IEEE 802.11 WEP (Wired Equivalent Privacy) Concepts and Vulnerability

by Shivaputrappa Vibhuti
San Jose State University, CA, USA.
Shivu.Vibhuti@sun.com
CS265 Spring 2005

Abstract

The wireless networking is becoming very popular among large number of internet users. Because of the popularity of the wireless networking technology, large number of wireless networking products and protocols are available for the home and business use. Prior to the introduction of 802.11 standard by IEEE, many other technologies were developed that used various forms of spectrum hopping to facilitate wireless data transfer. Wireless transmissions are available to authorized users and also to the unauthorized users(hackers). The IEEE802.11 standard offers some level of protection. This protection, known as the Wired Equivalent Privacy (WEP) protocol, defines a set of instructions and rules by which wireless data can be transmitted over the airwaves with some amount of security. One of the objectives of WEP is to provide data privacy equivalent to the level of wired network. However, WEP protocol has many weaknesses. This paper discusses about concepts and weaknesses of WEP protocol. This paper also lists some of the available solutions for the WEP vulnerability.

1.0 Introduction

In the beginning it's believed that WEP offers impenetrable resistance to eavesdroppers/hackers. However, as wireless networks began to grow in popularity, many crypt analysts and researchers discovered flaws in the original WEP design. Many believe that there was little peer review performed on the WEP protocol. Many of the WEP flaws would have been caught in the early design phase if it's design and implementation specifications had been reviewed thoroughly. For most of the wireless networking users (especially home users), WEP is the only choice available until new security mechanisms are added to the IEEE 802.11 standard. But as people say “something is better than nothing”, even with it's known weaknesses, WEP is still more effective than no security at all. Atleast it will provide some security against unauthorized use of one's wireless network and eating up the bandwidth.

The design objectives of WEP as per section on 8.2.2 of the 1999 IEEE 802.11 standard states the following:

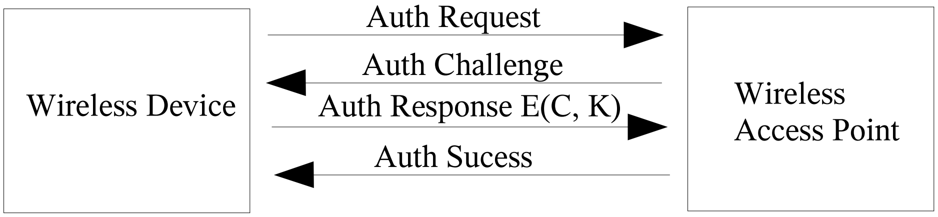
- *“It is reasonably strong:* The security afforded by the algorithm relies on the difficulty of discovering the secret key through a brute-force attack. This in turn is related to the length of the secret key and the frequency of changing keys. WEP allows for the changing of the key (K) and frequent changing of the Initialization Vector (IV).”

- *"It is self-synchronizing:* WEP is self-synchronizing for each message. This property is critical for a data-link-level encryption algorithm, where "best effort" delivery is assumed and packet loss rates may be high."
- *"It is efficient:* The WEP algorithm is efficient and may be implemented in either hardware or software."
- *"It may be exportable:* Every effort has been made to design the WEP system operation so as to maximize the chances of approval, by the U.S. Department of Commerce, of export from the U.S. of products containing a WEP implementation. However, due to the legal and political climate toward cryptography at the time of publication, no guarantee can be made that any specific IEEE 802.11 implementations that use WEP will be exportable from the USA. "
- *"It is optional:* The implementation and use of WEP is an IEEE 802.11 option."

From the above objectives, it's clear that WEP was not designed to provide a high military level security. The intention was to make it hard to break-in as opposed to impossible to break-in.

2.0 WEP Authentication

WEP security involves two parts, Authentication and Encryption. Authentication in WEP involves authenticating a device when it first joins the LAN. The authentication process in the wireless networks using WEP is to prevent devices/stations joining the network unless they know the WEP key.



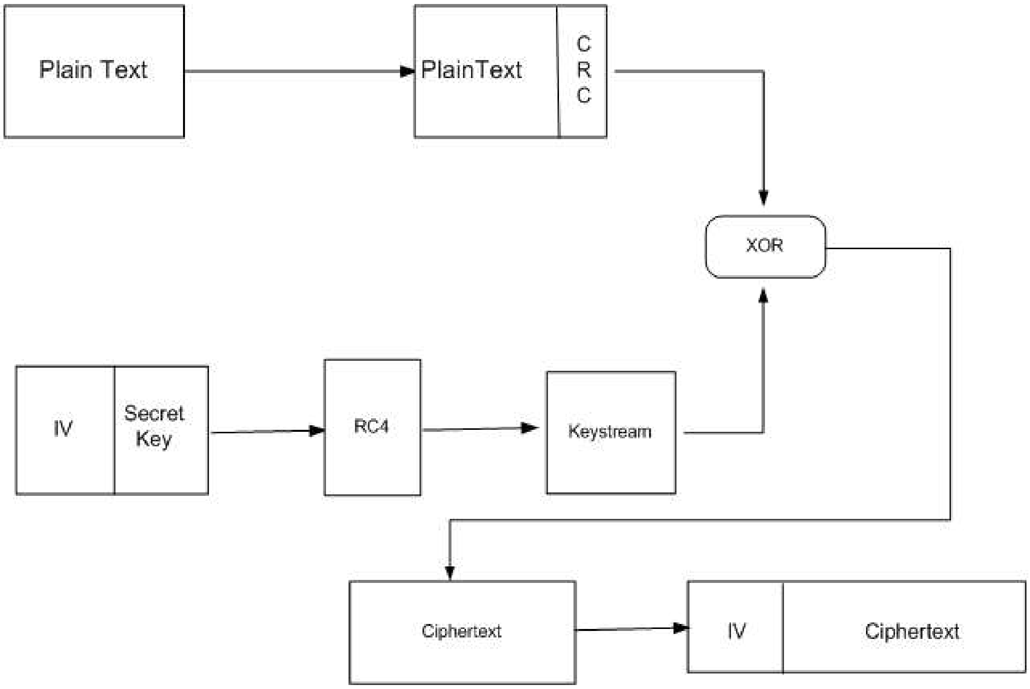
WEP Authentication

In WEP-based authentication, wireless device sends authentication request to the wireless access point, then wireless access point sends 128 bit random challenge in a clear text to the requesting client. The wireless device uses the shared secret key to sign the challenge and sends it to the wireless access point. Wireless access point decrypts the signed message using the shared secret key and verifies the challenge that it has sent before. If the challenge matches, then authentication succeeds otherwise not.

Unfortunately, in WEP, no secret key is exchanged after authentication. The same secret key or shared key is used for both authentication and encryption. So there is no way to tell whether the subsequent messages come from the trusted device or from an impostor. This kind of authentication is prone to man in the middle attack. This authentication is really not a best effort here. In the Wi-Fi specification, authentication was completely dropped, despite being in the IEEE 802.11 standard.

3.0 WEP Encryption

WEP uses RC4 stream cipher to encrypt data between access point and wireless device. WEP uses 8-bit RC4 and operates on 8-bit values by creating an array with 256 8-bit values for a lookup table (8-bits of 8-bit values).



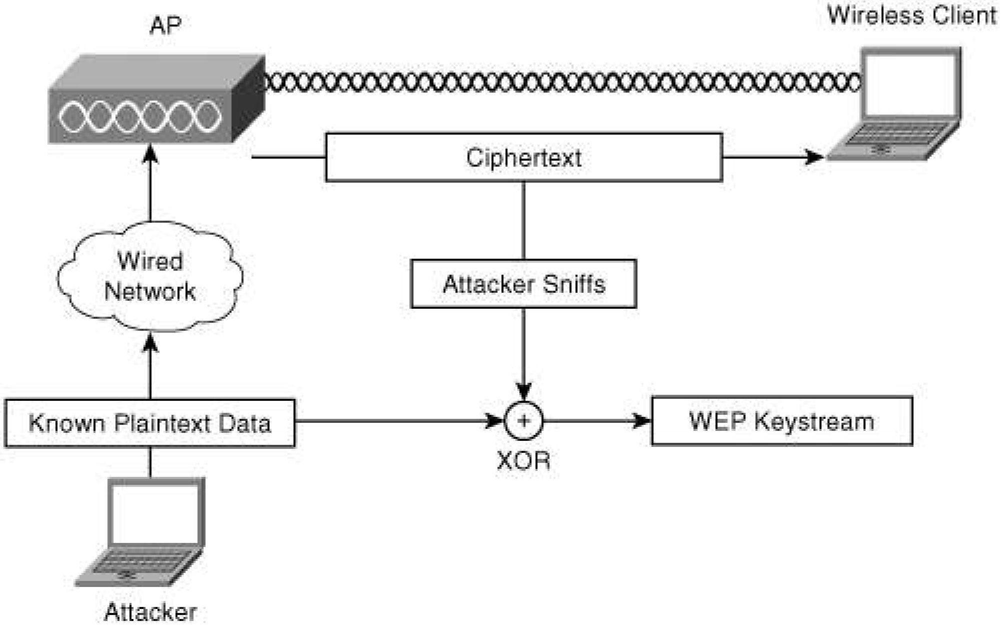
WEP Encryption

WEP uses CRC for the data integrity. WEP performs CRC (Cyclic Redundancy Check) checksum operation on the plaintext and generates CRC value. This CRC value is concatenated to the plaintext. The secret key is concatenated to the Initialization Vector(IV) and fed into the RC4. Based on the secret key and IV, RC4 generates keystream. The keystream and plaintext+CRC message are XOR'ed together. The result is the ciphertext. The same Initialization Vector that was used before, is prepended in clear text to the resultant ciphertext. The IV + Ciphertext along with the frame headers are then transmitted over the air.

4.0 WEP Vulnerability

The implementation of IV mechanisms in WEP has made the protocol vulnerable as oppose to strengthen the encryption. The IEEE 802.11doesn't specify how to generate IV's. The purpose of IV in RC4 algorithm is to ensure that the keys are not repeated. But in WEP there is no clear guidance about how to choose IV, should it be chosen randomly? Or should it be started with zero and incremented it by 1? WEP, uses either 40 or 104 bit protection with a 24-bit IV. The entire 24 bit IV space can be used up within few hours and IV's are repeated again. As the shared key is fixed, the key to RC4 keystream generator is repeated if IV's are repeated. This violates the RC4 rule of never repeating the keys. As IV is sent in clear text, the attacker can identify when

IV collision occurs. IV collisions help attacker to determine the keystream. By analyzing the two packets derived from the same IV, keystream can be obtained.



Known plaintext attack

Suppose, plaintexts are P1 and P2, keystreams K1 and K2 and the resulting ciphertexts are C1 and C2 respectively. Suppose, attacker picks two packets derived from the same IV and if he/she knows one plaintext then he/she can obtain the other unknown plaintext.

C1 XOR C2 = P1 XOR P2

If P1 or P2 is known, the other unknown plaintext can be derived using the above equation. The key or IV repetition is a major flaw in the design/implementation of WEP. Once a key stream is known, a new ciphertext can be constructed by XORing the new plain text and the known key stream to create a new, fraud cipher text. The IEEE 802.11 standard does not require the IV to change with every packet, the same IV can be used with every packet. The fraud ciphertext messages can be injected into the network by doing the above mentioned operation. The accesspoint or the wireless device cannot differentiate between the forged packets and the actual original packets.

The same key is shared between accesspoint and wireless device. If there are multiple users/devices using the same key, it helps to make the attacks on WEP more practical and increases the chances of IV collision. The key change at accesspoint requires every user to change their key accordingly. So, the key management is difficult to administer manually. Hence, most of the users don't change acesspoint keys frequently. They keep the same key for many months or years or forever. This buys an attacker more time to analyze the traffic and identify the keystream and IV reuse.

In WEP, data integrity is verified using the CRC checksum operation. The idea behind CRC is to to prevent anyone from tampering with the message in transit. The CRC is performed on the plaintext but not on the ciphertext. CRC was designed to detect random errors in the message but not to prevent from any harmful attacks. It is possible to make changes to the ciphertext without affecting the checksum. This shows that the WEP checksum failed to protect data integrity (one of the main goals of the WEP). If an attacker knows the plaintext he/she can easily compute the checksum and can inject the forged messages into the network. An attacker can also change the destination address of the packet and replace the old CRC with the modified CRC and also re-compute the IP checksum. The accesspoint won't be able to notice the changes to the original packet and forward it to the selected IP address.

Fluhrer, Mantin, and Shamir discovered a flaw in the WEP key scheduling algorithm. The main function of RC4 is pseudorandom generation. RC4 works by setting up a 256 byte array containing 0 to 255 values. Each value in the array appears only once. The order of the values can be randomized, known as permutation. So, there will be different permutation of the array each time. So there are many permutations i.e. 512 * 256! possibilities. This property makes RC4 implementation strong. However , Fluhrer, Mantin, and Shamir analyzed that "some part of the secret key is used with different exposed values, an attacker can generate the secret part by analyzing some portion of number of bits in the first few bytes of the keystream with relatively less work"[1]. In WEP the secret shared key is concatenated with the visible IV value. This weakness is known as "IV weakness"[1]. This method has been used to recover the original key in the real WEP networks. Many people have written and published software to break the WEP by capturing the network traffic to see the repeated IV's and employing the above mentioned methods.

5.0 Strengthening WEP

There are many solutions available to overcome the weaknesses of WEP that are discussed in this paper. Some of them are:

- The bigger size of the Initialization Vector (IV) can be chosen.
- The hashed value of IV can be prepended or appended to the ciphertext instead of the clear text.
- Instead of using CRC checksum, different method can be used for the data integrity verification. i.e. Hash functions
- Change secret key regularly, dynamically using secure symmetric key distribution protocols.
- Better key management using security handshake protocols .
- New authentication mechanisms using the Extensible Authentication Protocol (EAP).

6.0 Conclusion

The WEP protocol provides some level of security to wireless communication between wireless accesspoint and wireless devices. But it has many weaknesses due to the small IV space and a poor selection of CRC32 for the data integrity verification. So, instead of just relying on the WEP security alone additional measures must to be taken to provide better security among wireless devices.

7.0 Reference

[1] Scott Fluhrer, Itsik Mantin, Adi Shamir “Weaknesses in the Key Scheduling Algorithm of RC4” Lecture Notes In Computer Science; Vol. 2259 archive. Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography table of contents Pages: 1 - 24 Year of Publication: 2001 ISBN:3-540-43066-0

[2] J. R. Walker. “Unsafe at any key size; an analysis of the WEP encapsulation”. IEEE Document 802.11-00/362, Oct. 2000.

[3] Nikita Borisov, Ian Goldberg, David Wagner “Intercepting Mobile Communications: The Insecurity of 802.11”, 2001

[4] Adam Stubblefield, John Ioannidis, Aviel D. Rubin “Using the Fluhrer, Mantin, and Shamir Attack to Break WEP”, 2001

[5] Cyrus Peikari, Seth Fogie “Maximum Wireless Security” Publisher : Sams Publishing
Pub Date : December 18, 2002, ISBN : 0-672-32488-1

[6] Jon Edney, William A. Arbaugh “Real 802.11 Security: Wi-Fi Protected Access and 802.11i” Publisher : Addison Wesley, Pub Date: July 15, 2003, ISBN : 0-321-13620-9

[7] Lee Barken CISSP, CCNA, MCP, CPA “How Secure Is Your Wireless Network? Safeguarding Your Wi-Fi LAN”, Publisher : Prentice Hall PTR, Pub Date : August 26, 2003, ISBN : 0-13-140206-4

[8] Anton Chuvakin, Cyrus Peikari, “Security Warrior”, Publisher: O'Reilly, Pub Date : January 2004, ISBN : 0-596-00545-8

[9] Matthew Gast, “802.11 Wireless Networks: The Definitive Guide”, Publisher: O'Reilly, Pub Da te: April 2002, ISBN : 0-596-00183-5

[10]Krishna Sankar, Sri Sundaralingam, Andrew Balinsky, Darrin Miller, “Cisco Wireless LAN Security”, Publisher: Cisco Press, Pub Date : November 15, 2004, ISBN : 1-58705-154-0

***