間破解。

2.2.2 FMS 攻擊

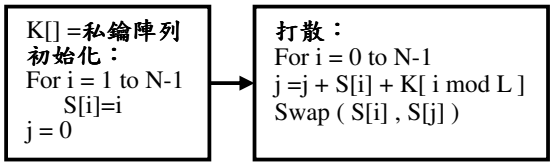
由 Scott Fluhrer，Itsik Mantin 和 Adi Shamir 三位學者所提出的 FMS Attack[10]，利用未加密的 IV 以及其建置的缺失來達到破解加密金鑰的目的。

WEP所使用的加密技術為RC4，是一種同步的串流加密法[10]，利用XOR的邏輯運算結合金鑰串流產生器和明文產生最後輸出的密文，而RC4之所以被稱為串流加密法的原因在於他會隨機產生一個初始向量來產生唯一的金鑰，但這也是其被破解的主要因素。

RC4最主要分成兩個部份

1.金鑰排程法 (Key Schelduling Algorithm，KSA)：

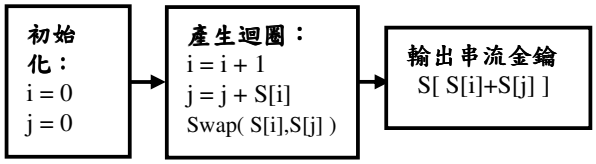
最主要是初始化一個陣列值來作為串流金鑰產生來使用，其過程先排定一個陣列，然後打散其順序。



圖一 KSA 演算法

2.虛擬隨機金鑰產生法(Pseudo Random Generation Algorithm，PRGA)：

首先將兩個變數初始化為 0，然後丟入迴圈為每個封包建立金鑰串流，然後再跟明文做XOR的邏輯運算產生密文。



圖二 PRGA 演算法

WEP破解的因素主要有以下幾點

1. 所使用的IV長度為3byte（24bit），其所能提供的金鑰產生可能為2^{24}＝16777216，但事實上在隨機的選取下可能在傳輸了5000個封包後產生重複的現象，增加了破解的可預測性。
2. 根據IV的缺陷所產生的弱密鑰(Weak Key)[2]，也就是密鑰最後仍會出現在串流的位元組裡的情形，只要蒐集足夠的弱密鑰，就可以反推出金鑰。
3. 幾乎所有的無線封包傳送時都會以SNAP檔頭做為第一個位元組，這個檔頭的值OxAA是由明文的第一個位元和PRGA做XOR邏輯運算後的第一個位元組，這也是WEP的一個重大的缺失。

破解方式（FMS 攻擊）：

假設IV封包格式：B+3、N-1、X（弱密鑰格式）

B：是欲猜測的密碼位元組，但由於密鑰是由IV+共享密鑰，而前三個byte的為明碼，所以在這裡我們設為 0

N：在WEP中均為256

X：可用ASCII、十進位或十六進位來表示從0-255的值，在這裡設定為7

密鑰格式（IV+共享密鑰）：

K[0]	K[1]	K[2]	+	K[3]	K[4]	K[5]	K[6]
3	255	7		?	?	?	?

利用四次的KSA迴圈、PRGA演算法加上SNAP標頭檔位元組OxAA即可反推得第一個金鑰位元。

初始狀態：i=0 j=0 ，S[0]=0 S[1]=1 S[2]=2….S[255] = 255，L = 8

表一 破解流程

KSA first loop1	**KSA second loop2**
j=j+S[i]+K[imodL] =0+S[0]+K[0]=3 S[0]=0，S[3]=3 Swap(S[0]，S[3]) =＞S[0]=3，S[3]=0	i=1，j=3 j=j+S[i]+K[imodL] = 3+S[1]+K[1] = 3+1+255 = 259mod256=3 S[1]=1，S[3]=0 Swap(S[1]，S[3]) =＞S[1]=0，S[3]=1
KSA third loop3	**KSA fourth loop4**
i=2，j=3 j=j+S[i]+K[i mod L] = 3+S[2]+K [2] = 3+2+7=12 S[2]=2，S[12]=12 Swap(S[2]，S[12]) =＞S[2]=12，S[12]=2	i= 3，j=12 j=j +S[i]+K[i mod L] =12+S[3]+K [3] **=12+1+K[3]=？** S[3]=1，S[？]=？ Swap(S[3]，S[？]) =＞S[3] =？，S[？]=1
PRGA i=0，j=0 ，i=i+1=0+1=1，j=j+S[1]=0+0=0 Swap(S[1],S[0])=＞S[1]=3，S[0]=0 **輸出串流金鑰** S[S[1]+S[0]]=S[3]=？	

利用前面所提到加密封包SNAP的第一個位元組為OxAA與利用嗅探軟體所抓取的密文位元組做XOR的邏輯運算Z = OxAA ⊕ CiperText = 170 ⊕ 165 =15（密文資料來源[3]），可得 S[3] = 15 反推 S[15] = 1 得到 K[3] = 15−12−1 = 2破解成功

2.3 802.1x

IETF 於 2001 年制定了 802.1x RADIUS Usage GuideLine 身份認證及密鑰管理協定，802.1x 主要分成客戶端（Supplicant，SP）、認證系統（Authenticator，AP）及認證伺服器（Authentication Server，AS），而 802.1x 機制仍存在以下安全問題

1.中間人攻擊（Man-in-Middle-Attack）

在 802.1x 的驗證系統（Authenticator system）中只能單純的接收客戶端（SP）的 EAP 信息或向客戶端提出 EAP 的請求，無法做到雙向的認證，有可能會遭受的中間人的攻擊，這也是 802.1x 設計最大的缺陷，Attacker 可先假冒 AP 發出一個 EAP succeed 訊息給 SP，因為 SP 沒有對 AP 認證的機制[2]，所以會把 Attacker 當作合法的 AP 開始傳送資料，Attack 就可以開始中間人攻擊。

2.會話劫持（Session Hijacking）

Attacker 在客戶端與認證系統完成認證後，對客戶端發動攻擊，使其無法工作，但此時認證系統對客戶端仍處與認證完成的階段，Attacker 可以利用客戶端的 MAC 取得認證系統的服務，達到攻擊的目的。

3.阻斷攻擊（Denial-of-Service，DoS）

802.1x 的協定中的 DoS 攻擊可分為兩階段，第一階段：當客戶端未完成驗證時，驗證系統發送一個 EAP-Failure 的封包給客戶端，然後客戶端保持 HELD 的狀態，此時 Attacker 可以冒充驗證系統，對客戶端每 60 秒送出一個 EAP-Failure 的封包，欺騙客戶端使用者，達到阻斷目的。第二階段：驗證如已完成，Attacker 會冒充客戶端送出中止服務的 EAP-logoff 的封包，欺騙驗證系統，阻斷服務。

目前實現 802.1x 的身份認證技術各家不同，如 EAP-TLS、EAP-TTLS、LEAP 等都具有雙向認證的技術，可預防中間人攻擊。

2.4 802.11i

WI-FI聯盟針對WEP的缺失，提出過渡的解決方案WPA（Wi-Fi Protected Access)，但WPA的出現雖然解決了一些WEP的問題，但也產生了一些新的問題，在安全度上反而沒有更大的提升[9]，在IEEE通過了802.11i之後安全性才獲肯定。

802.11i最主要分成兩個部分

1. PRE－RSNA：包含之前的WEP和802.11實體的認證。
2. RSNA（Robust Security Network Association）：結合802.1x、TKIP（Temporal Key Integrity Protocol）、CCMP（Counetr-mode/CBC-MAC）。

2.4.1 TKIP

TKIP加密特性如下：

1. 使用48bits的IV值（WEP所使用的為24bits）
2. 每個Packet都會產生不同的加密金鑰，而WEP會將IV直接與WEP Key經過RC4演算法之後來做加密的RC4 Key，而TKIP只是把IV當作加密的參數。
3. 使用的Key分成兩個部份，128bits的Key用於金鑰混合，另外64bits的Key用於Michael演算法[3]。
4. 訊息完整碼MIC（Message Integrity Code）使用Michael演算法雖然強大，但須配合Sequence Number的使用尚可達到安全標準[3]
5. 仍然使用有缺陷的RC4加密演算法。
6. 與目前硬體相容性較佳。

2.4.2 CCMP

CCMP（Counetr-mode/CBC-MAC）與 TKIP 許多相似的特性，為長期解決 wireless 的方案，特性如下：

1. 使用 48bits 的 IV 值。
2. 使用 AES（Advanced Encryption Standard）演算法，但目前尚未經過完整的測試，且相容性低，執行難度高。
3. 不對每個封包加密，而是對所有封包，並利用使用 CTR（Counetr）模式，因為沒有對每個封包實施加密的程序，也變成在安全上的一個缺點。
4. 資料完整性的部分使用的 CBC-MAC 比 TKI

P 所提供的 Michael 演算法強大，提供 8-octet 的 MIC（Message Integrity Check），而且在加密資料最後不加 ICV（Integrity Check Value），比 WEP 的 CRC 的安全性提高很多。

5. 在資料的加密和完整性使用同樣的 Key。

2.4.3 RSNA 的機制

802.11i RSNA 機制主要分成 802.1x 和金鑰的管理，由 Supplicant（SP）、Authenticator(AP)、Authentication Server（AS）三個實體及六大步驟[4]

1. 網路及安全能力檢測

AP 會在特殊的通道上週期性的廣播 RSN IE（Robust Scurity Network Information Element），並且會偵測探測請求（Probe Request）及回應請求，SP 也可以在此時藉由被動的偵測 Beacon Frames 或主動偵測所有頻道（channel）來搜尋可用的 AP。

2. 認證（Authentication）與連結（Association）

這個階段 SP 會選擇適合連線的 AP，嘗試對 AP 進行認證與連結

3. EAP、802.1x、RADIUS 認證

SP 和 AS 會在此階段交互認證，認證完成後會產生一個共用的 Key，叫做 MSK（Master Session Key），SP 會利用 MSK 產生 PMK（Pairewise Master Key），然後 AS 也會將 PMK 傳給 AP 產生相同的 PMK。在這個階段如果 SP 和 AP 使用 PSK（Pre-Shared Key）來註冊，則這個階段可以省略。

4. 四向交握（4-Way Handshake）

四向交握對於建立成功的 RSNA 是必要的[9]，這個階段最主要驗證 SP 和 AP 在第三步驟所產生的 PMK 和選擇加密的機制（Ciper suite），且產生一個 Session Key，PTK（Pairwise Transient Key），作為之後資料加密的依據，此階段在 PMK 產生後開始[4]，由 AP 開始。

5. Group Key 的交握

這個階段 AP 會產生 GTK（Group Trasient Key），並分送給 SP 使用，此階段的工作如果於第四階段執行的話可省略。

6.加密資料的傳輸

使用 PTK 或 GTK 來進行資料加密及傳輸。

雖然 RSNA 的機制已算完備，但還是有可能遭受攻擊，分析如下：

1. **回滾攻擊（Rollback Attack）**

雖然 802.11i 中並沒有規範一個 TSN（Transient Security Network）同時支援 Pre-RSNA 和 RSNA，但這種情形在一般使用的情況下可能發生，當 Pre-RSNA 和 RSNA 同時執行時，會遭受到此攻擊，在執行 Pre-RSNA 的情況下，Attacker 此時可扮演類似中間人的角色，交替扮演，會冒充 AP 發出一個偽造的 Beacon 或探測回應封包（Probe-Response frames），也會冒充 SP 來發出偽造的連線請求（Association Request），達到竊取金鑰的目的

解決方式：

（1） SP 和 AP 均使用 RSNA，但會缺乏彈性和相容性

（2） 能提供一個 Pre-RSNA 與 RSNA 兼具並有安全選擇機制的 TSN（Transient Security Network），提供使用者選擇其所需要的安全層級，需要安全性較高的資料可選擇 RSNA。

2. 反射攻擊（Reflection Attack）

在一般的無線網路基礎建設中，一台主機不可能同時扮演 SP 和 AP，但在支援 802.11i 協定的 IBSS 網路中，這種情形是有可能的，IBSS 是一種 ad hoc LAN 的應用，沒有 AP，所以每台主機都有可能扮演 AP 和 SP。在這種情況下使用 802.11i 建立 RSNA 之四向交握（4-Way Handshake），可能會遭受到此攻擊，Attacker 會扮演一個受害的主機發出特殊封包，使合法的 AP 回應，最後完成四向交握。雖然反射攻擊並不能在這個攻擊行動中獲得之後合法的加密金鑰，但仍破壞原有的交握機制。

解決方式：

（1） 要能避免此狀況發生，一台主機所扮演的角色要單一化，也是就在 ad hoc 網路下，固定主機擔任類似像 AP 功能。

（2） 如果在同一台主機上扮演兩種角色，可使用不同的 PMK，不過此方法會增加交握的複雜度。

3. 阻斷攻擊（DoS,Denial of Server）

由於 802.11i 所定義的部份是在資料鏈結層，

在認證層級之下，故認證的部份並沒有規定，各家不同，因此在這個部份，如果未選用具有雙向認證及動態金鑰加密的話，則可能遭受到攻擊。

綜上所述，在無線區域網路中，要做到雙向驗證的機制、動態金鑰的交換、資料完正整性的保護、建立錯誤回復機制，才能將傷害減至最低。

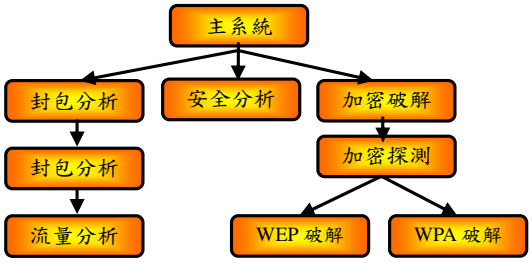
表二 WEP、TKIP、CCMP 的比較

	WEP	TKIP	CCMP
加密演算法	RC4	RC4	AES
金鑰的長度	40bit 104bit	認證：64bit 加密：128bit	128-bit
初始向量	24-bit	48-bit	48-bit
每個封包之加密金鑰	IV+ WEP Key	兩階段金鑰融合	無
金鑰管理	無	802.1x	802.1x
資料完整性	CRC	Michael	CCM

2.5 系統實做

本系統以利用 Windump、Aircrack、Nmap、WepLab 等破解及擷取封包開放原始碼軟體，以 Microsoft Windows XP 為平台、結合 Microsoft Visual C++ 6.0 與 Borland C++ Builder 6.0，以視窗化的介面來呈現，以便於使用。

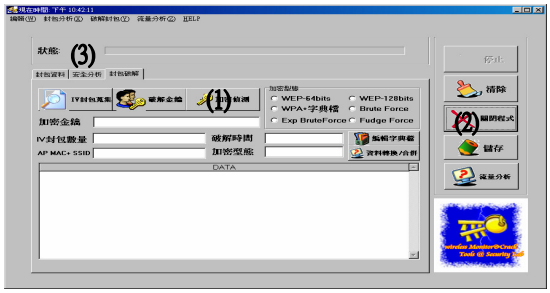
系統硬體：CPU：Pentium Celeron 1.3GHz、記憶體 512 MB



圖三 系統架構

2.5.1 系統說明

1.系統介面



圖四 系統介面

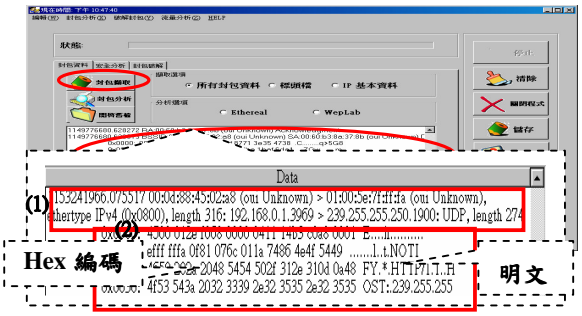
（1） 主功能介面：包含封包分析、安全分析、破解分析、流量分析。
（2） 基本操作功能
（3） 狀態列

2.5.2 功能介紹

（1） 封包分析

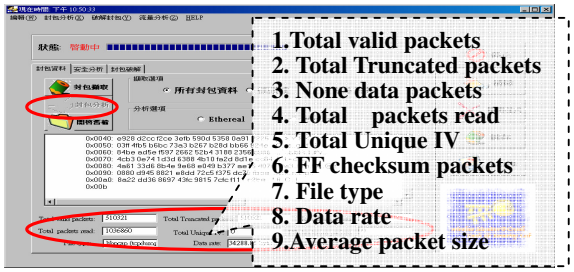
操作流程：選取網卡→封包擷取→封包分析

可以需要選擇擷取所有封包、標頭檔及 IP 基本資料的功能，可分析擷取各類不同封包個數。



圖五 封包資料

（1）AP 通訊協定、IP、MAC 位址、UDP、封包長度等資訊
（2）封包編碼及明文資料



圖六 封包分析

（2） 加密破解

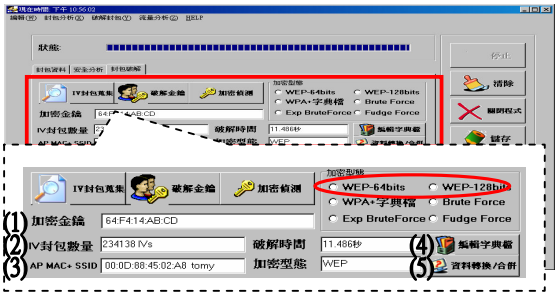
操作流程：擷取 IV 封包→選擇加密型態（加密型態可自動偵測可不選取）→破解

主要分成 WEP 64、128 bits 和 WPA-PSK 破解，破解後顯示（1）加密金鑰（2）IV 封包量（3）AP 的 SSID 和 MAC address（4）破解時間（5）加密型態。

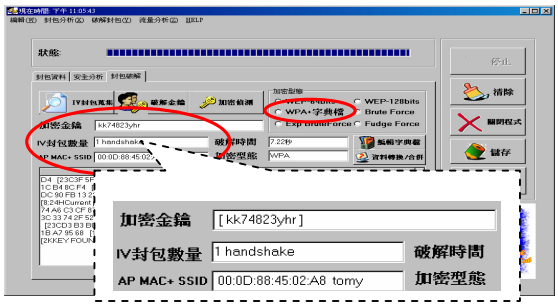
- WEP 64 bits：蒐集含 IV 封包大約須 10 萬-20 萬，破解時間不定，取決密碼設定的複雜度，但一般於 1 分鐘內均可破解。
- WEP 128 bits：蒐集含 IV 封包大約須 90 萬-

100 萬，破解時間 3-5 分鐘。

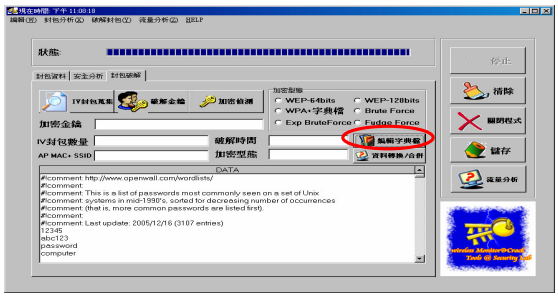
- WPA：需擷取到具有交握（Handshake）封包並配合字典檔才可破解，破解的可能取決於字典檔的豐富性，本系統提供字典檔的編輯。



圖七　破解 WEP 加密

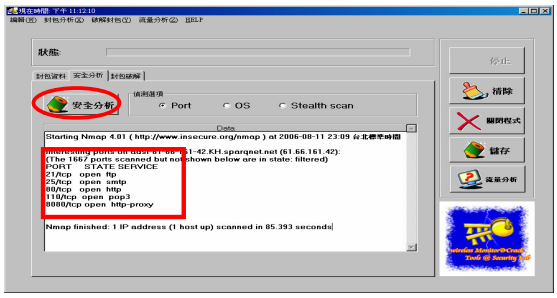


圖八 破解 WPA-PSK



圖九 字典檔編輯

（3）　安全分析



圖十 安全分析

操作流程：輸入無線 AP IP Address→安全分析

此功能可分析 AP 的安全性問題，包含開放的 PORT、使用軟體的版本等。

3. 結論

無線網路的普及提供給人們使用網路上一個更方便的選擇，由於它的機動性（Mobility）高，不需佈線的優點，使得普及率越來越高，但也因傳播的介質是空氣，遭到攻擊的機會也變高，本系統整合開放原始碼工具，實做便利使用的視窗介面，提供封包分析、安全分析及封包破解的功能，可提供管理者在無線區網的安全管理上一些建議與幫助。

4. 參考文獻

[1] 蔡孟凱、雷穎傑、黃昭維、陳錦輝、陳正凱(2003) ."C++ Builder 6 完全攻略”，金禾資訊。

[2] 賴溪松，韓亮，張真誠，近代密碼學及其應用，松崗書局。

[3] Reverse engineering of AirCrack software, http://asi.insa-rouen.fr/~lfallet/docs/concordia/aircrack.pdf

[4] Changhua He、John C Mitchell, Security Analysis and Improvements for IEEE 802.11i, http://www.isoc.org/isoc/conferences/ndss/05/proceedings/papers/NDSS05-1107.pdf

[5] Donald Welch, Senior Member, IEEE, and Scott Lathrop,Wireless Security Threat Taxonomy, In Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society, Page 76-83, 2003

[6] Hal Berghel and Jacob Uecker, WiFi Attack Vectors, In Communications of the ACM, 2005

[7] T. Newsham, Cracking Wep Key, http://www.lava.net/~newsham/wlan/WEP_password_cracker.ppt

[8] Nancy Cam-Winget, Russ Housley, David Wagner, and Jesse Walker，Security Flaws in 802.11 Data Link Protocol, In Communications of the ACM, Page 35-39, 2003

[9] Ross Hytnen and Mario Garcia,AN ANALYSIS OF WIRELESS SECURITY*,In Journal of Computing Sciences in Colleges, Page 210-216, 2006

[10] Scott Fluhrer,Itsik Mantin,and Adi Shamir , Weakness in the Key Scheduling Algorithm of RC4, http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf