國立交通大學

網路工程研究所

碩士論文

以HMAC強化WEP加密機制

Enhance WEP Protocol with HMAC

研究生：鄭家明

指導教授：黃世昆　教授

　　　　　葉義雄　教授

中華民國九十七年六月

以 HMAC 強化 WEP 加密機制

Enhance WEP Protocol with HMAC

研究生：鄭家明　　Student：Chia-Ming Cheng

指導教授：黃世昆　　Advisor：Dr. Shih-Kun Huang

葉義雄　　Dr. Yi-Shiung Yeh

國立交通大學

網路工程研究所

碩士論文

A Thesis

Submitted to Institute of Network Engineering

College of Computer Science

National Chiao Tung University

in partial Fulfillment of the Requirements

for the Degree of

Master

in

Computer Science

June 2008

Hsinchu, Taiwan, Republic of China

中華民國九十七年六月

以 HMAC 強化 WEP 加密機制

研究生：鄭家明　　　　　指導教授：黃世昆 博士

葉義雄 博士

國立交通大學網路工程研究所碩士班

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。

Enhance WEP Protocol with HMAC

Student：Chia-Ming Cheng Advisor：Dr. Shih-Kun Huang

Dr. Yi-Shiung Yeh

Institute of Network Engineering College of Computer Science

National Chiao Tung Tuiversity

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.

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

致　　謝

在研究所就讀的這兩年來發生了許多事情，無論是在學問或者待人處事方面都讓我獲益良多。特別感謝定宇、韓禹、鎮宇學長以及靜紋學姊，在我碩士班期間遇到困難時，給了我相當多的寶貴意見，也因為如此這篇論文才能完整呈現。此外，帶著我騎腳踏車並四處比賽的龍哥以及佳君、小強和在交大所認識的朋友們，讓我這兩年的碩士生活更加地多采多姿，祝福他們在未來能夠一帆風順。

而最讓人感到遺憾的則是葉義雄教授在2007年的暑假腦溢血過世，雖然與葉老師相處的時間不長，卻能夠深刻地體會到葉老師愛護學生的心意，在此要對葉老師說一聲謝謝您！！

最後，要感謝評審委員們在口試時給我的各項建議，以及黃世昆教授在論文方面給我的指導。還有家人這麼多年來的栽培與支持，在念書這條路上我並不是一位優秀的學生，但是一路走來無論遇到任何事情，家人的支持始終讓我感到溫馨，僅將這篇論文獻給所有關心我與支持我的人，謝謝你們！！

鄭家明

中華民國九十七年七月

Contents

Figure List

Table List

Chapter 1 Introduction

1.1 Background

Over the past several years, the appearance of wireless network enables users to access network resources immediately and rapidly. Therefore the populations of wireless network users are getting more and more since then. The table 1.1 [4] shows a survey of encryption methods found in the middle of German in March 2007. Another survey was performed in September 2006. According to the table 1.1, Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA)[5] are adopted by 46.3% and 19.6% users of wireless network in March 2007. Both data sets proved that WEP is still the most popular mechanism for securing wireless network.

Time	No Encryption	WEP	WPA	WPA2
March 2007	21.8%	46.3%	19.6%	7.3%
Middle of 2006	23.3%	59.4%	14.5%	3.3%

Table 1.1 Encryption methods for wireless network

WEP is defined in the second edition of IEEE 802.11, and it also provides related works of security, privacy, and data source authentication. Wireless networks broadcast messages using radio and are thus more susceptible to eavesdropping than wired networks. When introduced in 1999, WEP was intended to provide confidentiality comparable to that of a traditional wired network. Beginning in 2001, several serious weaknesses were identified by cryptanalysts with the results that today a WEP connection can be cracked with readily available software within minutes.

Within a few months the IEEE created a new 802.11i task force to solve the problem. In the later, Fluhrer, Mantin, and Shamir designed a census attack against WEP called the “FMS attack”. It used initial vector (IV) and RC4 properties to collect enough packets in wireless network and then focused on a specific weak key in the form of (B+3)：FF：N. Due to this, FMS attacks can recover RC4 keys. By 2003, the Wi-Fi Alliance announced that WEP has been superseded by WPA, which was a subset of then upcoming 802.11i amendment.

Finally in 2004, with the ratification of the full 802.11i standard, the IEEE declared that WEP has been deprecated as they fail to meet their security goals. Despite its weaknesses, WEP is still widely in use. Up to now, there are lots of developed hacker tools based on F.M.S attacks such as Aircrack-ng[4].

1.2 Motivation and purpose

Although WEP is known to be insecure and has replaced by Wi-Fi Protected Access (WPA), it is still widely used. In this paper, we present an optimized solution to eliminate the security holes of WEP using "The Keyed-Hash Message Authentication Code" (HMAC).[3] As compared with WPA, optimized WEP (O-WEP) can withstand replay attack and FMS attack without modifying any hardware equipments. In addition, O-WEP can be regarded as the best alternative before hardware update (chipset, access point).

1.3 Structure

There are six chapters in this thesis. The content of each chapter in this paper is organized in the follow ways：

Chapter 1 Introduction：

Chapter 1 describes the motivation, purpose and the structure of the thesis.

Chapter 2 Related Works

Due to WEP, it is a security mechanism of wireless network, and there is a lot of relative security information used in wireless network, this chapter introduces this knowledge briefly such as HMAC, WEP cryptographic operations which will be used in this paper.

Chapter 3 Technicalities Overview of WEP

In this chapter, we are going to briefly analyze the weakness of WEP and describe the eWEP scheme offered by Hani Ragab Hassan. The encryption and decryption process of eWEP are described in this chapter step by step. Besides, we are going to propose a brand-new scheme called O-WEP in the following section.

Chapter 4 Optimized WEP Protocol (O-WEP)

In this chapter, we propose the O-WEP scheme and the detail encryption and decryption process are presented. The brand-new scheme aims to withstand the threat of WEP with the least modification. Hence, the scheme is called “Optimized” WEP.

Chapter 5 Security Analyze

The major motive of this chapter is to compare the security between WEP and O-WEP. We analyze the security holes of WEP and then make a discussion of the original security mechanism. The improved mechanism, O-WEP, can overcome these security holes of WEP without any hardware modification.

Chapter 6 Conclusion and Future work

This chapter is going to make a conclusion on this thesis and describe the relative work and future work.

Chapter 2 Related Works

2.1Wired Equivalent Privacy (WEP)

This section describes the concepts and cryptographic operations of WEP[2].

2.1.1 Concepts

Wireless network is an open medium, and the risk of using it is greatly increased if without cryptographic protection can be applied on the link. In 1999 September, WEP was intended to provide secure information comparable to a traditional wired network. However, researchers present several cases to prove WEP was insecurity in the following four years. Today, WEP is still available 46.3% (Table 1.1) users of wireless network. In many case, it is the only security support particular devices. Although WEP is not powerful as later cryptographic protocols, it does not require the computational power, either. In addition, older devices may lack processing ability to run anything better, and WEP is the best option.

In order to protect secret data, WEP requires the RC4 cipher, which is a symmetric stream cipher. In generally, RC4 does not require the use of any specific key length, and WEP can be used with keys of any size. But the only key size present in the 802.11 standard is a 64-bit WEP seed, which 40 bits are secret between clients and access point and 24 bits are initial vector (IV). There is also another longer key length called “128-bit WEP”. Similarly, 128-bit WEP include 104 bits secret data and 24 bits IV such as “104+24 – bit WEP”. In a designed cryptographic system, we can obtain additional security by using a long key. However, WEP is not a well-designed cryptographic system, and extra bits can not acquire any additional security. On the contrary, additional bits may condense decryption time.

RC4 Algorithm

RC4 [1] is the most widely used *stream cipher* in software applications. Ron Rivest designed the RC4 algorithm for RSA Security Company in 1987. It kept as a trade secret until it leaked out in 1994. Up to now, many papers have published to analyze “how to attack RC4”. (e.g. [KNUD98] [8] [MIST98] [9] 、 [FLUH00] [7] 、 [MANT01] [1]). [FLUH01] has recorded a thornier problem; the author proves that secure mechanism of WEP is easy cracked by specific attack style. Basically, the problem is not in RC4 itself, but the way of generate secret key as RC4 input. The problem has not certainly occurred in other uses RC4 in the application formula. It also spot left the design safety system difficulty.

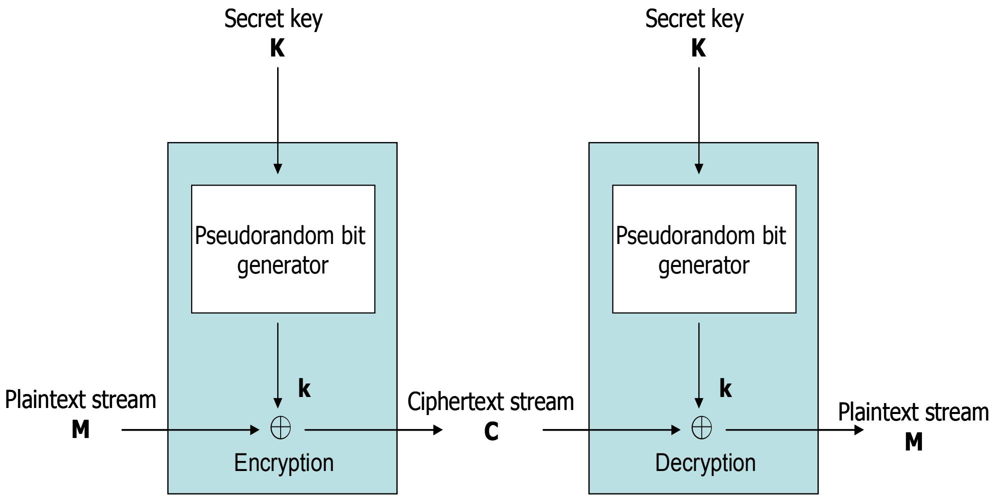


Figure 2.1 stream cipher schematic drawing.

Form figure 2.1, we can see the result of pseudorandom generator is decided by secret key, and the generator needs enough length to avoid brute force attack. If the length of secret key is similar, well-designed pseudorandom generator may make stream cipher as secure as block cipher. The major advantages of stream cipher are quick speed and few source codes (e.g. RC4).

2.1.2 WEP Cryptographic Operations

On this section, we will describe the process that packets encrypted and decrypted by WEP on the wireless networks. First we define the nomenclature that will be used in the paper：

k	The secret key of WEP

KS	Keystream produced by k and IV_i using RC4 algorithm
M_i	The i^{th} message to send
C_i	The i^{th} cipher text
IV_i	The i^{th} initial vector
CRC	*Cyclic Redundancy Check* widely used in network protocol
RC4	A stream cipher

Table 2.1 notation and nomenclature.

Let S be a source which sends messages M to a receiver R. k is the secret key of WEP, and both communication entities share the secret key k.

(1). RC4 is a stream cipher and it uses two inputs to generate a keystream KS

- The 40 bits secret key which shared between S and R
- An initialization vector(IV)

(2). Using CRC(Cyclic Redundancy Check) to calculate check sum of transited messages and let CRC concatenate M note as T(=M || check sum).

(3). Let T XOR with KS to produce cipher text C.

(4). IV concatenates after cipher text C (note that IV is sent as clear text without any encryption).

(5). finally, sender S can transmit the encrypted packets to receiver R.

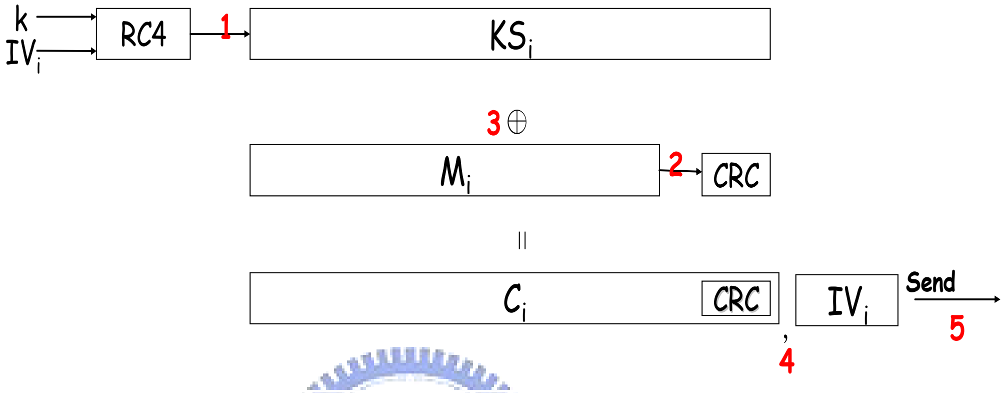


Figure 2.2 Encryption process in WEP.

In Figure 2.1, numbers show the different steps of encryption process in WEP. After processing, an encrypted frame is ready for transmission over an un-trusted network with enough information to enable decryption at the remote end. Similarly, decryption happens in the reverse order.

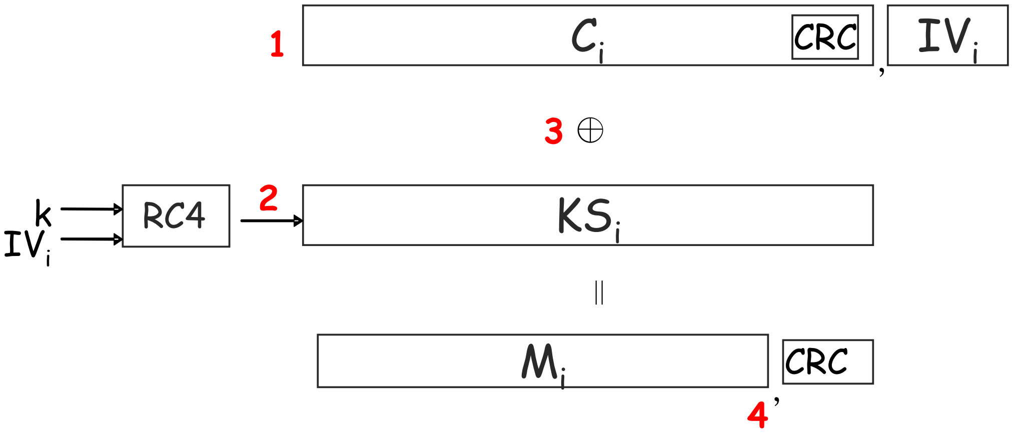


Figure 2.3 Decryption process in WEP.

As R receives the packet from S, we can see the decryption process in Figure 2.2：

(1). R receives the encryption packets include cither text and IV.

(2). Using the IV that was appended to cipher text and k to generate the keystream by RC4 algorithm.

(3). Next, let cipher text XOR with keystream to recover and then gets original message and its CRC check sum.

(4). Last, using the CRC check sum to verify message M if it was modified by someone or not.

The encrypted process of WEP can ensure data privacy, data integrity and authentication. In general, the meaning of data privacy is that all transited packets are encrypted and only remote end can decrypt them. In addition, data integrity and authentication can achieve by the check sum verified. Thus, all modified message can be detected.

2.2The Keyed-Hash Message Authentication Code (HMAC)

This standard describes a key-hash message authentication code (HMAC), the mechanism for message authentication using cryptographic hash functions. HMAC is defined in Federal Information Processing Standards Publication (FIPS PUB 198) that is issued by the National Institute of Standard and Technology (NIST). In the later chapter, we are going to provide an improved WEP scheme called O-WEP. O-WEP uses the HMAC to keep the security of information transmitted over sender and remote end.

2.2.1 Concepts

HMAC is a standard that specifies an algorithm for applications require message authentication. In addition, message authentication is achieved via the construction of a message authentication code (MAC). MAC based on hash function is known as HMAC. MAC is used to authenticate both the source of message and its integrity without using any extra mechanisms. HMAC has the major factor; a message input and secret key are known only to the sender of message and remote receiver.

The hash function of HMAC is used by the message sender to compute a value (MAC) that is formed by the secret and the message input. Then the remote receiver uses the same secret key and hash function as sender to compute the MAC on the received message. If the two match, the message has been received correctly or message has been modified.

2.2.2 HMAC Specification

Glossary of Terms

The following definitions are used throughput by HMAC algorithm：

Approved：FIPS-approved or NIST recommended. A technique that is (1) specified in FIPS or NIST Recommendation, (2) adopted in FIPS or NIST Recommendation and specified either FIPS or NIST Recommendation, or in the document referenced by the FIPS or NIST Recommendation.

Cryptographic key：A parameter used in conjunction with a cryptographic algorithm that determines the operation of the algorithm. The cryptographic key is used by the HMAC algorithm to produce a MAC on the data in this standard.

Hash functions：An approved mathematical function that maps a string of arbitrary length to a fixed length string. It may be used to produce a checksum called hash value or message digest for a potentially long string or message.

Keyed-hash based message authentication code (HMAC)： a message authentication code that uses a cryptographic key in conjunction with a hash function.

Message Authentication Code(MAC)： A cryptographic checksum that result from passing data through a message authentication algorithm. In this standard, the message authentication algorithm is called HMAC, while the result of applying HMAC is called the MAC.

Secret key：a cryptographic key that is uniquely associated with one or more entities. The use of the term “secret” in the text does not imply a classification level; rather the term implies that need to protect the key from discloser or substitution.

Acronyms

The following acronyms are used throughout in HMAC standard：

FIPS	Federal Information Processing Standard
FIPS PUB	FIPS Publication
HMAC	Keyed –Hash Message Authentication Code
MAC	Message Authentication Code
NIST	National Institute of Standard and Technology

Table 2.2 The throughout in HMAC standard

HMAC Symbols and Parameters

HMAC uses the following parameters：

B	Block size (bytes) of the input to the hash function.
H	An approved hash function.
ipod	Inner pad.
K	Secret key shared between sender and remote receiver.
K_0	K after some preprocessing to form a B byte key.
L	Block size (bytes) of the output to the hash function.
Opad	Outer pad.
t	The number of byte of MAC.
text	The data which the HMAC is calculated.
$\Vert$	Concatenation.
$\oplus$	Exclusive Or operation.

2.2.3 HMAC Algorithm

The following operation is performing that to compute a MAC of the data “text” by using the HMAC algorithm.

$$\boxed{MAC(text)_t = HMAC(K, text)_t = H((K_0 \oplus opad) \| H((K_0 \oplus ipad) \| text))_t}$$

Figure 2.3 and Table 2.2 describe the step by step process in the HMAC algorithm.

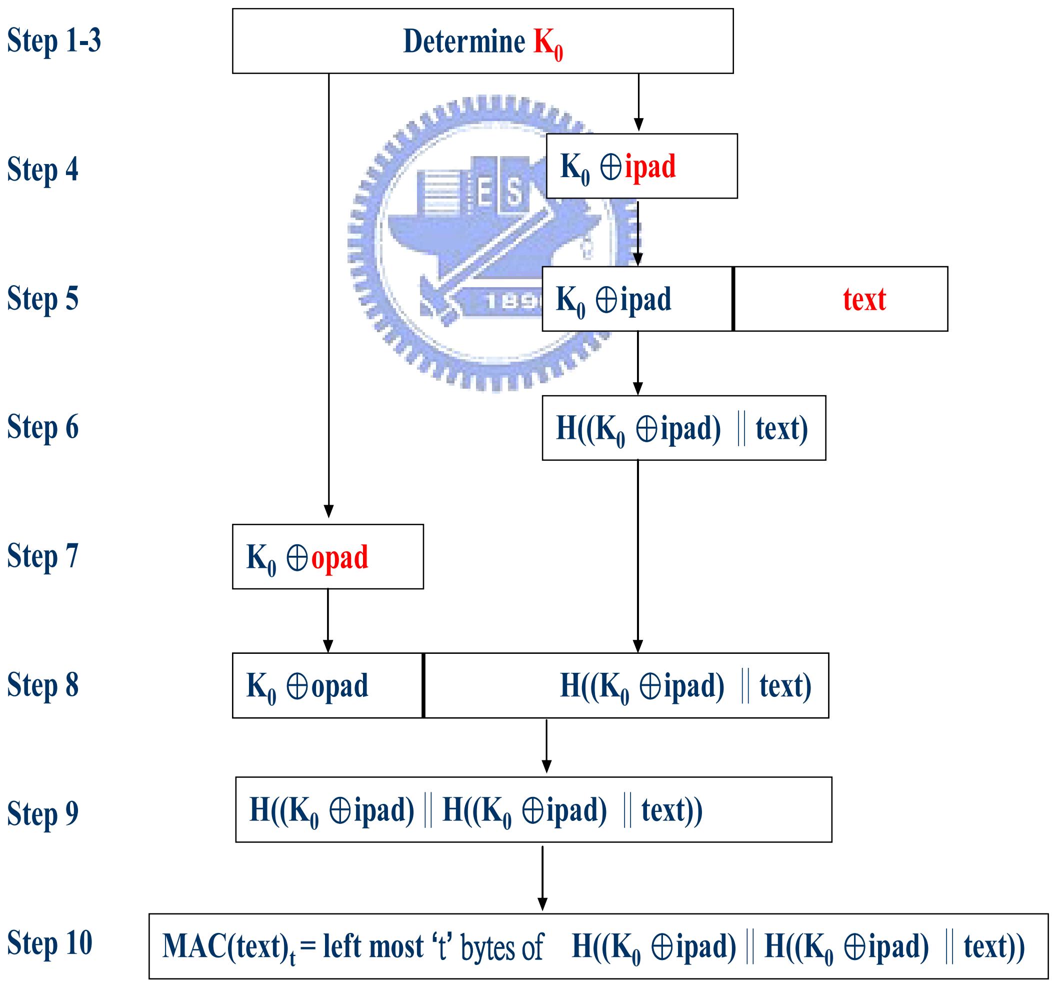


Figure 2.4 Illustrates Construction of HMAC.

Steps	***Description of each step***
Step1~Step3	Determine the pre-processing of K_0
Step4	Exclusive Or K_0 with ***ipad***
Step5	Append the text to the result of Step4
Step6	Using the result of Step5 as input of H
Step7	Exclusive Or K_0 with ***opad***
Step8	Append the result of Step6 to the result of Step7
Step9	Using the result of Step8 as input of H
Step10	The MAC is the leftmost ***t*** bytes of the result of Step9

Table 2.3 The HMAC algorithm

HMAC Examples

Text： "Sample #3"

Key：

```
50515253 54555657 58595a5b 5c5d5e5f

60616263 64656667 68696a6b 6c6d6e6f

70717273 74757677 78797a7b 7c7d7e7f

80818283 84858687 88898a8b 8c8d8e8f
```

```
90919293 94959697 98999a9b 9c9d9e9f
a0a1a2a3 a4a5a6a7 a8a9aaab acadaeaf
b0b1b2b3
```

Hash (Key)：

```
a4aabe16 54e78da4 40d2a403 015636bf
4bb2f329
```

K_0：

```
a4aabe16 54e78da4 40d2a403 015636bf
4bb2f329 00000000 00000000 00000000
00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000
```

$K_0 \oplus$ ipad：

```
929c8820 62d1bb92 76e49235 37600089
7d84c51f 36363636 36363636 36363636
36363636 36363636 36363636 36363636
```

```
36363636 36363636 36363636 36363636
```

(Key ⊕ ipad)||text：

```
929c8820 62d1bb92 76e49235 37600089
7d84c51f 36363636 36363636 36363636
36363636 36363636 36363636 36363636
36363636 36363636 36363636 36363636
53616d70 6c652023 33
```

Hash ((Key ⊕ ipad) ||text):

```
d98315c4 2152bea0 d057de97 84427676
2a1a5576
```

K_0 ⊕ opad：

```
f8f6e24a 08bbd1f8 1c8ef85f 5d0a6ae3
17eeaf75 5c5c5c5c 5c5c5c5c 5c5c5c5c
5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c
```

$(K_0 \oplus \text{opad}) \,||\, \text{Hash}((\text{Key} \oplus \text{ipad}) \,||\text{text})$:

```
f8f6e24a 08bbd1f8 1c8ef85f 5d0a6ae3

17eeaf75 5c5c5c5c 5c5c5c5c 5c5c5c5c

5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c

5c5c5c5c 5c5c5c5c 5c5c5c5c 5c5c5c5c

d98315c4 2152bea0 d057de97 84427676

2a1a5576
```

HMAC (Key, Text) = $\text{Hash}((K_0 \oplus \text{opad}) \,||\, \text{Hash}((\text{Key} \oplus \text{ipad}) \,||\text{text}))$:

```
bcf41eab 8bb2d802 f3d05caf 7cb092ec

f8d1a3aa
```

20-byte HMAC (Key, Text):

```
bcf41eab 8bb2d802 f3d05caf 7cb092ec

f8d1a3aa
```

In general, the type of SHA hash functions is not designed for MAC. These hash functions can’t use to MAC directly because they don’t rely on secret key. Up to now, the HMAC algorithm is widely used to add secret key to hash function. And it also included in several national standards such as RFC 2104, IP security, SSL, and NIPS 198.

A Limitation of MAC Algorithms

The successful verification of a MAC does not completely guarantee that the accompanying message is authentic：There is a chance that a source with no knowledge of the key can present a purported MAC on the plaintext message that will pass the verification procedure. For example, an arbitrary purported MAC of t bits on an arbitrary plaintext message may be successfully verified with an excepted probability of $(1/2)^t$. this limitation is inherent in any MAC algorithm.

Design goal of HMAC

HMAC uses a secret key for the calculation and verification of the MAC. The main goals behind the HMAC construction are：

- To use available hash functions without modifications.
- If needs more efficient hash functions, it is easy to replace hash function which inlays.
- To maintain the original performance of the hash function

without incurring a significant degradation.

- To use and handle secret keys in a simple way.
- To have a well-understood cryptographic analysis of the strength of the authentication mechanism.

First two items are the reasons that HMAC algorithm is widespread using. If the original hash function has not secured, we can replace the one by another secure hash function to improve the security of HMAC. The last item is a vital excuse that HMAC superior to other method. If the security of hash function is power enough, the security of HMAC can be proved.

Chapter 3 Technicalities Overview of WEP

3.1 WEP Weakness

Previous chapter has introduced the step processing of WEP, and in this section we are going to make a discussion on WEP weaknesses.

Security Holes Analysis

The WEP packets are encrypted by RC4 algorithm. And designers specified the use of RC4, which is extensively accepted as a cryptographic algorithm. However, attackers can attack any weak points in the cryptographic system. The techniques of defeating WEP come from all angles. Once the RC4 secret text is decrypted, there is no security service can be guaranteed. In general, CRC is not verified by source. Thus attacker can decrypt and then arbitrarily modify or forge the original message.

All WEP security holes can define as four main conception flaws：

(1). First, the 24 bits initialization vector is transmitted as plain text：

The malicious attackers may easily collect weak IV, and uses this IV corresponds the specific RC4 weak secret key to start the attack.

(2). Second, data source authentication：

The WEP has not designed a mechanism to guarantee data source authentication. WEP uses the CRC check to ensure integrity of transmitted data. If the check of integrity is not complete, these transmission messages have the possibility to be able to forge by the attacker in the transmission process. Then attackers may recomputed the integrity check value (is called ICV) but was not realized.

(3). Third, reuse secret keystream：

Stream ciphers are vulnerable to analysis when the keystream is reused. WEP selects IV method, lets attacker be able to discover something in the repetition use secret keystream. Two packets that share the same IV almost certainly use the same secret key and keystream. As WEP selects 24 bits IV (2^{24} ≒ 16, 777, 216), by the *birthday attack* law knew that every 4,096 packets will have the redundant situation to be bigger than one half.

(4). Fourth, using *Cyclic Redundancy Check*：

Due to CRC check value decrypted by RC4 keystream, CRC still has not security in cryptography. If data integrity can not assured by CRC, attackers could modify frames and not realized. 802.11 standard defines retransmission when frames lost occur, and attackers could retransmit the modified packets to make receivers accept them.

RC4 Key Recovery against WEP

In 2001, Scott Fluhrer, Itsik Mantin and Adi Shamir present several weaknesses in the key scheduling algorithm of RC4, and describe their cryptanalytic significance. They identify a large number of weak keys, in which knowledge of a small number of key bits suffices to determine many state and output bits with non-negligible probability. They also use these weak keys to construct new distinguishers for RC4, and to mount related key attacks with practical complexities. And show that RC4 is completely insecure in a common mode of operation which is used in the widely deployed WEP.

The Fluhrer, Mantin and Shamir (FMS) attack takes advantage of a weakness in the RC4 key scjeduling algorithm to reconstruct the key from a number of collected encrypted messages. The FMS attack gained popularity in tools such as AirSont and aircrack[4], both of which attack WEP encrypted wireless networks. For this discussion, they use the blow RC4 key scheduling algorithm (KSA) and pseudo-random generation algorithm (PRGA).

Key scheduling algorithm (KSA)

```
begin ksa(with int keylength, with byte key[keylength])
    for i from 0 to 255
        S[i] := i
    end for
    j := 0
    for i from 0 to 255
```

```
        j := ( j + S[i] + key[i mod keylength]) mod 256
        swap(S[i] , S[j])
    end for
end
```

Pseudo-Random Generation Algorithm (PRGA)

```
begin prga(with byte S[256])
    i := 0
    j := 0
    while GenerationOutput
        i := ( i + 1 ) mod 256
        j := ( j + S[i] ) mod 256
        swap( S[i], S[j])
        output S[( S[i] + S[j] ) mod 256]
    end while
end
```

Key Recovery Defense

Longer secret keys can not defend against key recovery attacks. The time required to recovery a secret key can be broken up into the gathering time required to collect enough packets for the attack, and the computational time required to run the program and get the secret key.

In general, gathering time is the major factor of the attack and computational time is only a few seconds. Longer keys require slightly more computational time, but gathering time still maintained invariably. As the key length increase, more weak IVs are caught.

Many vendors adopt the defense is to avoid using weak IVs. Most vendors have changed their products for each IV to be checked, and all weak IVs are replaced non-weak IVs. However, reducing the size of the IV space may cause IV reuse earlier.

3.2 Brief Review of eWEP Scheme

The eWEP scheme is proposed by Hani Ragab Hassan. eWEP [6] aims to solve WEP flows without hardware modification while keeping a good interoperability with existing WEP.

Encryption principle of eWEP

eWEP is similar to WEP. The difference between them is that eWEP encrypts the concatenation of the message and IV with RC4. Encrypting IV aims to avoid eavesdropping. As shown in Figure 3.1 and Figure 2.2, let's focus on M_i. In WEP, IV transmitted as plaintext and concatenate after C_i. Eavesdrops can use the security hole to gather enough initial vector and then crash the whole WEP secure mechanism. In order to eliminate the secure hole, the authors of eWEP offered the idea to enhance WEP. They concatenate the IV after M and CRC check value and then XOR with keystream.

We can see step5 of Figure 3.1, include message and IV are send as cipher text. Now, eavesdrops try to gather IV is not easy. They have to decrypt each packet before gather initial vector. That can increase mostly security of WEP.

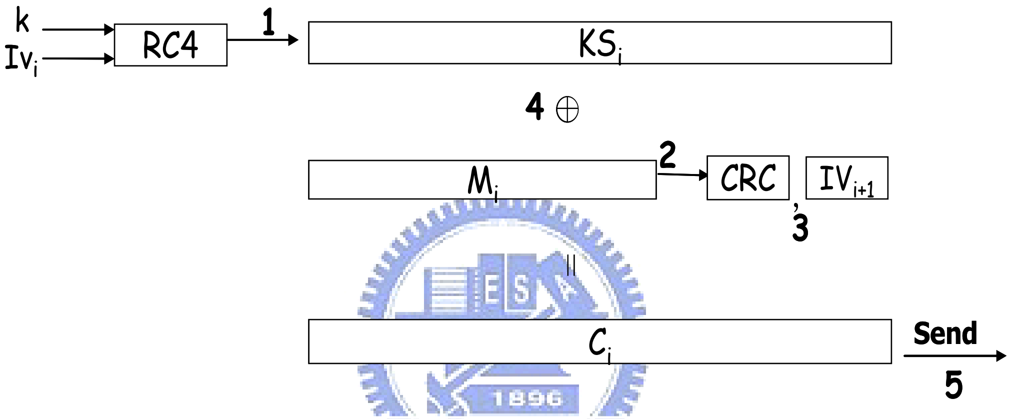


Figure 3.1 Encryption process of eWEP.

As shown in Figure 3.2, eWEP sender uses IV$_i$ to encrypt the concatenation of M$_i$ and IV$_{i+1}$. Thus, it is sufficient for the receiver to know the initial IV (e.g. IV$_1$) to decrypt the first packet which contains IV$_2$ used to decrypt second packet and so on. The dependency between frame and frame is a vital property. This means that remote end has to receive first initial packet and then the following packet could be decrypted.

On the other hand, attacker attempts to modify or forge frame will cause the following packet can't be decrypted. Even packet was lost during transmission process; the following packet can't be decrypted, either. We can also achieve the replay detection by verifying whether the received packet is decrypt able or not. If the packet is a replay, it can't be decrypted by the current IV because it changes for every packet.

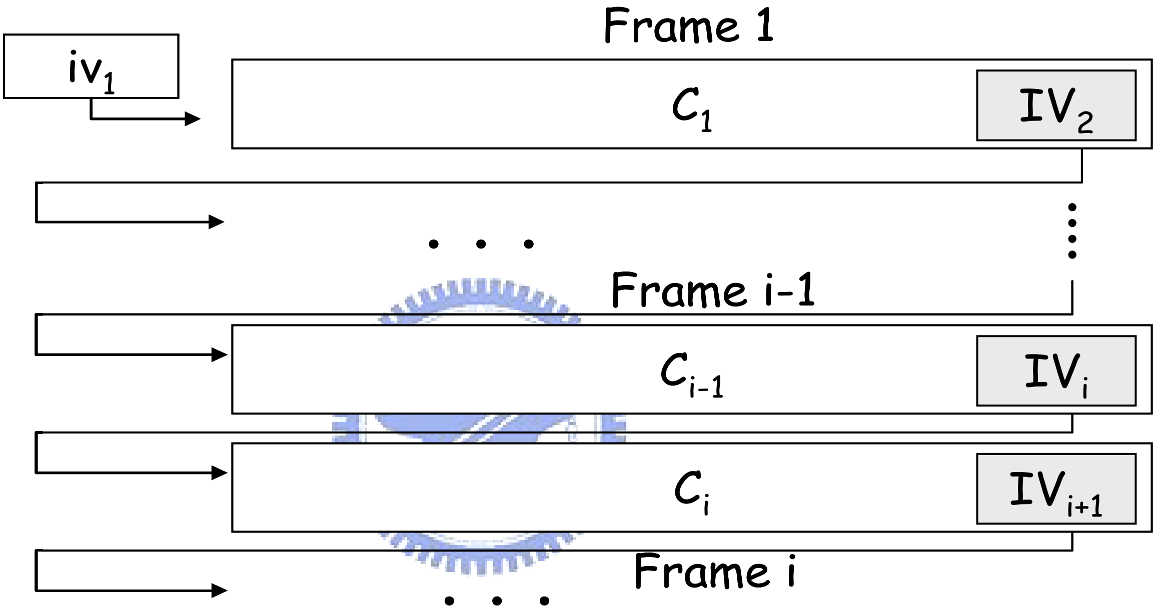


Figure 3.2 cipher principle of eWEP.

eWEP Analysis

We compare WEP with eWEP according three criteria. The first is level of security; the second is the packet format and finally the computational overhead.

(1). Security：

Security mechanism of WEP has already broken, as shown Figure 3.1 and Figure 3.2, privacy of eWEP is resistant against instructors.

(2). Packet Format：

According to eWEP packets, the format of eWEP is different from original WEP packet. In fact, the difference of packet format will impact the performance of interoperability between WEP and eWEP.

(3). Computational Overhead

In general, using keystream allows separate computation in two different sections. The first one is generating keystream and it is done off-line. The second is the XOR of the message to the keystream. Although eWEP maintains the principle, it still needs to encrypt additional 24 bits initial vectors.

From all of the above, we have a conclusion on eWEP. It could improve the secure level, but packet format and computational overhead are new problems. Next chapter we are going to provide a new scheme called Optimized WEP Protocol (O-WEP). O-WEP is able to resolve the WEP threats and avoid these new problems.

Chapter 4 Optimized WEP Scheme (O-WEP)

The protection offered by WEP enables users to have the convenience and the security. However, the paper described "Weakness in the Key Scheduling Algorithm of RC4" was published in 2001 August. The paper presents the famous FMS attack against WEP. In this chapter, we provide the new WEP scheme is called Optimized WEP Protocol (O-WEP).

4.1 Notation and Nomenclature in O-WEP

In order to enhance the performance (security) of WEP, we provide the O-WEP mechanism. O-WEP aims to resolve the problem of WEP without changing or adding hardware but merely software updating. O-WEP also keeps original packet format to have a great interoperability with WEP. In this section, all components of O-WEP are described in the following Table 4.1.

k	The secret key of WEP.
HMAC_k	Keyed-Hash Message Authentication Code and k is the secret key.

MS_i	MS_i is similar to IV_i of WEP. it also used to generate key stream (KS_i) dynamically.
KS_i	The dynamical key stream that is produced by MS_i and IV_i.
M_i	The ith transmitted message.
C_i	The ith encrypted packet.
CRC	*Cyclic Redundancy Check* widely used in network protocol.

Table 4.1 Notation in O-WEP

MS_i and KS_i can be written as following functions：

$$MS_0 = \mathrm{HMAC}_k(\mathrm{IV}_0) \qquad (1)$$

$$MS_i = \mathrm{HMAC}_k(\mathrm{IV}_i, MS_{i-1})\ \forall i \geq 1 \qquad (2)$$

$$KS_i = \mathrm{RC4}(k, MS_i)\ \forall i \geq 0 \qquad (3)$$

$$C_i = M_i \oplus KS_i \qquad (4)$$

The HMAC_k used in the function (1) and function (2) is a message authentication code (MAC) that constructed by secure hash algorithms. The purpose of using HMAC is computing the M_i (see the function (1) and (2), MS can be computed by HMAC algorithm). In addition, the k of HMAC is a secure key (In initial, the secret key is setup by users).

The HMAC has included in several international standard such as SSL protocol and NIST. Besides, IP security also requests that MAC must implement by HMAC algorithm. In addition, HMAC can use embedded hash functions without any revision. (In this paper, we recommend using the SHA2 hash function) The function (3) means that secret key k and MS_i (MS_i replaces the original IV_i in WEP) produce key stream KS_i by RC4 algorithm. The function (4) explains that how to produce cipher text C_i by M_i and KS_i.

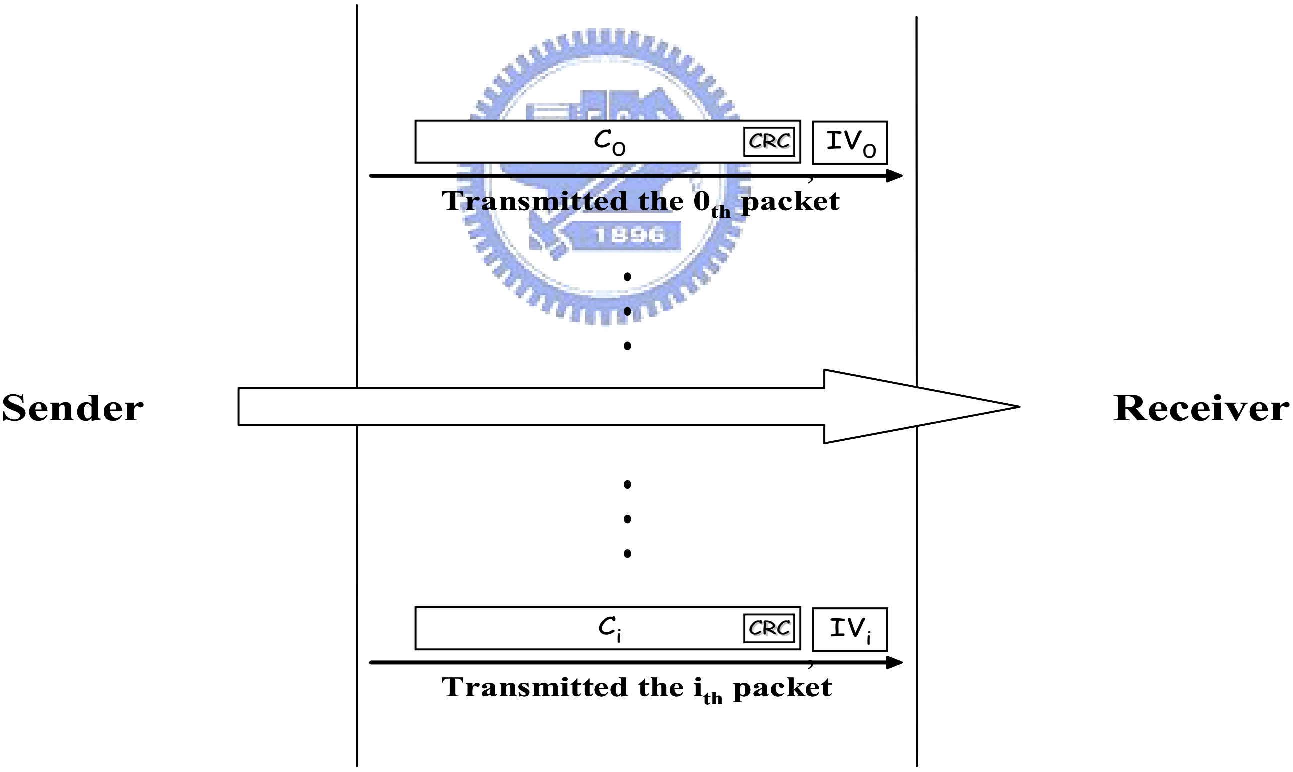

C_0
CRC
IV_0
Transmitted the 0_{th} packet
Sender
Receiver
C_i
CRC
IV_i
Transmitted the i_{th} packet

Figure 4.1 transmission processes of O-WEP packets.

Figure 4.2 explains the process of packets transmitted between sender and receiver. The transmitted packet can be distinguished into the initial packet and non-initial packets. The initial packet uses MS_0 to encrypt packet and others use MS_i to do. The detailed encryption and decryption processes will make a discussion in the following section.

4.2 O-WEP Cryptographic Operations

In this section, we will show the detailed process of O-WEP. See the Figure 4.3, the encryption process of O-WEP is similar to WEP. O-WEP has the same encryption processing as WEP except that O-WEP replaces IV_i with MS_i as the input of RC4 (MS is defined in function (1) and function (2)). In the following words, we are going to consider two different situations of O-WEP encryption and decryption process between sender and receiver. First, the encrypted packet is initial packet, and the second is that the encrypted packet is non-initial packet.

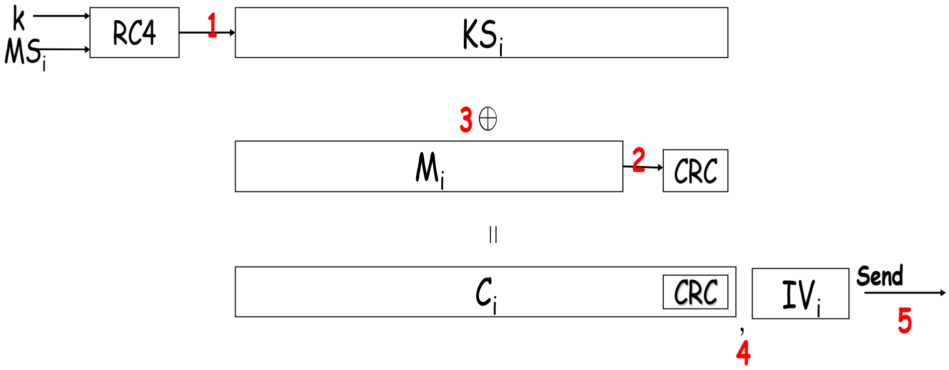


Figure 4.2 Encryption process in O-WEP.

First, to encrypt the initial packet：

When sender transmits the initial packet, he is able to acquire MS_0 by function (2) and then computes RC4 algorithm to acquire KS_0 by function (3) and secret key. Using KS_0 to encrypt transmitted packet and then concatenate the IV_0 that has used in function (2) to encrypted packet and transmit together. If remote end receives the encrypted packet, receiver uses IV_0 to acquire MS_0 by function (1) and computes the KS_0 to decrypt the packet.

Second, to encrypt the non-initial packet：

If sender transmits the non-initial packet (e.g. $i > 0$), MS_i is going to generate by function (2) then. However, to produce MS_i needs IV_i and MS_{i-1}(which used by previous packet). This means that each computed MS_i has to keep for next transmitted packet to encrypt. Similarly, when remote end decrypts the packet, he also needs the MS_{i-1} that used by previous packet. Due to this, whether sender or remote receiver should keep least continuous two MS to generate later MS.

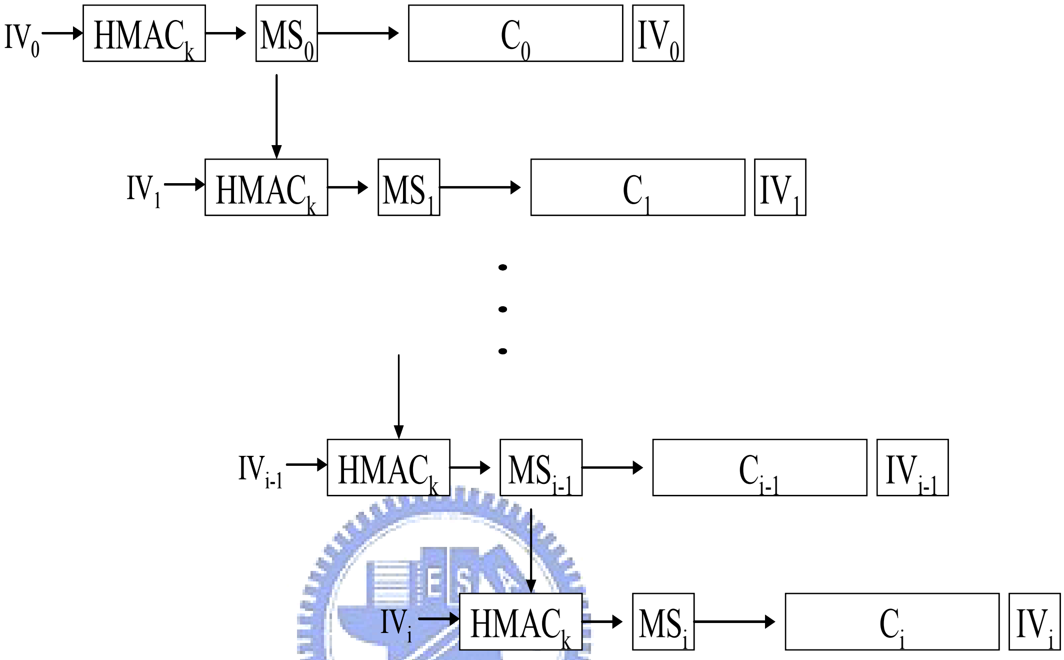


Figure 4.3 The dependency between O-WEP packets

According to the special mechanism, we can observe the rule of the packet encryption. Figure 4.4 is showing that the dependency around O-WEP packets. The relation of packets that links with each other is like chain architecture. Due to the chain architecture of O-WEP, each packet needs the packet previous to itself to encrypt and decrypt. The advantages of this chain architecture are going to have a detailed conclusion in the following chapter.

Chapter 5 Security Analyze

In the above chapter, we use HMAC to improve the security of WEP, and the following content of this chapter is going to show that the security analysis of O-WEP.

5.1 Security Improved

We point out that several weakness in the chapter three such as initialization vector is transmitted as plain text, data source authentication, reuse secret key stream ,and using Cyclic Redundancy Check… and so on. Now, we are going to have the conclusion in the following words.

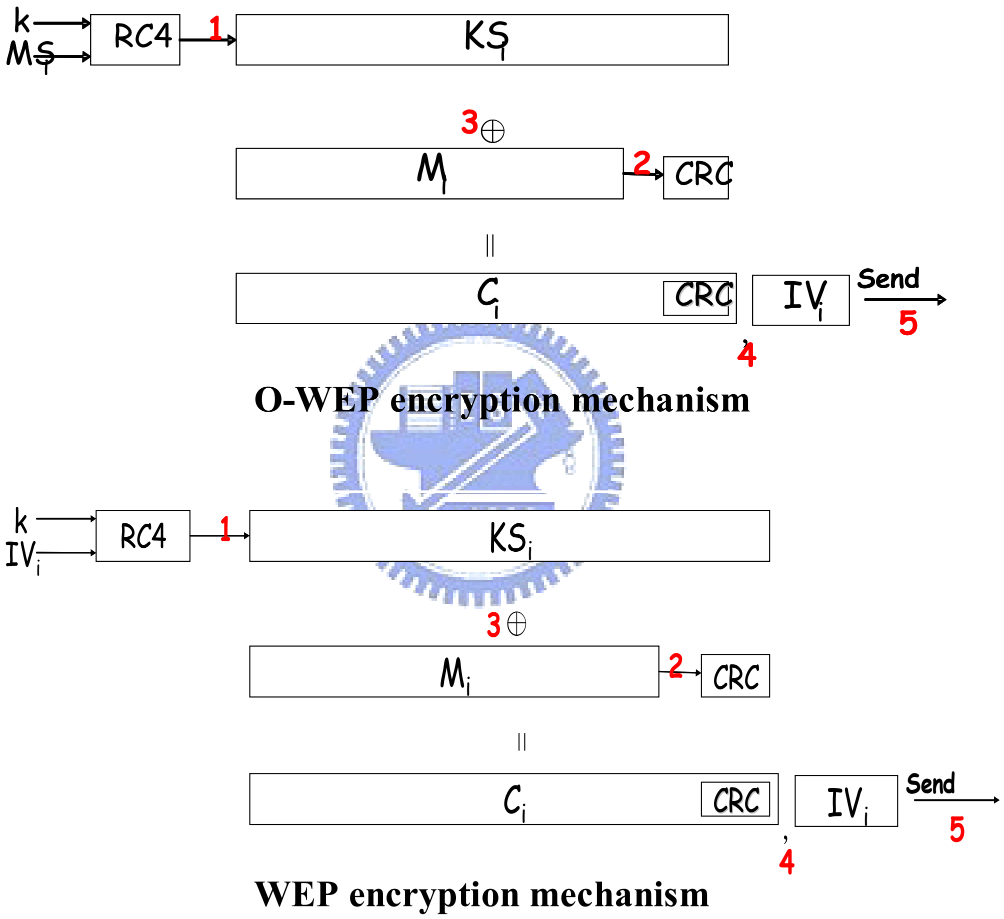
(1). Initialization vector is transmitted as plain text： Although packets still transmitted as plain text in the O-WEP, the key stream (KS_i) used to encrypt packets is not produce by IV_i and k but MS_{i-1} and IV_i. Considering that attackers attempt to deliver FMS attack to gather lots packets, and try to analyze the encrypted key stream for guessing the original secret key. However, FMS attack still needs MS_{i-1} to find initial vector in the decryption processing. Comparing to WEP, O-WEP can improve the weakness of WEP. Due to this, attacker is much difficult to decrypt O-WEP.

(2). Data source authentication： According to Figure 4.4, we can observe that the dependency around O-WEP packets. When O-WEP suffers reply attack, the resend or fake packets can not be decrypted and verified CRC check value. Due to this, the process of illegal deliver could be detected.

(3). Reuse secret key stream： WEP uses 24 bits initial vector (about 16 millions types) and secret key to produce key stream. In a busy network transmission process, the 24 bits IV too easy to cause repeated use. (By birthday attack law known that every 4,096 packets will have the redundant situation to be bigger than one half) In addition, O-WEP uses the MS_i that generate by $HMAC_k$ (MS_{i-1}, IV_i) to produce secret key. If $HMAC_k$ adopts the SHA-256 hash function, the length of generated MS_{i-1} is 256 bits. However, the probability of repeat using key stream will drop largely. (By birthday attack law, every 2^{140} packets will have the redundant situation to be bigger than one half)

(4). Reliability： we are going to make a discussion on this part： How to solve the problem that packets lose during the transmission? According to Figure 4.4 should simply realize that O-WEP has the feature of packets dependency. When occur that packet losing and then the following packet can not be decrypted. Due to this, if the receiver R detects packets losing, R is going to return a special message M_L to sender. After the sender S receives the special message, S is going to retransmit the packet.

According to above analysis, the security strength of O-WEP merely depends on the hash function which HMAC$_k$ adopted. As to SHA-256, when attacker uses *birthday attack* to crack 256 bits message digest, it needs $2^{(256+24)/2}$ time complexity to meet one collision. This makes attackers pay the very great price if they attempt to crack the O-WEP mechanism.



O-WEP encryption mechanism

WEP encryption mechanism

Figure 5.1 the comparison between WEP and O-WEP

In addition, from Figure 5.1 knows that the packet format of O-WEP is the same as WEP and the only difference between them is that WEP uses IV_i and k to produce KS_i but O-WEP uses MS_i and k to do. In addition, O-WEP does not add any extra fields. Due to this, O-WEP does not use additional network band. As to additional computation quantity, O-WEP needs that is the part used by $HMAC_k$. In fact, $HMAC_k$ is included in lots international standard such as RFC 2104, IP security, SSL, and NIPS 198. Besides, HMACk is a special algorithm that could be support by most hardware. Due to this, the extra computation is the available scope of common computer system.

Chapter 6 Conclusion and future work

6.1 Conclusion

In this paper, we describe the security holes of WEP working architecture. In order to eliminate the security holes, we offer the optimized WEP security mechanism called O-WEP. The great advantage of O-WEP is that O-WEP does not need any other hardware renew. Due to this, O-WEP can be the optimized replacement case of WEP. To compare to original WEP, O-WEP has the great improvement in security. Although O-WEP increases neglected additional computation, the extra computation overhead is the available scope of computer system.

6.2 Future work

Future works should focus on the problem of interoperability. Indeed, deploying mixed networks will be an unavoidable step towards deploying O-WEP. Thus, security threat in this case is the basis issue.

Reference

[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.

[6] H. Ragab Hassan, and Y. Challal, “Enhanced WEP: An efficient solution to WEP threats”

[7] S. Fluhrer, and D. McGrew, “Statistical Analysis of the Alleged RC4 Key Stream Generator.” Proceeding, Fast Software Encryption 2000.

[8] L. Knudsen, et al. “Analysis Method for Alledged RC4.” Proceedings, ASIACRYPT’98, 1998

[9] S. Mister and S. Tavares. “Cryptanalysis of RC4-Like Ciphers.” Proceedings, Workshop in Selected Areas of Cryptography, SAC’98. 1998.