最佳化的 WEP 加密機制
(Optimized WEP Protocol)

黃定宇	林韓禹	鄭家明	葉義雄
國立交通大學	國立交通大學	國立交通大學	國立交通大學
資訊工程系	資訊工程系	資訊工程系	資訊工程系
hdy00000@gmail.com	hanyu.cs94g@nctu.edu.tw	t3702020@yahoo.com.tw	ysyeh@csie.nctu.edu.tw

摘要

有鑑於無線網路所提供的機動性，只要使用者處於基地台的服務範圍，就能使用相關的網路資源；具有高度的便利性，使得無線網路的使用人數逐年增加。此外，不論是在固定(有線)網路或者無線網路下，網路安全始終是一門相當重要的議題。本篇論文即針對無線網路中的加密機制 WEP 所遭遇到的安全性上的漏洞，包括附加於封包後的初始向量為明文、無法抵抗重送攻擊及可靠性等問題，提出最佳化的解決方法。相較於遵守 IEEE 802.11i 標準所規範的 WPA，改良後的 WEP 僅需要執行軟體上的更新，而不須硬體上的變動。

關鍵詞：初始向量、安全漏洞、弱點金鑰、無線網路。

Abstract

The mobility offered by wireless networks enables users to have the access to related network resources if they are within served area of access points. Owing to the convenience of wireless networks, the population of it users are getting more and more. In addition, network security is always a vital issue for either the Ethernet or wireless networks. This paper presented an optimized solution to eliminate the security holes of WEP (Wired Equivalent Privacy) which includes the plaintext transmission of IV, vulnerable to replay attacks and the reliability problem. As compared with WPA (Wi-Fi Protected Access) which complies with the standard of IEEE 802.11i, optimized WEP (O-WEP) only requires the update of software instead of modifying any hardware equipments.

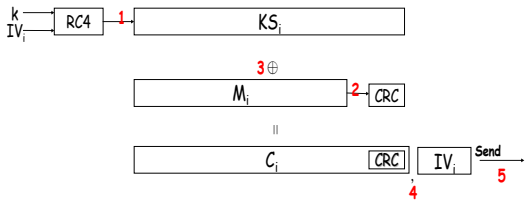
Keywords: initial vector, security holes, weak key, wireless networks

一、前言

自 2006 年中至 2007 年 3 月為止，無線網路(Wireless Networks)的使用者中，有高達 46.3%的使用者利用 WEP (Wired Equivalent Privacy) [2]做為網路安全的加密機制，另外有 19.6%使用 WPA (Wi-Fi Protected Access) [5]。從這些數據可以發現，WEP 仍然是目前無線網路中最受歡的加密機制。WEP 被定義在 IEEE 802.11 的第二個版本 802.11b 中，並提供了安全性的相關服務，包含資料的私密性、完整性、資料來源的驗證。2001 年 8 月 Fluhrer 等人提出針對 WEP 而發展出來的統計攻擊(FMS attack) [1]，利用初始向量以及 RC4 的性質，在無線網路中收集足夠的封包後，針對以(B + 3)：FF：N 格式的弱點金鑰(weak key) [4]進行攻擊，再還原出 RC4 金鑰。即便如此，WEP 仍然是目前無線網路中被廣範使用的加密機制。本論文之方法，在不更新硬體的情況下，使用雜湊訊息認證碼(HMAC) [3]來改善目前 WEP 的安全性，以抵抗重送攻擊(replay attack)和 FMS attack 等攻擊。此外，更可以提供原本使用 WEP 的機構，在完成硬體設備(網卡晶片-802.11g、AP)更新之前的一個最佳替代方案。

二、最佳化的 WEP 加密機制

在介紹最佳化的 WEP 加密機制之前，本節會先討論原 WEP 的架構及其安全性上的漏洞。由於 WEP 採用 RC4 加密演算法，而 RC4 並未要求使用特定長度的金鑰，因此，理論上 WEP 可以搭配任意長度的金鑰。然就目前市面上所看到的 WEP 主要分為 64-bit 和 128-bit 兩種金鑰長度，其中包含 24-bit 的初始向量(initial vector，IV)及 40-bit 和 104-bit 的密鑰。



圖一　WEP 加密示意圖

圖一簡單地描述了一個無線網路中的封包經過 WEP 加密至傳送的過程：

(1). 將已知的密鑰 k 及初始向量 IV 透過 RC4 這個加密演算法產生一金鑰串流 (key stream) KS。
(2). 利用 CRC (Cyclic Redundancy Check) 計算出要傳送訊息 M 的 check sum，並將其附加於 M 之後，令其為 T (= M || check sum)。
(3). 將 T 與金鑰串流 KS 進行互斥(XOR)邏輯運算，以產生密文 C。
(4). 將 IV 附加於密文 C 之後便完成此封包。
(5). 將所產生的封包傳送出去。

根據以上 WEP 加密的過程，可以發現幾個較為明顯的安全漏洞(security holes)如下：

(1). **以明文傳送 24 位元的初始向量：**惡意的攻擊者可以輕易收集到所需要的弱點 IV (weak IV)，再利用此 IV 去對應特定的 RC4 弱點金鑰發動攻擊。

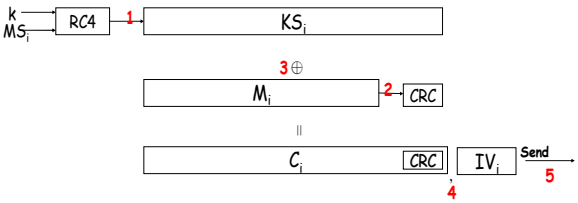
(2). **資料來源的驗證：**對於要傳送的資料，WEP 使用了 CRC 去做完整性的檢查。但完整性的檢查如果不夠完備，傳送的過程中，這些傳送的訊息有可能會被攻擊者所假造，重新計算出完整性檢驗值 (integrity check value，簡稱 ICV)，而不被察覺。

(3). **重覆使用金鑰串流：**用來加密封包的金鑰串流是利用 IV 和密鑰透過 RC4 來重覆產生。WEP 採用此 24 位元 IV 的方式($2^{24} \cong 16{,}777{,}216$)，由生日攻擊法(birthday attack)得知每 4096 (= 2^{12}) 封包發生重覆的狀況機率將大於 1/2。

為補強目前的 WEP 運作架構，本論文提出最佳化的 WEP 加密機制。我們把這個改良後的加密機制稱為 O-WEP。在不需要額外硬體設備的前提下，O-WEP 保留原來 WEP 的封包格式，僅須軟體上的更新，其目的在於以最少的變動來解決當前 WEP 所遭遇到的問題。首先，我們定義以下的符號意義：

k	：	WEP 中的密鑰。
HMAC_k	：	雜湊訊息認證碼，其中 k 為密鑰。
MS_i	：	功能類似原 WEP 中的 IV_i，用來動態產生金鑰串流。
KS_i	：	使用 MS_i 和 k 產生的動態金鑰串流。
M_i	：	第 i 個傳送的訊息。
C_i	：	第 i 個加密後的封包。
CRC	：	完整性檢驗值。

O-WEP 加密流程：圖二為 O-WEP 加密示意圖，其與原來 WEP 架構的差異在於 O-WEP 使用 MS_i 去產生金鑰串流，而非原來的 IV_i。

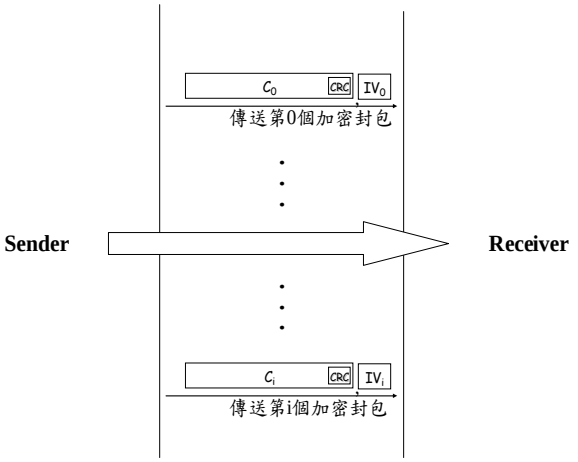


圖二　O-WEP 加密示意圖

MS_i 和 KS_i 的產生方式可由下面式子推得：

$$MS_0 = \mathrm{HMAC}_k(\mathrm{IV}_0) \quad (1)$$
$$MS_i = \mathrm{HMAC}_k(\mathrm{IV}_i, MS_{i-1}) \ \forall i \geq 1 \quad (2)$$
$$KS_i = \mathrm{RC4}(k, MS_i) \ \forall i \geq 0 \quad (3)$$
$$C_i = M_i \oplus KS_i \quad (4)$$

(1)式和(2)式中所使用的 HMAC_k (Hash Message Authentication code)為採用安全雜湊演算法(Secure Hash algorithms，SHAs)所建構的 MAC，其在此的作用為計算所需的 MS_i，式中的 k 即為密鑰(最初是由使用者所設定)。使用 HMAC 的原因在於其已被納入多項國際標準，其中 IP security 的規格要求 MAC 必須以 HMAC 實做，其它如 SSL 等協定以及 NIST 也是採用 HMAC 做為標準。此外，不需大幅修改就可使用現有的雜湊函數，以及能輕易地更換內嵌的雜湊函數(在本篇論文中建議採用 SHA2)，這也是 HMAC 被廣為採用的原因。(3)式以 MS_i 取代原來的 IV_i 帶入 RC4 中產生 KS_i。(4)式則說明密文 C_i 如何產生。

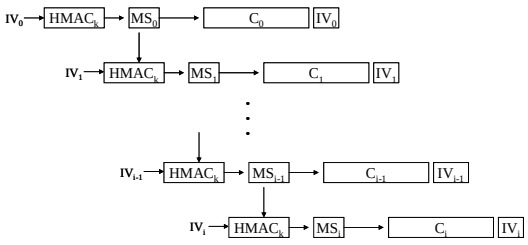


圖三　O-WEP 封包傳送示意圖

圖三說明傳送者和接收者之間封包加解密的過程。考慮以下傳送者對封包做加密時的兩種情況；第一種是對初始封包做加密，另一種則是非初始封包的加密。

(1). **加密初始封包：**當傳送者欲傳送初始封包時，可由(1)式算出 MS_0，再根據(3)式和密鑰 k 運算 RC4 產生 KS_0。利用 KS_0 來加密欲傳送的封包，並將(1)式中使用到的 IV_0 附加於加密的封包後一併傳送出去。當接收者收到此加密封包後，先將封包後的 IV_0 透過(1)式算出 MS_0，即可由(3)式獲得解密用的 KS_0，將封包解密。

(2). **加密非初始封包：**若傳送者欲加密的封包不是初始封包，即($i > 0$)，此時的 MS_i 則由(2)式來產生。然而產生 MS_i 需要 IV_i 以及前一個封包所使用的 MS_{i-1}，這表示每次計算出來的 MS_i 必須保留給下一個要加密的封包使用。同樣地，當接收者在解密時，仍然需要前一個封包所使用的 MS_{i-1}。由圖四即可以看出封包之間加解密的相依性。



圖四　O-WEP 封包之間的相依性示意圖

三、安全性分析

在上一節中，我們使用 HMAC 去改善 WEP 的安全性，本節的內容將會分析改良後的 O-WEP 安全性。

(1). **以明文傳送 24 位元的初始向量：**在 O-WEP 中雖然初始向量仍然是以明文傳送，但是用來加密封包的金鑰串流

(KS_i)不再是以 IV_i 和 k 產生，而是改由 MS_{i-1} 以及 IV_i 產生。假設攻擊者欲採取 FMS attack 收集大量的封包，嘗試去分析加密的金鑰串流，進而推導出密鑰。然而在破解的過程中仍需要 MS_{i-1}，因此，破解的難度將會大幅的提升。

(2). **資料來源的驗證**：從圖四中，我們可以發現 O-WEP 加密時，前後封包的相依性。當遭受到 replay attack 時，此重送或偽造的封包將無法解密及驗證 CRC。因此，非法的傳送過程都將會被偵測到。

(3). **重覆使用金鑰串流**：WEP 使用 24 位元的 IV (約 1600 多萬種)和密鑰去產生金鑰串流。在繁忙的網路傳輸過程中，此 24 位元的 IV 很容易就出現重覆的情形(由生日攻擊法得知每 4096 封包發生重覆的狀況機率將大於 1/2)。而 O-WEP 中用來產生密鑰的 MS_i 是透過 $HMAC_k(MS_{i-1}, IV_i)$ 所產生，假設 $HMAC_k$ 採用的雜湊函數為 SHA-256，此時產生的 MS_{i-1} 長度為 256 位元，金鑰串流重覆使用的機率將大幅度下降(由生日攻擊法得知，每 2^{140} 封包發生重覆的機率才會大於 1/2)。

(4). **可靠性**：在這個部份我們考慮一個問題：當傳送的過程中，發生封包遺失的情形該如何解決？根據圖四可以簡單了解，O-WEP 具有前後封包相依的特性。若有任一封包遺失的情形發生，則下一個封包將無法解密。因此，當接收者發現有封包遺失時，會回傳一個特殊的訊息 M_L 給傳送者。傳送者收到此訊息後，會把遺失的封包重新發送一次。

由上述的分析可以發現，O-WEP 的安全性完全仰賴 $HMAC_k$ 所採用的雜湊函數所決定。以 SHA-256 來說，攻擊者採用生日攻擊法時，破解長度為 256 bits 的訊息摘要，需要 $2^{(256+24)/2}$ 的時間複雜度才能產生一次碰撞，這使得攻擊者要付出相當大的代價。此外，從圖一及圖二中得知，O-WEP 與 WEP 的封包格式相同，並沒有額外增加其它的欄位，因此在網路的部份，O-WEP 並沒有使用到額外的頻寬。至於在額外的計算量上，O-WEP 所需要額外增加的計算量為使用到 $HMAC_k$ 的部份。事實上，$HMAC_k$ 已經被納入多項國際標準，且為一般硬體可支援之演算方法，因此所增加的計算量是系統可以負擔的。

四、結論

本篇論文中描述了目前 WEP 運作架構下的安全漏洞。為補強這些安全漏洞，我們提出最佳化的 WEP 加密機制，稱為 O-WEP，其最大的優點在於不需要任何硬體設備的更新，因此可視為原 WEP 協定的最佳替代方案。與原 WEP 相比較，O-WEP 大幅提升運作的安全性，雖在計算量的部分增加了些微的負擔，但增加的運算量都在一般系統可容許的範圍內。

五、參考資料

[1] S. Fluhrer, I. Mantin and A. Shamir, “Weaknesses in the key scheduling algorithm of RC4”, Selected Areas in Cryptography, pp. 1-24, 2001.

[2] M. S. Gast, 802.11 Wireless Networks: The Definitive Guide, 2e, 2005.

[3] H. Krawczyk, M. Bellare and R. Coretti, “The key-hash massage authentication code (HMAC)”, Federal Information Processing Standards Publication 198, 2002.

[4] E. Tews, R. Weinmann and A. Pyshkin, “Breaking 104 bit WEP in less than 60 seconds”, http://www.aircrack-ng.org.

[5] Wi-Fi Alliance, “Wi-Fi Protected Access (WPA)”, http://www.wi-fi.org.