A Scheme for Key Management on Alternate Temporal Key Hash

Song-Kong Chong[1], Hsien-Chu Wu[2] and Chia-Chun Wu[3]
(Corresponding author: Hsien-Chu Wu)

Graduate Institute of Networking and Communication Engineering, Chaoyang University of Technology[1],
168 Gifeng E. Rd., Wufeng Taichung County, Taiwan 413, R.O.C.
Department of Information Management, National Taichung Institute of Technology[2],
129 Sec. 3, San-min Rd., Taichung, Taiwan 404, R.O.C. (Email: wuhc@ntit.edu.tw)
Department of Computer Science, National Chung Hsing University[3],
250 Kuo Kuang Rd., Taichung, Taiwan 402, R.O.C.

(Received Jan. 5, 2005; revised and accepted Feb. 15, 2005)

Abstract

Wired equivalent privacy encryption of IEEE 802.11 standard is based on the RC4 stream cipher, but the weakness in its Initialization Vector (IV) derivation causes the Key Scheduling Algorithm (KSA) of RC4 to leak out the information about the secret key. It is shared among the particular participants in the Wireless LAN (WLAN). Housley et al. proposed an Alternate Temporal Key Hash (ATKH) to solve the weakness of the KSA; they defeated the particular IV may make the KSA to leak out the information about the shared secret key. However, the ATKH did not solve the key management in WLAN. Since a robust key management is a critical factor to prevent the eavesdropping from attackers. Therefore, in this paper, we shall propose a scheme to make key management feasible in their solution without changing the framework of the ATKH and the existing 802.11 standards.

Keywords: Key management, security, temporal key hash, wireless LAN

1 Introduction

The demand for wireless network access is proliferate in recent years. When transmission is broadcasted over the air, protection of the connected resources becomes critical to prevent unauthorized accessing, intercepting and masquerading [5, 6, 7, 8]. Wireless LAN (WLAN) based on IEEE 802.11 standard [9] defines the Wired Equivalent Privacy (WEP) which applies the well-known RC4 stream cipher attempt to bring the security level of wireless systems closer to those of wired ones. The RC4 is a symmetric cryptography, which consists of two part: a Key Scheduling Algorithm (KSA), which derives the initial permutation from a random size key (the typical size is 40-256 bits), and a Pseudo Random Generation Algorithm (PRGA), which uses the initial permutation to generate a pseudo-random output sequence (RC4 key). To ensure that the encrypted data is secure, it is important that each data packet be encrypted with different RC4 keys, such as:

$$C = P \oplus RC4(IV, K), \tag{1}$$

where C is ciphertext, P indicates a plaintext, K donates the pre-shared secret key among the participants, IV (Initialization Vector) is a seed that makes the RC4 key encrypt data packet variant every time under the same secret key K, and $RC4(IV, K)$ means the input values to RC4 stream cipher are IV and K, and output result is the RC4 key. After plaintext P XORed with the RC4 key ($RC4(IV, K)$), the ciphertext is produced.

Unfortunately, WEP fails to meet its expected goal. These weaknesses of WEP stem from the misapplication of cryptography and can be roughly summarized into two main problems [1, 11]:

1) The limitation of IV's length is only 24 bits which will cause IV collisions. The IV collisions will make the difference data packets encrypted with the same RC4 key if the shared secret key K remains unchanged. It causes the RC4 key of two different packets will be cancelled, such as:

$$\begin{aligned} & C_1 \oplus C_2 \\ = \; & (P_1 \oplus RC4(IV, K)) \oplus (P_2 \oplus RC4(IV, K)) \\ = \; & P_1 \oplus P_2. \end{aligned}$$

Key stream reuse may experience a serious attack, statistics analysis attack. The attack is employed

to decrypt the $P_1 \oplus P_2$ because the redundancy of real-world plaintexts have enough information to recover the ciphertext. It will become even worse if the attacker obtains many data packets encrypted with same the RC4 key.

2) Use the Cyclic Redundancy Check (CRC) improperly to prevent tampering with transmitted data packets. Unlike the MAC (Message Authentication Code), the CRC is designed to detect transmission error. Since it is an unkeyed function, it does not have the capability to resist malicious attacks from attackers. Those attacks may include message modification, message injection and so on.

In [2], Fluhrer et al. described two weaknesses about the KSA of the RC4. The first weakness is that a great number of bits of KSA output are determined by a small part of the secret key. The second one is a passive ciphertext-only attack, in which the known particular IV will make the KSA into a state to leak out the information about the shared secret key in the WEP. In this mode, attacker can restore an arbitrary key size; the amount of time used is negligible and only grows linearly with its size. Based on [2], Stubblefield et al. [10] implemented the WEP attacks in practical. They also discussed several modifications which can improve the performance of key recovery attack on the WEP.

To solve the weaknesses in the KSA, Rivest (the author of the RC4) suggested two solutions to overcome these defects [3, 4]:

1) The first 256 bytes output of the PRGA should be discarded before encryption begins.

2) Use a one-way hash function, such as MD5, to preprocess the shared secret key and the IV.

However, neither of these two solutions had been accepted due to their cost [3, 4]. Therefore, Housley et al. [4] proposed the Alternate Temporal Key Hash (ATKH) to solve the attack of [2]. In addition, they also expanded the life span of a temporal shared secret key to 2^{48} MPDUs (Medium access control (MAC) Protocol Data Unit), which is longer than [3].

To employ the ATKH, all the participants must use the RC4 stream cipher. A well-know pitfall of the RC4 is that if the same IV and the same shared secret key are used more than once when encrypting, two message will lead to data recovery attack [1]. Therefore, the ATKH is expected that the same IV should not be used more than once with each shared secret key. However, the management of the shared secret key has never been solved in the [4]. In this paper, we consider the key management of the ATKH should be simple and easy to implement without neglecting the security or decrease the efficiency of the ATKH. Here, we propose a simple solution to solve the key management problem of [4]. Our scheme is efficient and does not alter the framework. The most important of all, we keep the existing 802.11 standard remain unchanged.

The next section of this paper is devoted to an overview of the ATKH and the problems it tries to address. In Section 3, we propose a solution that the key management based on ATKH which can be easily applied. Section 4 will shows the security analysis for our scheme. Finally, the conclusions are presented in Section 5.

2 Review of ATKH

In this section, we will review the schemes proposed by Housley et al. [4]. The solution was selected over the traditional hashing schemes, such as SHA-1 or MD5, because of its ability to produce secure keys rapidly, which fill the bill of the RC4 used in the WEP [4]. Three requirements must be satisfied in the ATKH:

1) All participants use the RC4 stream cipher to encrypt the communication data packet.

2) All participants share a 104-bit Temporal Key, TK, such as $RC4(IV, TK)$, however IV and TK should be preprocessed by the ATKH before getting into the RC4 stream cipher.

3) Each participant must ensure that there is no IV collision under same as TK and Transmitter Address, TA.

Figure 1 shows the ATKH scheme.

Phase One:
The inputs of the phase one are 128 bits TK mixed with 48 bits TA and the most significant 32 bits of IV (called $IV32$). These used to make sure that the participants encrypt their own data packets by using different key streams. Since each participant's TA is unique, the key streams used to encrypt data packets will be guaranteed that there is no collision among all the participants although their IV values may be the same. The outputs of phase one are 80 bits, which can be cached to improve the performance of encryption.

Phase Two:
The outputs of phase one are mixed with the least significant 16 bits IV (called $IV16$) and 128 bits TK. The output of phase two is a 128-bit per-packet key called $RC4key$. To conform to the WEP specification, the first 24 bits will be transmitted into plaintext as IV values. The $IV32$ will be conveyed into another field in the frame.

In [4], the weak key pointed out by Fluhrer et al. [2] was precluded by reconstructing the WEP IV format. Moreover, to prevent data recovery attack, the authors expected that the same IV should not be used more than once with each TK.

The role of TK act as the same function with K in Equation (1). However, the authors did not mention how

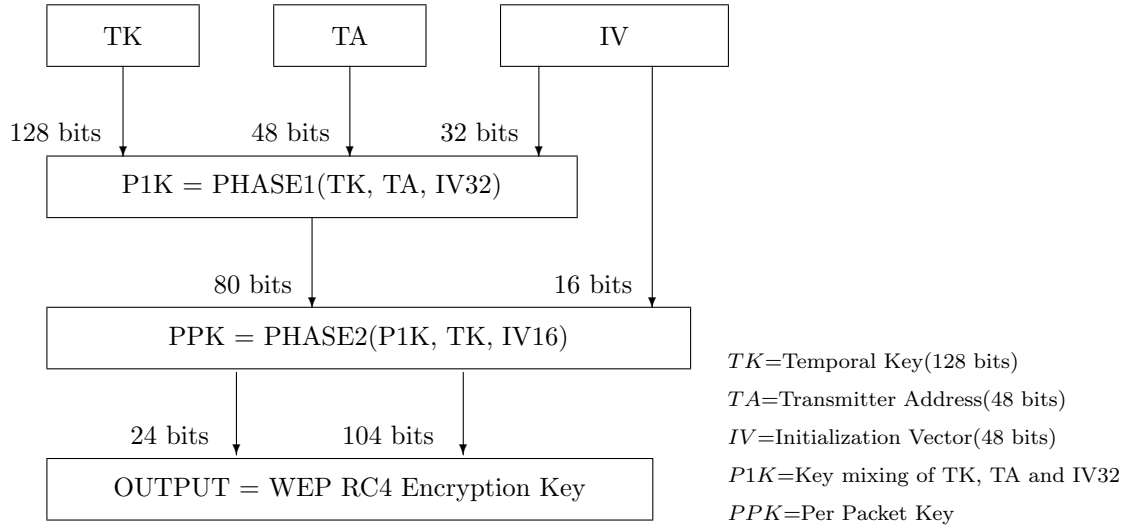

Figure 1: Alternate temporal key hash

to install the TK in the wireless equipment. Therefore we assume that the TK may be presumed to be delivered to all of the participants in the particular WLAN via a secure channel before starting the ATKH. To let the result of scheme of [4] be sound, we proposed an efficient scheme to solve the shared secret key management problem. Our scheme makes the automatically key management of the ATKH become feasible without the manual key renewal of the system operator. In addition, we keep the framework of the ATKH remain unchanged and we do not alter the existing 802.11 standard.

3 The Proposed Scheme

In this section, we propose an efficient scheme to make the key management become feasible in [4]. The expected result of this proposal is to achieve the following requirements:

1) Prevent IV collisions with the same TK, which lead to the reuse of the RC4 key-streams and cause data recovery attack.

2) Do not introduce complicated computations in the proposed scheme, and prevent the computation overhead.

3) The computation result of the new TK can be cached to improve the performances of the ATKH.

4) Zero information has been sent when updating TK.

5) Do not alter the framework of the ATKH.

6) It is easy to apply without changing the existed IEEE 802.11 standard.

Our scheme employ a special frame of 802.11 standard, called "beacon", to renew the shared secret key TK of the participants. We use the timestamp contained in "beacon" to achieve the above requirements. Before that, we need to take a review to the 802.11 frame format [9]. According to the 802.11 standard, the frame format for a Management frame is defined as that in Figure 2. Moreover, An AP (Access Point) shall be able to periodically transmit the special frames, called "beacon", which contain the information shown in Table 1.

The valid type and subtype combinations in frame control field of management frame format used to define a beacon are 00 and 1000. Here, 00 is the type description of the management frame format and 1000 is the subtype description of beacon, and the subtype value 1101-1111 is reserved. The way we make the key management feasible is to apply an AP to transmit a special beacon to all the stations in a BSS (basic service set) with the reserved subtype value 1101 when 48-bit IV space is nearly exhausted. When receiving stations obtain such beacons, they will first check the validity of time. If the timestamp is valid, the receiving stations will extract the 64 bits timestamp from beacon frame body and implement the following action to extend the TS (new Timestamp) into 128 bits respectively, where $\|$ denotes the concatenation:

$$TS = Timestamp \| left - shift\ 1\ bit\ (Timestamp).$$

Now all the participants have obtained the same TS. In the next step, they need to renew their TK defined in the ATKH, which just takes a simple computations exclusive-or operation between TK_o and TS, where TK_o is an original shared TK presume delivered to all the participants in the particular WLAN via a secure channel before starting the ATKH.

$$TK_n = TK_o \oplus TS.$$

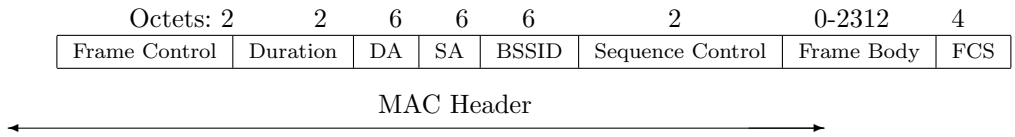

Figure 2: Management frame format

Table 1: Beacon frame body

Order	Information
1	Timestamp (64 bits)
2	Beacon interval
3	Capability information
4	SSID (service set identifier)
5	Supported rates
6	FH Parameter Set
7	DS Parameter Set
8	CF Parameter Set
9	IBSS Parameter Set
10	TIM

All the participants now regard TK_n as a new shared key instead of TK_o and use it as the input of phase one and phase two in the ATKH. Therefore, the shared key of all the participants remain unchanged, and the improved method is depicted in Figure 3. The AP need to retransmit this special beacon before the IV is exhausted. When participants receive such a beacon, they need to implement the steps described above again to obtain their new shared key by just taking a simple exclusive-or with TK_o. When a new station needs to join into the BSS, it will use the TK_o to authorize itself to AP. If the user is legitimate, AP will transmit the special beacon to all the participants to inform them to renew their TK. Besides, the new station also needs to renew its TK. After that, the resources of this WLAN allowed to be used. Figure 3 shows the proposed scheme.

In our scheme, no modification was made to the framework of [4]. Moreover, we keep the existing 802.11 standard remain unchanged by just transmitting a special beacon to accomplish the key management of [4]. In the next section, we will show that our scheme is secure and efficient and functions well in the WLAN environment.

4 Security Analysis

The user's long-term shared key TK_o is used for authentication by his/her home network and it is used only when renewing a shared key of the participants. All participants will use a new TK_n every time when a station joins into the network. Since there is a center master AP which is used to monitor the IV and force all of the participants to renew their shared key before IV is exhausted, therefore, we success to prevent the problems of RC4 key-stream reused which will cause data recovery attack [1, 11]. The proposed scheme satisfies Requirement 1 mentioned in Section 3.

Moreover, our proposed solution for key management will just take a simple left shift 1 bit and a simple exclusive-or operation. The time of the computation is negligibly short, which satisfies Requirement 2 mentioned in Section 3. The output of phase one can be cached to improve the performance until the stations receive the special beacon again, and this satisfies Requirement 3 mentioned in Section 3.

The timestamp contains zero information for attackers since attackers do not know the shared key (TK_o) of the participant. The timestamp is renewed and never duplicated every time when it is transmitted, so it contains zero information and it is useless for attackers to obtain any information about the shared key. Moreover, the new-shared key (TK_n) will be the input of the phase one and the phase two of the ATKH; the non-linear substitution function S-box of [4] will make the key recovery attack become impossible since Requirement 4 mentioned in Section 3 is achieved. The never duplex timestamp provides us a good method to make key management feasible while applying the ATKH solution, since we do not change the framework of the ATKH and 802.11 standard, and the proposed scheme satisfies Requirements 5 and 6 mentioned in Section 3. The attacker cannot obtain the shared key among the participants using the previous attacks [1, 11] because the temporal key will have been renewed before IV is exhausted in our proposal.

5 Conclusions

In the key management scheme proposed in this study, we solve the problems of IV reused and the key management

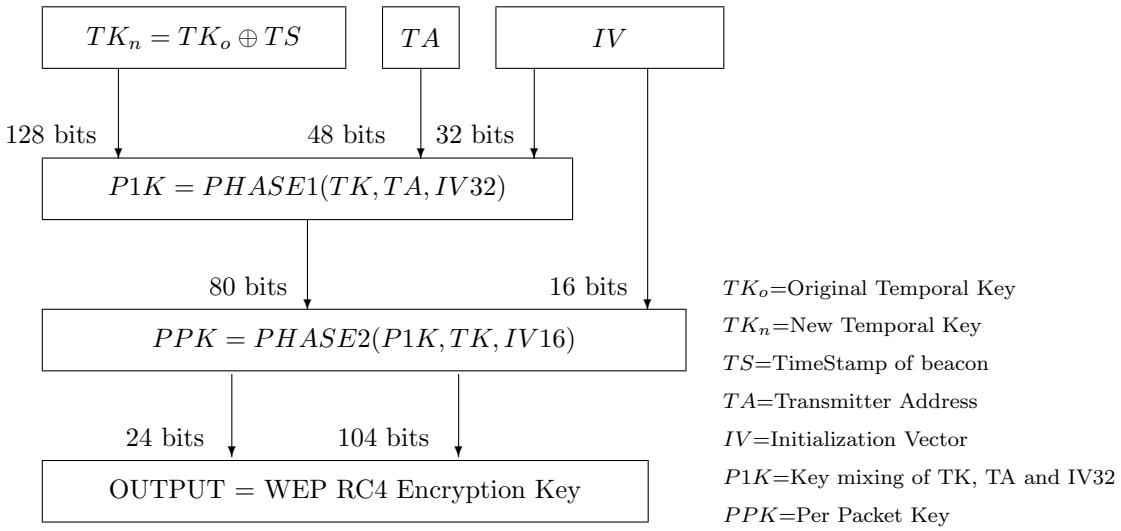

Figure 3: The improved scheme for key management on the ATKH

based on [4]. This study do not solve the problems, such as improper use of CRC checksum, which leads to message modification or message injection because it is not within the scope of this paper. Our key management scheme is generally suitable in WLAN environments. Since we do not change the WLAN standard, it is compatible with those existing wireless products. Moreover, our scheme is easy to design. The computation time of a new-shared key is negligibly short, and it will not affect the performance of the WLAN communication.

Acknowledgment

This research was partially supported by National Science Council, Taiwan, R.O.C., under contract no.: NSC92-2213-E-005-027.

References

[1] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications: The insecurity of 802.11," *7th Annual Int'l. Conf. Mobile Comp. and Net.,*, Rome, Italy, Jul 2001.

[2] S. Fluhrer, I. Mantin, and A. Shamir, "Weaknesses in the key scheduling algorithm of RC4," *Eighth Annual Workshop on Selected Areas in Cryptography*, Toronto, Canada, Aug 2001.

[3] R. Housley and D. Whiting, *Temporal Key Hash.* IEEE 802.11-01/550r3, Dec 2001.

[4] R. Housley, D. Whiting, and N.Ferguson, *Alternate Temporal Key Hash.* IEEE 802.11-02/282r2, Apr 2002.

[5] M. S. Hwang, "Dynamic participation in a secure conference scheme for mobile communications," *IEEE Transactions on Vehicular Technology*, vol. 48, no. 5, pp. 1469–1474, 1999.

[6] M. S. Hwang, C. C. Lee, and W. P. Yang, "An improvement of mobile users authentication in the integration environments," *International Journal of Electronics and Communications*, vol. 56, no. 5, pp. 293–297, 2002.

[7] M. S. Hwang and C. H. Lee, "Secure access schemes in mobile database systems," *European Transactions on Telecommunications*, vol. 12, no. 4, pp. 303–310, 2001.

[8] C. H. Lee, M. S. Hwang, and W. P. Yang, "Enhanced privacy and authentication for the global system of mobile communications," *Wireless Networks*, vo. 5, pp. 231–243, July 1999.

[9] LAN MAN Standards Committee of the IEEE Computer Society, *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.* IEEE Standard 802.11, 1999 edition, 1999.

[10] A. Stubblefield, J. Ioannidis, and A. D. Rubin, "Using the fluhrer, mantin, and shamir attack to break WEP (rev. 2)," Technical Report TD-4ZCPZZ, AT&T Labs Technical Report, Aug. 2001.

[11] J. Walker, Unsafe at any key size: An analysis of the WEP encapsulation. Technical report, IEEE 802.11 Task Group E, Oct 2000.

Song-Kong Chong received the B.S. degree in Information Management and M.S. in Graduate Institute of Networking and Communication Engineering from Chaoyang University of Technology (CYUT), Taichung, Taiwan, Republic of China, in 2002 and in 2004. His current research interests include cryptography, information security, and network security.

Chia-Chun Wu received a B.B.A degree in Information Management from National Taichung Institute of Technology (NTIT), Taichung, Taiwan, Republic of China in 2004. He is currently pursuing his M.S. degree in Computer Science from National Chung Hsing University (NCHU). His current research interests include Two-Dimensional Gel Electrophoresis, DNA Microarray Images, Image Compression and Secret Image Sharing.

Hsien-Chu Wu was born in Tainan, Taiwan, Republic of China, on October 26, 1962. She received the B.S. and M.S. degrees in Applied Mathematics in 1985 and 1987, respectively, from the National Chung Hsing University, Taichung, Taiwan. She received her Ph.D. in Computer Science and Information Engineering in 2002 from National Chung Cheng University, Chiayi, Taiwan. From 1987 to 2002, she was a lecture of the Department of Information Management at National Taichung Institute Technology, Taichung, Taiwan. Since August 2002, she has worked as an associate professor of the Department of Information Management at National Taichung Institute Technology, Taichung, Taiwan. Her research interests include image authentication, digital watermarking, image processing and information security.