# Wired Equivalent Privacy (WEP)

ARASH HABIBI LASHKARI
FCSIT, University of Malaya (UM)
Kuala Lumpur, Malaysia
a_habibi_l@hotmail.com

FARNAZ TOWHIDI
Computer Science Faculty, UTM City Campus
Kuala Lumpur, Malaysia
Farnaz.towhidi@gmail.com

RAHELEH SADAT HOSSEINI
Faculty of Computer Science, University of Ljubljana
Ljubljana, Slovenia
rahele_h@yahoo.com

***Abstract*— there are some demonstrable reasons for customers who like use from wireless technology and this is clear because there are various benefits for using wireless technology. The contrast between wireless usage and security techniques growing, show that the security is not adequate enough for this data growing. It's obvious that the hackers are able to monitor the transmitted data and hack whatever they want. So we see that these days Companies are investing more money on securing their wireless networks. There are three major type of security in wireless. In this paper, at first we try to completely explain the structure of WEP as a first wireless security technique and discuss about all versions of it. At the second step, we discuss about all problems of WEP and finally explain the solutions and improvements that done on this security technique. Then we are in the next plan witch is explain the structure of two other techniques (WPA, WPA2) and we hope that we will publish a completely comparison among wireless techniques in the near future.**

***Keywords— WEP, Wireless, Security, WLAN Protocol, 802.11***

## I. INTRODUCTION

The 802.11 WLAN standards specify the two lowest layer of the OSI network model which are physical and data link layers. The major goals of IEEE for creating these standards were made different approach to the physical layer, for example different frequencies, different encoding methods, and share the same higher layers. They have succeeded, and the Media Access Control (MAC) layers of the 802.11a, b, and g protocols are considerably identical. At the next higher layer still, all 802.11 WLAN protocols specify the use of the 802.2 protocol for the logical link control (LLC) portion of the data link layer. As you can see in Fig.1, in the OSI model of network, such protocols as TCP/IP, IPX, NetBEUI, and AppleTalk, still exist at higher layers. Each layer utilizes the services of the underside layers. "Fig. 1"

In WLANs, privacy is achieved by data contents protection with encryption. Encryption is optional in 802.11 WLANs, but without it, any other standard wireless device, can read all traffic in network. There have been three major generations of security approaches, which is mentioned below:

- WEP (Wired Equivalent Privacy)
- WPA (Wi-Fa Protected Access)
- WPA2/802.11i (Wi-Fa Protection Access, Version 2)

Each of these protocols has two generations named as personal and enterprise template.

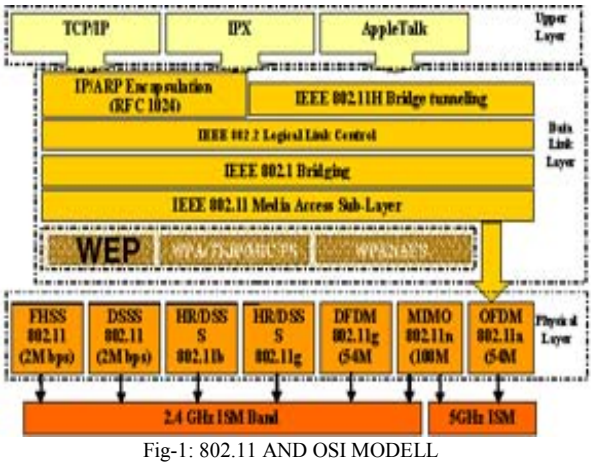


Fig-1: 802.11 AND OSI MODELL

## II. WEP- STATIC OR PERSONAL

The Wired Equivalent Privacy (WEP) was designed to provide the security of a wired LAN by encryption through use of the RC4 algorithm with two side of a data communication.

### A. *In the sender side:*

WEP try to use from four operations to encrypt the data (plaintext).At first, the secret key used in WEP algorithm is

978-0-7695-3591-3/09 $25.00 © 2009 IEEE
DOI 10.1109/ICFCC.2009.32

40-bit long with a 24-bit Initialization Vector (IV) that is concatenated to it for acting as the encryption/decryption key. Secondly, the resulting key acts as the seed for a Pseudo-Random Number Generator (PRNG).Thirdly, the plaintext throw in a integrity algorithm and concatenate by the plaintext again. Fourthly, the result of key sequence and ICV will go to RC4 algorithm. A final encrypted message is made by attaching the IV in front of the Cipher text. Now in "Fig. 2" define the objects and explain the detail of operations.

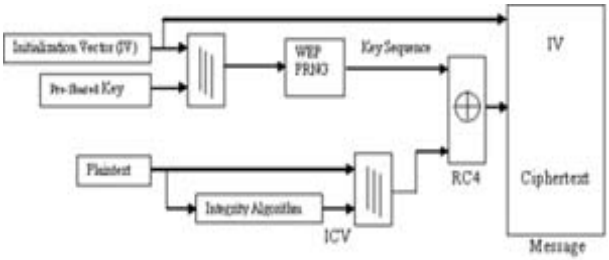


Figure 2: WEP encryption Algorithm (Sender Side)

B. *In the Recipient side:*

WEP try to use from five operations to decrypt the received side (IV + Cipher text).At first, the Pre-Shared Key and IV concatenated to make a secret key. Secondly, the Cipher text and Secret Key go to in CR4 algorithm and a plaintext come as a result. Thirdly, the ICV and plaintext will separate. Fourthly, the plaintext goes to Integrity Algorithm to make a new ICV (ICV') and finally the new ICV (ICV') compare with original ICV. In "Fig. 3" you can see the objects and the detail of operations schematically:

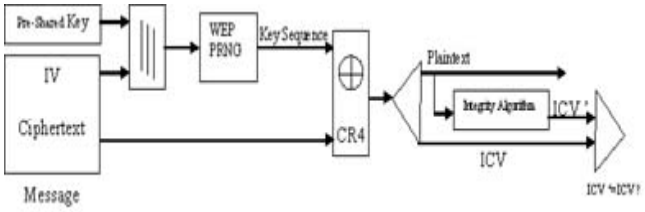


Figure 3: WEP encryption Algorithm (Recipient Side)

Now try to describe and define all of boxes in 2 previous diagrams:

**Initialization Vector (IV)**: is a randomly bits that size of it depends on the encryption algorithm and is normally as large as the block size of the cipher or as large as the Secret key.

The IV must be known to the recipient of the encrypted information to be able to decrypt it that in WEP algorithm does this by transmitting the IV along with the packet. For two different lengths (64, 128 bit) of keys IV is 24-bit.

**Pre-Shared Key**: is a simple 5- or 13-character password that is shared between the access point and all wireless network users. This key is available by administrator an bye system auto generation. For the 64-bit key the length of secret key is 40 bits and for 128-bit key the length is 104 bits.

**PRNG**: In WEP defined a method to create a unique secret key for each packet using the 5- or 13-characters of the pre-shared key and three more pseudo-randomly selected characters picked by the wireless hardware (IV).

For example, our Pre-shared key is "ARASH". This word would then be merged with "AHL" as IV to create a secret key of "AHLARASH", which would be used in encryption operations of packet. The next packet would still use "ARASH", but concatenate it this time with "ARA" to create a new secret key of "ARAARASH". This process would randomly continue during the transmission of data.

**ICV & Integrity Algorithm (CRC-32)**: is one of hashing algorithm and it is abbreviated of "Cyclic Redundancy Code". CRCs is a family of algorithms and CRC32 is one certain member of this family (other members are CRC16, XMODEM...) that 32 represent the length of checksum in bits (= 4Byte). The "CRC" term is reserved for algorithms that are based on the "polynomial" division idea. The base of the idea to compute the checksum in all CRC algorithms is the same: Take the data as a VERY long binary number and divide it by a constant divisor. If you do this with integer values you get a rest; this rest is the CRC checksum. For example 7 / 3 = 2 + rest 1 => 1 are the checksum of 8.

In CRC algorithm, four operations are doing:

Choose a width (W).

Choose a poly (P) on width W.

Append W zero bits to the message (M).

Divide M by P using CRC algorithm (XOR). The reminder is checksum.

Notice, The length of additional bits to message is the actual bit position of the highest bit in W. For example, if your W is 10011 then the length of zero bits is 4, not 5(1*2^4 + 0*2^3 + 0*2^2 + 1*2^1 + 1*2^0).

As an example:

Message: 1101011011

Poly: 10011

So W=4 and then M=1101011011+0000=11010110110000, now we can calculate with XOR:

```
11010110110000
10011
----------
01001,

1001110110000
10011
----------
00000,

10110000
10011
----------
00101,

101000
10011
----------
001110
```

Then the result is 1110, it means the checksum or ICV is 1110.

**RC4**: RC4 that is not specific to WEP; it is a random generator, also known as a key stream generator or a stream cipher, and was developed in RSA Laboratories in 1987. RC4 works by logically XORing the key to the data. In the fig.3 you can see the operation of RC4 simply:

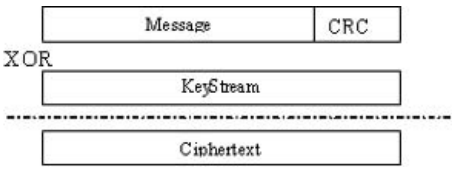


Figure 4: RC4 Algorithm

For example, if the data has the format 10010100 and the key is 1011, then RC4 (data, key) = 00101111. Since RC4 is a two-way algorithm, a second call to RC4 (encrypted data, key) is 10010100 which is the original data.

## III. WEP-DYNAMIC OR ENTERPRISE

There are some other implementations of WEP that all of them are non-standard fixes and implemented by some companies. I will explain 3 of them here:

### A. *WEP2*

This stopgap enhancement to WEP was present in some of the early 802.11i drafts. It was implement able on some (not all) hardware not able to handle WPA or WPA2, and extended both the IV and the key values to 128 bits. It was hoped to eliminate the duplicate IV deficiency as well as stop brute force key attacks. After it became clear that the overall WEP algorithm was deficient however (and not just the IV and key sizes) and would require even more fixes, both the WEP2 name and original algorithm were dropped. The two extended key lengths remained in what eventually became WPA's TKIP.

### B. *WEP plus*

WEP+ is a proprietary enhancement to WEP by Agree Systems (formerly a subsidiary of Lucent Technologies) that enhances WEP security by avoiding "weak IVs". It is only completely effective when WEP plus is used at both ends of the wireless connection. As this cannot easily be enforced, it remains a serious limitation. It is possible that successful attacks against WEP plus will eventually be found. It also does not necessarily prevent replay attacks.

### C. *Dynamic WEP*

Change WEP keys dynamically. Vendor-specific feature provided by several vendors such as 3Com. The dynamic change idea made it into 802.11i as part of TKIP, but not for the actual WEP algorithm.

## IV. WEP PROBLEMS

- *Size of IV is short and reused:*

Regardless of the key size, 24-bit long of WEP's IV can only provide 16,777,216 different RC4 cipher streams for a given WEP key. On a busy network this number can be achieved in a few hours and reuse of the same IV then becomes unavoidable. In WEP the RC4 cipher stream is XOR.ed with the original packet and the IV is sent in the clear format with each packet. If the RC4 cipher stream for a given IV is found, an attacker can decrypt subsequent packets that were encrypted with the same IV or can forge packets. If a hacker collects enough frames based on the same IV, the individual can determine the shared values among them, i.e., the key stream or the shared secret key. Because XORing two ciphertexts that use the same key stream would cause the key stream to be cancelled out and the result would be the XOR of the two plaintexts [2], [3].

Key management is lack and updating is poor:

Most wireless networks that use WEP have one single WEP key shared between every node on the network. Access points and client stations must be programmed with the same WEP key. Since synchronizing the change of keys is difficult, network administrators must personally visit each wireless device in use and manually enter the appropriate WEP key. Access points and client stations must be programmed with the same WEP key. Since the change of keys task is tedious and difficult, they are rarely changed by the system administrators. This may be acceptable at the installation stage of a WLAN or when a new client joins the network, but anytime the key becomes compromised or there is a loss of security, the key must be changed. This may not be a huge issue in a small organization with only a few users, but it can be impractical in large corporations, which typically have hundreds of users. [2], [3]

- *Problem in the RC-4 algorithm:*

RC4 implementation has been considered to have weak keys, meaning that there is more correlation between the key and the output than there should be. Determination of which packets were encrypted with weak keys is an easy job. Since the first three bytes of the key are taken from the IV that is sent unencrypted in each packet, this weakness can be exploited easily by a passive attack. Out of the 16 million IV values available, about 9,000 are interesting. They indicate the presence of weak keys. The attacker captures "interesting packets" filtering for IVs that suggest weak keys, then analyses them and only has to try a small number of keys to gain access to the network. Because all original IP packets start with a known value, it's easy to know when he/she has the right key. To determine a 104-bit WEP key, he/she has to capture between 2,000 and 4,000 interesting packets. On a fairly busy network the capture of the interesting 5,000 packets might not pose any difficulty and can be achieved in a short period of time. [2]

- *Easy forging of authentication messages:*

802.11 standards declare two types of authentication; Open System and Shared Key authentication. The theoretical idea was that an authentication would be better than no authentication. But in reality the opposite is emerged to be true. Turning on authentication with WEP, actually reduce the total security of the network and make it easier to guess WEP key for the intruders and attackers. Shared Key authentication involves demonstrating the knowledge of the shared WEP key by encrypting a challenge. The problem here is, any monitoring attacker can observe the challenge and the encrypted response. From those, then can determine the RC4 stream used to encrypt the response, and use that stream to encrypt any challenge he/she would receive in the

future. So by monitoring a successful authentication, the attacker can later forge an authentication. The only advantage of Shared Key authentication is that it reduces the ability of an attacker to create a denial-of-service attack by sending garbage packets (encrypted with the wrong WEP key) into the network [14]. To handle the task of proper authenticating wireless users turn off Shared Key authentication and depend on other authentication protocols, such as 802.1x.[2], [3]

## V. ENHANCEMENTS OVER WEP

- *Improved data encryption (TKIP)*

Temporal Key Integrity Protocol (TKIP) using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with. TKIP, is a

Temporal Key Hash Function and it is an alternative to WEP that fixes all the security problems and does not require new hardware. Like WEP, TKIP uses the RC4 stream cipher as the encryption and decryption processes and all involved parties must share the same secret key. This secret key must be 128 bits and is called the "Temporal Key" (TK). TKIP also uses an Initialization Vector (IV) of 48-bit and uses it as a counter. Even if the TK is shared, all involved parties generate a different RC4 key stream. Since the communication participants perform a 2-phase generation of a unique "Per-Packet Key" (PPK) that is used as the key for the RC4 key stream. [2].

TKIP is a TGi's response to the need to do something to improve security for equipment that already deployed in 802.11. TGi has proposed TKIP as a mandatory-to-implement security enhancement for 802.11, and patches implementing it will likely be available for most equipment in late 2002.

TKIP is a suite of algorithms wrapping WEP, to achieve the best security that can be obtained given the problem design constraints. The TKIP algorithms are designed explicitly for implementation on legacy hardware, hopefully without unduly disrupting performance. TKIP adds four new algorithms to WEP:

- A cryptographic message integrity code, or MIC, called Michael, to defeat forgeries;
- A new IV sequencing discipline, to remove replay attacks from the attacker's arsenal;
- A per-packet key mixing function, to de-correlate the public IVs from weak keys; and
- A re-keying mechanism, to provide fresh encryption and integrity keys, undoing the threat of attacks stemming from key reuse.

The remainder of this section analyses each of the TKIP components, and the next section indicates how they are intended to work together to rescue WEP.

TKIP is an acronym for "Temporal Key Integrity Protocol." The name is something of a misnomer. The TKIP re-keying mechanism updates what are called temporal keys, which are consumed by the WEP encryption engine and by the Michael integrity function.

- *User authentication (Use EAP Method)*

Which is missing in WEP, through the extensible authentication protocol (EAP)? WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network. For detailed information about EAP please refer to [2].

- *Integrity (Michael Method)*

A new mechanism Message Integrity Code (MIC) for TKIP is computed by a new algorithm namely Michael. Message Integrity Code (MIC) is computed to detect errors in the data contents, either due to transfer errors or due to Purposeful alterations. The new MIC for TKIP is computed by a new algorithm called "Michael". It is a 64-bit MIC that is added to the Data and the ICV. The ICV is CRC of Data and MIC. [2]

## CONCLUSIONS

In this research we explain the structure of WEP in sender and receiver side and try to describe about all steps verbally and practically at the same time. Then discuss about all major problems in WEP as IV length and RC-4 algorithm and key management. Finally explain about improvement and solutions that submitted till now like TKIP, Mickael and EAP method.


## ACKNOWLEDGMENT

We would like to express our appreciation to our parents and all the teachers and lecturers who help us to understand the importance of knowledge and show us the best way to gain it.


## REFERENCES


[1] Donggang Liu, P. N. Security for Wireless Sensor Networks, Springer., November, 2006

[2] Garcia, R. H. a. M. AN ANALYSIS OF WIRELESS SECURITY*. CCSC: South Central Conference. 2006

[3] Kempf, J. Wireless Internet Security: Architecture and Protocols Cambridge University Press. October, 2008

[4] OZEL, H. I. B. a. I. B. a. M. "Wireless Network Security: Comparison of WEP (Wired Equivalent Privacy) Mechanism, WPA (WI-FI Protected Access) and RSN (Robust Security Network) Security Protocols." ICST 978-963-9799-19-6. Spring, 2008

[5] Seyit A. Çamtepe, B. Y. "Combinatorial design of key distribution mechanisms for wireless sensor networks" IEEE/ACM Transactions on Networking (TON) Volume 15(Issue 2): 13. April, 2007

[6] Whalen, S. Critical Review of Unsecured WEP. IEEE Congress on Services.2007

[7] Yanchao Zhang, Y. F. "A secure authentication and billing architecture for wireless mesh networks" Wireless Networks Volume 13 (Issue 5): 16, 2006

[8] Yoshiaki Hori, K. S. Security Analysis of MIS Protocol on Wireless LAN comparison with IEEE802.11i. Proceedings of the 3rd international conference on Mobile technology, applications & systems ACM, October, 2006

[9] Zang Li, W. X., Rob Miller, Wade Trappe. Securing wireless systems via lower layer enforcements 5th ACM workshop on Wireless security ACM , Sep 2006