Enhancing Message Privacy in WEP

Darshan Purandare Ratan Guha

School of Computer Science,
University of Central Florida, Orlando, FL 32816 USA
pdarshan@cs.ucf.edu, guha@cs.ucf.edu

Abstract. The Wired Equivalent Privacy (WEP) protocol for networks based on 802.11 standards has been shown to have several security flaws. In this paper we have proposed a modification to the existing WEP protocol to make it more secure. We also develop an IV avoidance algorithm that eliminates Initialization Vector (IV) collision problem by assigning unique pattern of IV bits to each node. We achieve Message Privacy by ensuring that the encryption is not breached. The idea is to update the shared secret key frequently based on factors like network traffic and number of transmitted frames. We show that frequent rekeying thwarts all kinds of cryptanalytic attacks on the WEP.

1 Introduction

Last few years have seen the advent of wireless technologies and IEEE 802.11 standards for wireless LAN [3] is one among them. The 802.11 standard defines the Wired Equivalent Privacy (WEP) and encapsulation of data frames. It is intended to provide data privacy to the level of a wired network. Wireless cards for laptops, wireless routers (access points) are in use everywhere ranging from large scale infrastructures to home networks. However, with this added convenience and luxury, it suffered threat of attacks from hackers owing to certain security shortcomings in the WEP protocol. Lately, many new protocols like WiFi Protected Access (WPA), WPA2, Robust Secure Network (RSN) and 802.11i have come into being, yet their implementation is fairly limited. Despite its shortcomings one cannot undermine the importance of WEP and we chose to address certain security issues and propose some modifications to make it more secure.

WEP failed to achieve its goals in almost all the areas including authentication, access control, replay prevention, message modification detection, message privacy and key protection [6]. Serious security flaws like presence of relatively short Initialization vectors (IVs) [4], keys that remain static, subtle vulnerability in RC4 algorithm's [2] usage in the WEP has made it relatively weak. We have focused mainly on the issue of message privacy because this is the most important security mechanism in the WEP. An attacker cannot accomplish much if the encryption method stays strong and unbroken. However, if an intruder gets the keys then he is into the system as a legitimate user and can perform all the malicious activities without getting noticed. Message Privacy thus becomes the most critical issue among all the security mechanisms of WEP. If we can ensure that the transmitted data in the air cannot be decrypted by the attacker in its meaningful time we achieve the notion

of Message Privacy. We propose a modification to the existing WEP protocol and also develop an IV avoidance algorithm to make WEP more secure and achieve Message Privacy. Section 2 is devoted to the description of the WEP protocol. Section 3 identifies the security flaws in the WEP protocol. Section 4 talks about our proposed idea to modify the WEP protocol. It includes an IV avoidance algorithm and an access point key management system. We analyze and enumerate the features of our protocol in Section 5. Subsequently, we have our conclusion and references.

2 The WEP Protocol

The IEEE 802.11 standards have been described in detail in [3]. In this section we review the key points of the WEP protocol followed by a comprehensive description of the WEP. IEEE 802.11 defines a mechanism for encrypting the contents of 802.11 data frames.

2.1 The WEP mechanism

In the first and foremost stage each member of the Basic Service Set (BSS) is initialized with a shared secret key K, (the details of initialization are not known. It could be either end user contacting the network administrator for the shared key or network administrator distributing the keys to the legitimate user). Before sending the frame the sender calculates the Cyclic Redundancy Check (CRC) of the frame payload and appends it to the frame, which now becomes the plaintext.

Encryption: The frame is encrypted using RC4 algorithm [7]. A new Initialization Vector (IV) is chosen and is appended to the shared key K to form a “per-packet” key. This is now used to generate a RC4 key schedule. The sender uses RC4 to generate a key stream equal to the length of the plaintext. The sender XORs the generated key stream against the plaintext. This now becomes the cipher text. The sender also sends the value of the IV in the unencrypted portion of the frame and sends a Key ID # which enables the user to identify which shared key he has to use to decrypt the frame. An appropriate bit is set in the frame header to indicate that it is WEP encrypted packet.

Decryption: The decryption process works fairly the same as encryption but the reverse way. The receiver checks the encrypted bit in the WEP frame. If it is enabled he takes out the IV and uses with his shared key to generate an RC4 key schedule. RC4 is applied to the key schedule to generate a key stream equal to the length of the encrypted payload from the frame. The receiver then XORs this key stream with the encrypted payload to get the plaintext. Finally, the receiver checks the CRC of the obtained plaintext to verify that the frame data was correctly sent.

3 Security Flaws in WEP

WEP has considerable flaws in mechanisms including authentication, replay prevention, message modification detection, and most importantly key protection and message privacy [1, 6]. We enumerate the flaws of the WEP.

IV Reuse Attack: In section 2.1 we describe the WEP protocol mechanism. In this section we delve into the intricacies about how IV is used in the WEP. Instead of using fixed secret key WEP appends the secret key to the 24-bit IV value. The combined IV and secret key is used as an encryption key. Effectively we have a different key for every transmitted frame. There can be 2^{24} different IVs and we don't intend to reuse the IV with the same shared secret key because that would help an attacker break the key [1, 4]. If we choose IVs randomly there is a good chance of reusing the same IV with the same-shared key due to the "Birthday Attack" [9]. Another way in which different IVs can be derived is to start the value of IV from 0 and increment it by 1 till we reach (2^{24}-1). A single access point BSS running at 11Mbps with a typical packet distribution can exhaust the derived key space in just a couple of hours. Therefore, we always run a risk of exhausting our IVs [4]. The consequence of this is enough samples of duplicated IVs that can help the attacker guess good amount of portions of the key stream making the decoding relatively easier [6].

RC4 Weak Keys: Fluhrer et al. [2] states that the way WEP uses RC4 creates subtle weaknesses. They have proved that for certain "weak" keys a disproportionate number of bits in the first few bytes of the key stream (pseudorandom bytes) are determined by a few bits in the key itself [2]. In the WEP first few bytes are the LLC headers that always start with the same hexadecimal value of "AA". So if you know the plaintext, you can derive the key stream and start attacking the key. These flaws have become an area of major concern.

4 The Modified WEP

4.1 Our Proposed method for WEP

In order to overcome the above-mentioned flaws we propose a modification in the current WEP protocol. The idea is to update the shared secret key between the access point and the wireless nodes. The update procedure depends on the following parameters.

1. Network Traffic
2. Number of transmitted frames.

From Borisov et al [1] we always run a risk of repeating IVs after 5000 frames due to birthday paradox [9]. To ensure IV is not reused we use these parameters namely network traffic and number of transmitted frames to change our shared secret key. For example, we can have a WEP system where after every 5000 frames shared secret key is changed. Network traffic determines the number of transmitted WEP frames and that is why these two parameters are important in determining when to change the

shared secret key. Our aim is to minimize the information that an attacker can retrieve from the transmitted frames and minimize time available to him to launch an attack.

Access point creates the key mapping for the clients; it can use the MAC addresses of the client to generate the new-shared secret key. The structure of the new WEP frame is as shown in Figure 1,

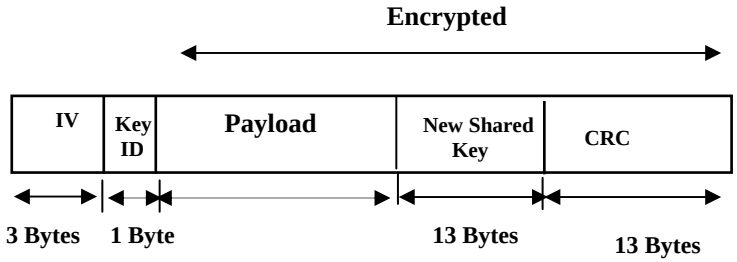

Figure 1. Proposed WEP Frame Structure

In the conventional WEP frame Key ID field signifies which key out of the four possible keys is used to decrypt the current frame. Key IDs are from 0 to 3. In our case whenever the value of the Key ID field is greater than 3, one needs to subtract 4 from that key ID value to get the correct key to decrypt the current frame. It would indicate that the data payload is carrying the new-shared key for future encryptions. For example, if the Key ID is 6 it would mean that the receiver has to use the original Key ID = (6 – 4) = 2 for decrypting the current frame. Out of the four keys this new-shared secret key will replace the first one. On subsequent updates it will replace the second key, third key and so on. At a given point of time we have 4-shared keys and new shared keys arrive at regular intervals and replace the old ones. Data Payload will be as usual except that it makes provision for extra 104 bits when the new shared secret key is being sent. When the receiver decrypts the frame it takes out the last 104 bits in the data payload and uses them as the shared secret key for future encryptions.

There are two different approaches to using keys under WEP; these are default keys and key mapping keys [6]. In the default keys all the wireless nodes and access points have the same set of shared secret keys while in the case of key mapping keys every individual wireless node has different set of shared secret keys. Default keys are easier to use and are widely used. The key mapping keys are more secure but are difficult for access points to handle. If there are large numbers of wireless nodes connected through an access point, it is difficult for an access point to keep track of the secret keys of all the wireless nodes. In the following section we have discussed updating mechanism of shared secret keys for both the cases.

A Default Key: If the system is using default keys, then access point will transmit the new-shared secret key for the future encryptions in the data payload. Since in the case of default keys all wireless nodes are using the same set of shared keys, we will need to update our shared secret keys more often. We use parameters like network traffic or number of frames transmitted for changing our shared secret key so that we do not reuse the IV for the same shared key. If a node is idle it will receive the updated shared secret key from the access point in the usual WEP frame but it won't

transmit any other data in it. Key ID field can be used to signify that this frame is carrying a new-shared key for the future encryptions.

B Key Mapping Key: In this type of system the access point will send the new-shared secret key only to the concerned individual node. Having more shared secret keys would help the system stay with the shared keys for longer as it takes more time to exhaust the IVs. The access point can generate the keys for individual nodes using the MAC addresses of the client cards.

4.2 IV Avoidance Algorithm

The WEP protocol suffered from several limitations like the IV reuse and weak RC4 keystream reuse attack as discussed in previous section. We tried to eliminate the IV reuse problem by updating the shared key as an enhancement to the existing WEP protocol. But there is always a chance of an IV reuse due to Birthday Paradox. Thus, the IV collision still remains a critical issue and cannot be ignored.

In the following section we propose an IV Collision Avoidance Algorithm that further strengthens our proposed new protocol and makes it foolproof.

1. The key idea in avoiding IV collision is to assign a unique pattern of bits to every wireless node in the system. The AP partitions the IV by choosing specific bits out of the 24 bits in the IV. AP chooses specific bits in order to avoid a predictable pattern. For e.g. consider an IV of 6 bits. The AP partitions the IV using a specific bit pattern say (1 and 3). The remaining bits (2, 4, 5 and 6) form the other partition and can assume all possible 2^4 = 16 values. The (1 and 3) pattern is unique to all the nodes. Howsoever, the values corresponding to these bit numbers vary in all possible 2^2= 4 nodes. These variations ensure that even if other partition bits assume the same values the possibility of collision is completely eliminated.
2. The above mentioned pattern will remain intact for a session and will be unique to each node to avoid IV reuse.
3. The AP communicates to each individual node by sending bits equal to (length of IV+ length of the partition number of bits). For e.g. in our case (24+N) bits following the data payload in the WEP frame structure where N is length of partition number of bits. The bits enabled in the first 24 bits will denote that they are partition bits and the remaining N bits will denote the values for that corresponding partition. For e.g. In an IV of 6 bits if the partition is (1, 3) and the corresponding value at these bit positions is (0 and 1) the AP will send a frame of (6+2) = 8 bit (101000, 01).
4. This pattern is transferred only once when the wireless node joins the access point. The pattern holds no good after the wireless node is disconnected from the network. Upon re-association a new pattern is provided by the access point.

The AP by ensuring that no bits at its pre determined pattern are repeated guarantees a complete security.

For example, if the IV length is of 4 bits and we partition it by using 2 bits. Upon joining a network the access point sends the wireless node a pattern of following

sequence numbers (0101, 01). This pattern is randomly chosen by the access point and is unique to every node. This would mean that that out of the 4 bits in the IV, bit numbers 2 and 4 are the partition bits since they are enabled and their values are 0 and 1 respectively which is shown by the two rightmost bits in the pattern as shown in the figure. Thus, we take care of IV collision by generating a pattern of sequence numbers unique to each node.

4.3 Access Point Key Management System

Our proposed method relies on updating the shared secret key. Thus it necessitates an efficient key management system on the part of the access point. In this section we suggest a framework for the access point key management system to further enhance the efficiency of the proposed protocol.

At an arbitrary time T in the system the Access Point distributes the new updated keys to all the nodes. Nodes upon receiving the keys respond by acknowledging the receipt of the key. The primary function of the access point is to keep track of the nodes that have received the new keys by monitoring the acknowledged frames. The access point distributes a pattern of sequence number to every node in the system. It ensures this pattern is unique to each node which helps eliminate IV reuse. Thus, the access point management system is pivotal to the efficiency of our proposed protocol.

5 Analysis of the Proposed WEP

5.1 Security Analysis

Our proposed technique proves to be better than the existing methods as it withstands the IV reuse attacks efficiently. Since shared keys are changed after every few thousand frames the chance of reusing the same IV is minimal. Even if an attacker finds a shared key using same IVs, which is highly improbable, by the time he detects it and launches an attack there will be a new-shared secret key in the system. In our case since we are updating secret key so often the probability of an IV being reused with the same secret key is $(1/ 2^{128})$. This makes the IV reuse attack extremely difficult for an attacker.

The WEP IV space is far too small; to give reader an idea J.R.Walker [2] has mentioned that we exceed a 50% chance of colliding IVs only after transmitting 4823 frames owing to the Birthday Paradox. For example if we perform some calculations we see that a busy access point sending 1500 byte packets and achieving an average 5 Mbps bandwidth will transmit 3500 frames per second.

Number of Frames transmitted / sec
= (5 Mbps/1500 bytes)
= 3495 (3500 approx.)

If we adhere to change of IV after every 5000 frames in order to avoid IV reuse with the same shared key, the time required between the key changes is 1.42 seconds.

Table 1 below shows the frequency with which we change our keys depending upon the bandwidth and number of frames transmitted.

Table 1. Time Evaluation between key changes [Varying Bandwidth]

Average Bandwidth	# of Frames transmitted in one second	Time[Π] between the key changes	Time[£] available to attacker
1 Mbps	700	7.14 sec	6.66 hrs
2 Mbps	1400	3.57 sec	3.33 hrs
3 Mbps	2100	2.38 sec	2.21 hrs
5 Mbps	3500	1.42 sec	1.33 hrs
7 Mbps	4900	1.02 sec	0.95 hrs
11 Mbps	7700	0.65 sec	0.60 hrs

Table 1 highlights the comparison between the times available to an attacker in the conventional WEP as against our proposed method. For this evaluation we have varying bandwidths with a utilization factor of 1.0. For e.g.

Let T = Time available to a attacker,

N = Number of Frames = 3500

Consider in the conventional WEP the shared secret key changes only after exhausting all possible 2^{24} IVs then,

$T = 2^{24}/ N = 16777216 / 3500$ sec = 1.33 hours

In our method we calculate time T by changing the shared secret key after 5000 frames.

T = 5000/3500 sec = 1.42 sec.

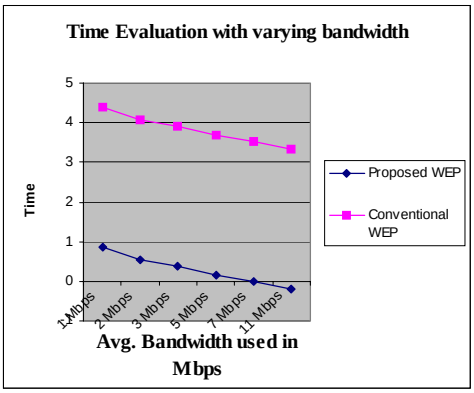

Figure 2. Log of Time in sec v/s Avg Bandwidth

[Π] Time available to an attacker in Proposed WEP

[£] Time available to an attacker in Conventional WEP

Table 2. Time Evaluation between key changes [Varying Network Load]

# of Frames transmitted per second	Time$^{\Pi}$ between the key changes	Time$^{£}$ available to attacker
500	10.0 sec	9.32 hrs
1000	5.0 sec	4.66 hrs
2000	2.5 sec	2.33 hrs
5000	1.00 sec	0.93 hrs
10000	0.5 sec	0.466 hrs
20000	0.25 sec	0.233 hrs

Table 2 shows time evaluation considering constant bandwidth (say 54 Mbps) and varying loads on the network (frames/sec). The bandwidth utilization factor is considered to be varying and less than 1. Computations are similar to those in Table 1.

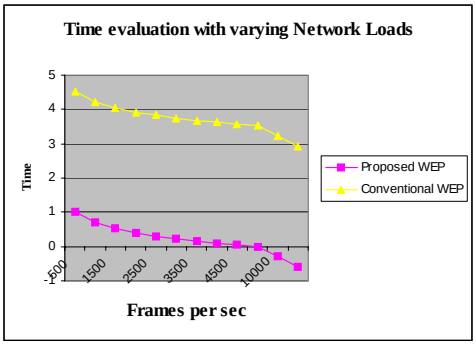

Figure 3. Log of Time in sec v/s Network Load

It is evident from Figure 2 and Figure 3 that in our proposed method the time available to an attacker is negligible and proves to be more efficient than the conventional WEP.

5.2 IV Collision Analysis

By using our proposed algorithm we successfully eliminate the IV collision problem that persisted in the conventional WEP. We change our shared secret keys after 5000 frames but using our IV avoidance algorithm we ensure that no IV is being reused in these 5000 frames thereby eliminating the security threat associated with the IV reuse.

Out of the possible 24 bits in the IVs we can have K bits for the pattern and remaining (24-K) bits varying thereby generating $2^{(24-K)}$ different IVs by each node. For example if K =8 then we have can have 8 bits for the pattern thereby meaning that

---

$^{\Pi}$ Time available to an attacker in Proposed WEP

$^{£}$ Time available to an attacker in Conventional WEP

we can have 2^8 = 256 nodes active at one point of time without collision. By incrementing the value of K we can increase the number of active wireless nodes in the network without IV collision. Similarly if K = 9, we can generate 2^{15} different combination of IVs.

We eliminate the IV reuse problem completely by following the IV avoidance algorithm. Thus, our IV avoidance algorithm in addition to the proposed WEP protocol together lays a framework for a strong and secure WEP protocol.

5.3 Overhead Analysis

Shared keys at most take 40 bits (5 bytes) or 104 bits (13 bytes). The size of the WEP frames varies from 10 bytes to 1500 bytes. The shared secret keys are exchanged at time intervals depending on various parameters previously mentioned.

Let the length of the data Payload be L, shared key length be S and K be the number of frames after which we change our shared key. That means, we use S bits out of (K*L) bits for transmitting the new shared key.

Overhead incurred = (100*S) / (K*L) %

As mentioned in J.R.Walker [4] and Borisov et al. [1], there is 50% chance of an IV reuse after transmitting 5000 WEP frames.[£] To avoid the IV reuse we take K= 5000 in the following table.

Table 3: Overhead Incurred by shared keys

L	**Overhead for S = 5 bytes**	**Overhead for S = 13 bytes**
10	0.01 %	0.026 %
50	0.002 %	0.0052 %
100	0.001 %	0.0026 %
200	0.0005 %	0.0013 %
500	0.0002 %	0.00052 %
1000	0.0001 %	0.00026 %
1500	6.67E-05 %	0.00017333 %

In Table 3 we have assumed the shared key size of 104 bits (13 bytes) and 40 bits (5 bytes). The overhead in the 13 byte case is obviously higher than 5 bytes because shared key occupies more space. These results show that the overhead associated with transmitting the shared key is very less and without loss of generality we can say that it has the same performance in terms of space occupied as the original WEP.

5.4 Analysis of hardware upgrade

The vendors can implement the above-mentioned changes in the protocol and a firmware upgrade is required to make complaint to our protocol. No additional hardware changes are needed unlike new systems such as 802.11i [10]. It's still

sometime before appropriate hardware is available for 802.11i and till then we can continue to use our existing systems efficiently and in a much more secured way.

6 Conclusions

Existing WEP protocol has been shown to be vulnerable to different kinds of cryptanalytic attacks [6]. These stem from inappropriate usage of cryptography and not because of the key size.

The possible drawback one can identify with our method is the computational overhead associated with generating, and transmitting the session keys at the access point.

In this paper we have shown that our proposed modification to the existing WEP protocol makes it more secure and robust in terms of Message Privacy. The fact that we frequently change the shared secret keys through the WEP mechanism makes any kind of cryptanalytic attack futile. The IV collision problem has been successfully resolved by our proposed IV avoidance algorithm that further enhanced the security of WEP. IEEE 802.11i standards have explicitly talked about key management which is must for its security but comes with the overhead of upgrading the hardware. Our proposed solution is a very efficient alternative till actual hardware is available and deployed for 802.11i. Our proposed system works well with the existing hardware and gives an edge over the present WEP protocol.

Reference

1. N.Borisov, I. Goldberg, and D.Wagner. Intercepting mobile communications: The insecurity of 802.11. In *MOBICOM 2001*, Rome, Italy, July 2001.
2. S.Fluhrer, I.Mantin, and A.Shamir. Weaknesses in the key-scheduling algorithm of RC4. In *Eighth Annual Workshop on Selected Areas in Cryptography*, Toronto, Canada, Aug. 2001.
3. L.M.S.C of the IEEE Computer Society. Wireless LAN medium access control (MAC) and physical layer specifications. *IEEE Standard 802.11, 1999 Edition*, 1999.
4. J.R.Walker. Unsafe at any key size; an analysis of the WEP encapsulation. IEEE Document 802.11-00/362, Oct 2000.
5. W.A.Arbaugh, N.Shankar, and Y.J Wan. Your 802.11 wireless network has no clothes. In *IEEE International Conference on Wireless LANs and Home Networks.*
6. J.Edney and W.A.Arabaugh, "Real 802.11 Security Wi-Fi Protected Access and 802.11i", 2004, Pearsons Education Inc.
7. William Stallings, Cryptography and Network Security, Principles and Practices", 3rd Edition, 2003, Pearsons Educations.
8. A.Stubblefield, J.Ioannaidis, and A.D.Rubin. ACM Transactions on Information and Security Security, Vol. 7, No. 2, May 2004, Pages 319-332.
9. http://en.wikipedia.org/wiki/Birthday_attack
10. http://csrc.nist.gov/wireless/S10_802.11i%20Overview-jw1.pdf