International Journal of Information Technology and Knowledge Management
January-June 2011, Volume 4, No. 1, pp. 91-95

ENHANCEMENT OF WIRED EQUIVALENT PRIVACY

Rajnesh Singh[1], Vipin Rai[1] & Amit Kumar[2]

The explosive growth of internet and consumer demand for mobility has fuelled the exponential growth of wireless communications and networks. Mobile users want access to services and information, from both internet and personal devices, from a range of locations without the use of a cable medium. IEEE 802.11 is one of the most widely used wireless standards. So Security is a strong requirement for effective deployment of business wireless communication applications. Therefore, many proposals dealt with security holes in Wired Equivalent Privacy protocol (WEP). The WEP is a security protocol implemented for the wireless networks 802.11b, possesses so many drawbacks. Indeed, it is possible to crack the WEP key used with a minimum of resources or a minimum of time. The results are different in time and from resources according to the size of the key and its complexity as well as the traffic circulating on the wireless network. In this write up, several weakness of the WEP has been studied. An enhanced version of WEP, which is more reliable and has many advantages over WEP, has been implemented. The eWEP protocol address a digitally signed authentication, uses AES to provide confidentially and hashing to provide integrity.

1. Introduction

Wireless connections have important security issues to keep the intruders from accessing, reading & modifying network traffic. However mobile systems need to remain connected while on the move. We need an algorithm, which provides same level of security as that of physical wires.

In this paper write up includes the detail Encryption and Decryption process of WEP, Limitation of WEP, Details of the Wired Equivalent Privacy protocol, Different weakness of this protocol, Possible attacks, Proposes a design for Enhancement of WEP i.e. eWEP:

The eWEP aims to provide establishment of enhanced security channels, between two nodes. In proposed eWEP using following algorithms.

1. Hash function (SHA-1) is used to generate the message digest.
2. The RSA algorithm is used for generating the signature.
3. The AES algorithm is used for Encryption and Decryption of message.

2. Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) is a scheme that is part of the IEEE 802.11 wireless Networking standard to secure IEEE 802.11 wireless networks(also known as Wi-Fi networks). The goal of WEP is to provide data privacy to the level of a wired network. It is widely deployed in Wireless Networks.

2.1. WEP Overview

IEEE 802.11 defines a mechanism for encrypting the contents of 802.11 data frames. The following elements are directly relevant to its analysis:

- A set of up to 4 keys shared between all the members of the network (KS);
- An encryption algorithm. For WEP this is the RC4 stream cipher, used to generate a key stream, which is XOR against plaintext to produce ciphertext (which is shown in fig. 2.1).

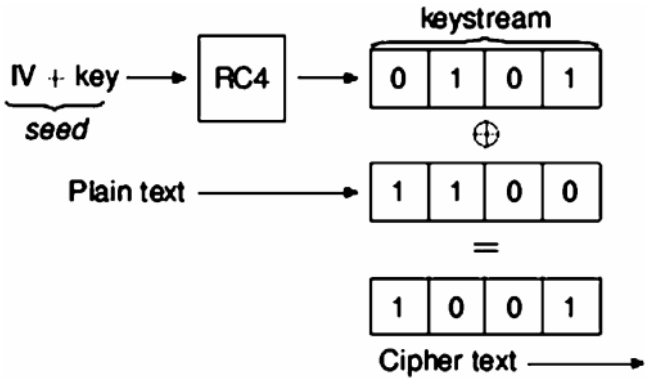

Fig. 1: Basic WEP Encryption: RC4 Keystream XOR with Plaintext [2]

[1]Department of Computer Science & Engineering, IIMT College of Engineering Greater Noida, India

[2]Department of Computer Science & Engineering, IEC-CET Greater Noida, India

Email: [1]Rajneshcdac.mtech@gmail.com, [1]Vipinrai82@gmail.com, [2]amitvnskumar@rediffmail.com

2.2. WEP Operation

The process of disguising (binary) data in order to hide its information content is called encryption. Data that is not enciphered is called plaintext (denoted by P) and data that is enciphered is called ciphertext (denoted by C). The process of turning ciphertext back into plaintext is called decryption. A cryptographic algorithm, [3] or cipher, is a mathematical function used for enciphering or deciphering data. Modern cryptographic algorithms use a key (denoted by k) to modify their output. The encryption function E operates on P to produce C:

$$Ek(P) = C \quad (1)$$

In the reverse process, the decryption function D operates on C to produce P:

$$Dk(C) = P \quad (2)$$

As illustrated in Figure 2.2, note that if the same key is used for encryption and decryption then

$$Dk(Ek(P)) = P$$

With the help of equation 1 and 2.

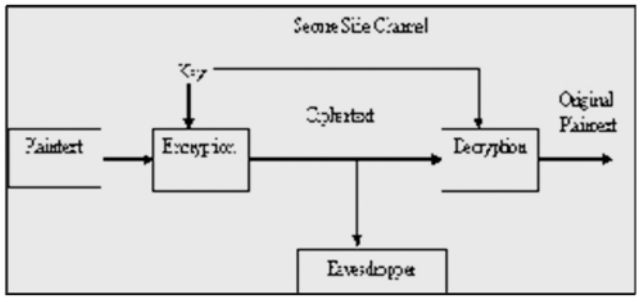

Fig. 2: Encryption and Decryption Process [3]

2.3. Encryption Process

The WEP algorithm proposed in this submission is a form of electronic code book in which a block of plaintext is bitwise XOR with a pseudo random key sequence of equal length. The key sequence is generated by the WEP algorithm.

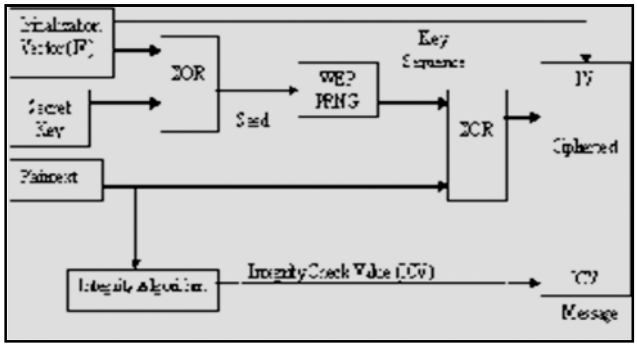

Fig.3: WEP Encipherment Block Diagram [3]

3. ENHANCED WEP (EWEP)

3.1. Introduction

The eWEP aims to provide establishment of enhanced security channels, between two nodes which is using eWEP. In this section encryption and decryption procedure of eWEP is explained.

In the section 2 describe that 1how WEP use RC4, but in proposed eWEP, RC4 is replace by SHA-1 algorithm. In the eWEP we are using the Hash function (SHA-1) which is generate the message digest, after that apply the RSA algorithm on the message digest with using the private key of sender i.e. generate a code which is called as the signature. This hash code is compare with the decrypted signature, if both message digest is match then message is right otherwise the message having some error.

In the table show some symbols, which is used to procedure of eWEP:

Table 1
Notation of eWEP

S	Sender, which send the message M.
R	Receiver, which receiving the message M.
M	Message i.e. sending from one node to another node.
E1	Encrypted message, this done by help of AES
E2	Encrypted message E1 appended with Signature (Encrypted hash message)
H1, H2	Hash code generated by SHA-1
Ka	Sender' Private key
Ua	Sender's Public key

3.2. Procedure for Enhanced WEP

The following steps are involved in design of enhanced WEP (eWEP) protocol as shown in figure No. 5.1 and 5.2.

Step 1: The sender S produces the message M.

Step 2: The message M is taken to be the input of SHA-1 to generate the hash code of The message M, i.e. H1.

Step 3: The hash code, H1 is encrypted by RSA using the sender's private key, Ka.

Step 4: The message, M is encrypted into E1 by using Advanced Encryption standard (AES), which uses the mathematical algorithm developed by Rajndeal.

Step 5: The Encrypted Hashed message Step-3 is appended with the encrypted message, E1 from step-4. (Encrypted message send with signature) i.e. E2= E1+ Encrypted H1 so E2 is send by sender S.

Sender's side:

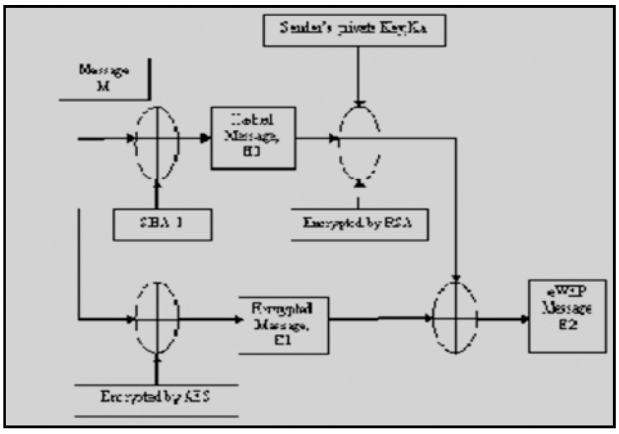

Fig. 4: eWEP on Sender Side

Receiver's side:

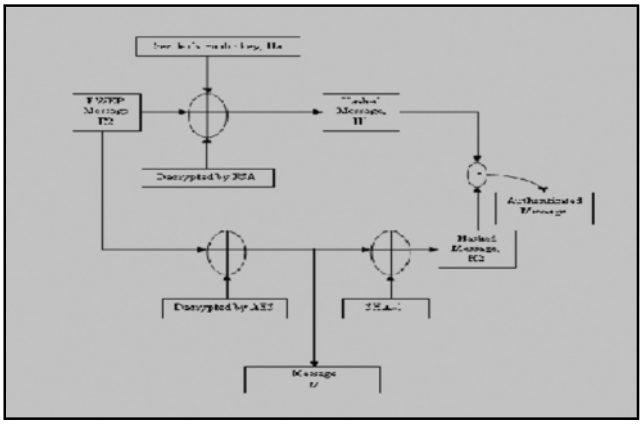

Fig.5: eWEP on Receiver Side

Step 6: The receiver uses RSA with sender's public key, 'Ua' to decrypt the encrypted H1 into H1. (only signature is decrypted with public key, Ua).

Step 7: At the receiver end, the encrypted message, E2 is decrypted by using AES (this is original message M).

Step 8: On the output of step 7 is apply hash function i.e. Use SHA-1 for generating Hash code H2. (This is done for signature verification)

Step 9: If comparison of H1 and H2 is successful i.e. the message M1 authenticated

4. RSA

The scheme developed by Rivest,Shamir and Adleman makes use of an expression with exponentials. Plaintext is enctypted in blocks, with each block having a binary value less than some number N. That is, the block size must be less than or equal to $\log_2(N)$; the block size is κ bits where $2^{\kappa} < N <= 2^{\kappa+1}$.

Here M is digest which is output of SHA-1, this digest is fixed in the length. Now we are generating the sign for original message by using the RSA. The operation of RSA is explain in this section [10].

4.1. Operation

RSA involves a public and private key. The public key can be known to everyone and is used for Decrypting messages. Messages encrypted with the private key can only be decrypted using the public key. The keys for the RSA algorithm are generated the following way.

Choose two large random prime numbers P and Q:

1. Compute N = PQ

   N is used as the modulus for both the public and private keys;

2. Compute the totient:. $\Phi(N) = (P - 1)(Q - 1)$;

3. Choose an integer e such that $1 < e < \Phi(N)$, and e is coprime to $\Phi(N)$.

   i.e. e and $\Phi(N)$ share no factors other than 1; gcd $(e, \Phi(N)) = 1$. e is released as the public key exponent;

4. Compute d to satisfy the congruence relation $de \equiv 1 \pmod{\equiv (N)}$.

i.e.: $de = 1 + \Phi(N)$ for some integer κ. d is kept as the private key exponent.

The private key consists of the modulus N and the private (or encryption) exponent d which must be kept secret. The public key consists of the modulus N and the public (or decryption) exponent e.

For efficiency a different form of the private key can be stored:

C and Q: the primes from the key generation,

d mod (P – 1) And d mod (Q – 1) often called dmp1 and dmq1.

$Q^{-1} \bmod (Q)$: often called iqmp.

- All parts of the private key must be kept secret in this form. P and Q are sensitive since they are the factors of N, and allow computation of d given e. If P and Q are not stored in this form of the private key then they are securely deleted along with other intermediate values from key generation.

4.2.1. Signature Generating

He first turns M into a number M < N by using an agreed-upon reversible protocol known as a padding scheme. He then computes the ciphertext C corresponding to:

$$C = M^d MOD\ N$$

This C is called signature which is appended with Encrypted message. Encryption of message is done by AES (which is showing in below section).

4.3. Advanced Encryption Standard (AES)

4.3.1. Introduction

The Advanced Encryption Standard (AES) specifies a FIPS-approved Cryptographic algorithm that can be used to protect electronic data. The AES algorithm is a symmetric block cipher that can encrypt (encipher) and decrypt (decipher) information. Encryption converts data to an unintelligible form called ciphertext; decrypting the ciphertext converts the data back into its original form, called plaintext.

The AES algorithm is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits [10].

This standard specifies the Rijndael algorithm a symmetric block cipher that can process data blocks of 128 bits, using cipher keys with lengths of 128, 192, and 256 bits. Rijndael was designed to handle additional block sizes and key lengths, however they are not adopted in this standard. Throughout the remainder of this standard, the algorithm specified herein will be referred to as "the AES algorithm." The algorithm may be used with the three different key lengths indicated above, and therefore these different "flavors" may be referred to as "AES-128", "AES-192", and "AES-256".

5. EXPERIMENTAL RESULTS

This section describes the experiment result of eWEP. In the Figure 9.1 shows the Main Form, which contain a textbox and six buttons i.e.

I. Encryption.

II. Signature.

III. Message_send.

IV. Message_Received.

V. Signature_Decryption.

VI. Authentication.

The textbox contain the message i.e.

Message is: "My name is vinod kumar".

This form shows the encryption of message by AES algorithm.

Key is hexadecimal type.

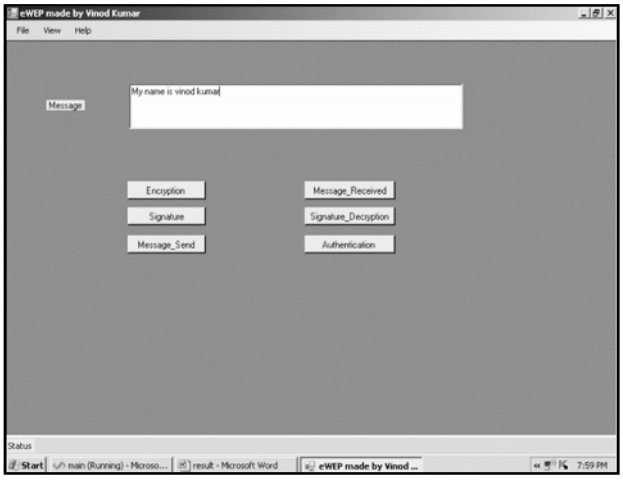

Fig. 6: Main Form of eWEP

So value of key = 23bc4ed675a80c09f132bc56 d076af65

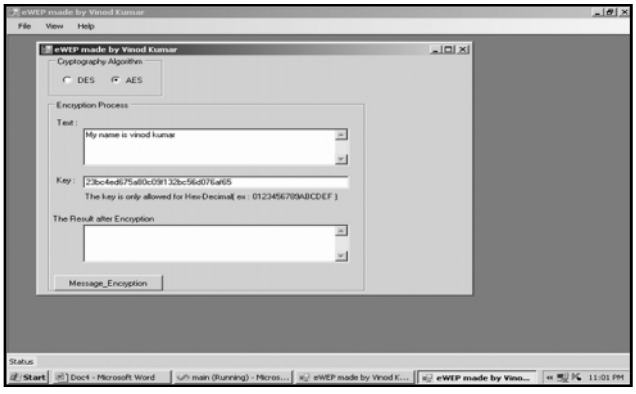

Fig. 7: Message before Encryption

- On clicking "Message_Encryption" Button.

Message is encrypted by AES algorithm, which shows in below figure 9.3

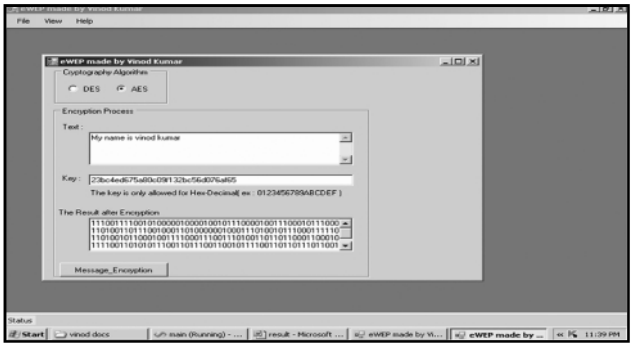

Fig. 8: Message Encryption by AES

Encryption message is:

11100111100101000001000010010111000010011100001011100011010011011100100011010000001000111101001011100011111011010010110001001111

00011100111010011011011000110001011110011 0
10101110011011100110010111100110110111011 0
01001010110001010111000111101000010100101 00010

This form shows the decryption of Signature. Signature is decrypt by the RSA algorithm.

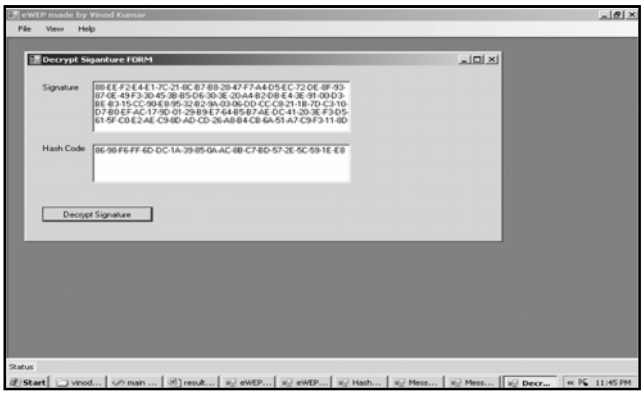

Fig. 9: Signature Decryption Form

Signature is:

88-EE-F2-E4-E1-7C-21-8C-B7-B8-28-47-F7-A4-D5-EC-72-DE-8F-93-87-0E-49-F3-30-45-3B-B5-D6-30-3E-20-A4-B2-DB-E4-3E-91-00-D3-BE-B3-15-CC-90-E8-95-32-B2-9A-03-06-DD-CC-C8-21-1B-7D-C3-10-D7-B0-EF-AC-17-9D-01-29-B9-E7-64-B5-B7-AE-DC-41-20-3E-F3-D5-61-5F-C0-E2-AE-C9-8D-AD-CD-26-A8-B4-CB-6A-51-A7-C9-F3-11-8D-38-80-FB-F4-BC-8D-37-B3-16-4D-B5-E5-36-9B-7A-0F-BC-F7-D0-B0-0A-AD-E5-C2-72-B0-D4-BE On clicking Decrypt_Signature Button, Signature is decrypted i.e.

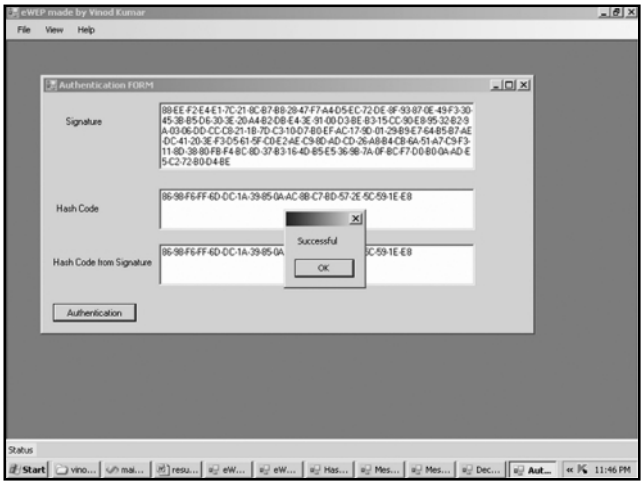

Fig. 10: Authentication Form

6. COMPARISON BETWEEN EWEP AND WEP

In the below table shows the comparison of eWEP with WEP:

Table 2
Comparison of eWEP with WEP

	WEP	eWEP
Cipher	RC4	AES
Key Length	40/104 bits	128 bits
Key life	24 bits	48 bits
Data Integrity	CRC32	Digital Signature
Replay Attack	None	IV sequence
Key Management	Bad	Good

7. CONCLUSION AND FUTURE WORK

7.1. Conclusion

This write up outlines various weakness of WEP. In this work, the RC4 algorithm, which was used in WEP has been replaced by AES. As the result, the Initialization Vector (IV) problem of WEP has been overcome. The methods of key management were weak and did not scale to large networks. The key length was too small in WEP.

This write up also implements a digital signature mechanism to provide authentication. And at last, the hash function (SHA-1) which has been used in the proposed protocol yields message integrity.

7.2. Future Work

In the future work the performance of enhanced WEP would be analyzed. In the future can focus on the problem to provide more security on data transmit and also can do focus change the key size

REFERENCES

[1] Walker, "J. Unsafe at Any Key Size: an Analysis of the WEP Encapsulation", IEEE 802.11 doc00362, Oct.27, 2000, grouper.ieee.org/groups/802/1.

[2] Hassan, Challal, "Enhanced WEP: an Efficient Solution to WEP Threats", Wireless an Optical Communications Networks, 2005. WOCN 2005. Second IFIP International Conference on March 2005.

[3] Borsc M. and Shinde H. "Wireless Security & Privacy", Personal Wireless Communications, CPWC, IEEE International Conference, 23-25 Jan., 2005.

[4] Scott Fluhrer, Itsik Mantin and Adi Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", Eighth Annual Workshop on Selected Areasin Cryptography (August 2001).

[5] W. Shunman, T. Ran, W. Yue, Z. Ji, "WLAN and its Security Problems", Proc. of the Parallel and Distributed Computing, Applications and Technology, Chengdu, China, 29 Aug. 2003.

[6] "The Security of WEP Wired Equivalent Privacy" http:/ www.cse.ogi.edu.

[7] Arbaugh, W., "An Inductive Chosen Plaintext Attack Against WEP/WEP2", IEEE Document 802.1102/ 230,May2001,grouper.ieee.org/groups/802/.