International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161
Available at http://inpressco.com/category/ijcet

©2016 INPRESSCO®, All Rights Reserved

Research Article

Refinement of Wired Equivalent Privacy

Mahak[*]

Department of CSE, Kurukshetra University Kurukshetra, India

Accepted 25 April 2016, Available online 30 April 2016, **Vol.6, No.2 (April 2016)**

Abstract

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 .It is required to protect and testify the wireless network as a reliable system for data communication. In this paper an enhanced version of WEP has been proposed which provides confidentiality, integrity, authentication and reply detection.

Keywords: *Wired Equivalent Privacy (WEP), Advanced Encryption Standard (AES). Secure Hash Algorithm 1(SHA-1), RSA, Digital Signature.*

1. Introduction

Wired Equivalent Privacy (WEP) is a protocol. WEP uses the stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity. Standard 64-bit WEP uses a 40 bit key, which is concatenated to a 24-bit initialization vector (IV) to form the RC4 traffic key (Hassan etal ,March 2005). A 128-bit WEP key is almost always entered by users as a string of 26 Hexadecimal (Hex) characters (0-9 and A-F). Each character represents 4 bits of the key. 4 × 26 = 104 bits; adding the 24-bit IV brings us what we call a "128-bit WEP key". A 256-bit WEP system is available from some vendors, and as with the above-mentioned system, 24 bits of that is for the IV, leaving 232 actual bits for protection. This is typically entered as 58 Hexadecimal characters. (58 × 4 = 232 bits) + 24 IV bits = 256 bits of WEP protection Key size is not the only major security limitation in WEP. In WEP plaintext (message) that is enciphered is called ciphertext. The process of turning ciphertext back into plaintext is called decryption. In the WEP RC4 algorithm is used for encryption and decryption process.(Borsc M etal ,25 Jan 2005).

This paper is organized as follows. Section 2 presents, weakness of Wired Equivalent privacy protocol, and possible attacks. Section 3, describes how Enhanced WEP is implemented. Section 4 describes security services of eWEP. Section 5 compares performance of WEP and eWEP. Section 6 provides conclusion and recommendations for future work and section 7 shows the references.

2. WEP

The Wired Equivalent privacy protocol (WEP) offers the following functionality:

1. *Data Privacy*: it is the basic service offered by the WEP. Transiting data can be read only by authenticated communicating members;
2. *Data Integrity*: WEP offers a guarantee to the receiver that data was not altered;
3. *Access Control*: depends strongly on data integrity; a corrupted message is considered as non authenticated and is automatically rejected.(Hassan etal ,March 2005) (Borsc M etal ,25 Jan 2005)

A. WEP's Security Mechanisms

In this section, provides WEP functioning processes, which mechanisms used to implement security

Initially, both of the communication entities share a secret key k. k will be used further to encrypt transmitted data. Let S be a source which sends a message M to a receiver R. S begins by calculating a checksum using the CRC (Cyclic Redundancy Check) algorithm widely used in network protocols. Let us note T=(M,CRC) the message produced by a simple concatenation of M and its CRC.

Then, S encrypts T using the RC4 algorithm. RC4 is a stream cipher. It generates a keystream KS using two inputs:

- The key k shared between S and R, which is 40 bits length;
- An Initialization Vector (iv), used principally to minimize probability of feeding RC4 with the same entries.

[*] Corresponding author is PhD Scholar

KS is XOR with T to produce the cipher text C. To decrypt C, R needs to reconstruct the same keystream KS and XOR it with C, indeed:

C XOR KS = (T XOR KS) XOR KS = T XOR (KS XOR KS) = T

However, to reproduce KS, R needs to know Initialization Vector (iv). In WEP, iv is concatenated to the cipher text C before sending it. Figure 1 illustrates this encryption process.

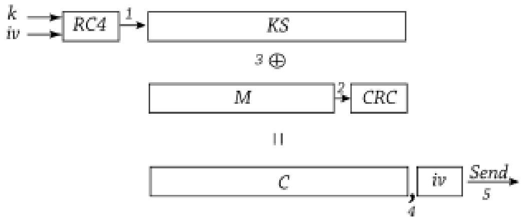

Fig. 1 Encryption process in the WEP. The numbers show the different steps to encrypt a message M

Note that iv is sent as clear text, without any kind of encryption. This process ensures:

- *Data Privacy*: All transmitted data is encrypted and only communication entities can decrypt it.
- *Data Integrity and Authentication*: the checksum is verified upon receiving the message. Thus, all modifications of the message during its transmission will be detected.

B. Attacks

All the security model of WEP is based upon its resistance against brute-force attacks. There are currently two implemented variants of the WEP:

- *Classical WEP*: as defined by IEEE, the key length is 40 bits and the 24 bits are reserved for iv.
- *128 bits WEP*: it is a version proposed by manufacturers, where the key length is 104 bits, the remaining 24 bits are reserved for iv.

It is important to note that the 128 bits version, and despite its name, offers only a 104 bit security. In fact, the part devoted to iv is transmitted as clear text on the wireless network. Some vendors have already made this mistake with the classical WEP while claiming that their products offer a 64 bits security. The basic threat in the WEP is due to a property of stream ciphering. Indeed, in XOR based stream cipher, there is a golden rule to respect: "Reuse of keystream is forbidden" . It is for this purpose that iv field was added, because the key k changes rarely. The security hole of WEP is induced by the following property: let KS be a keystream obtained with k and some initialization vector iv, T1 and T2 two messages we want to transmit, C1 and C2 encrypted messages corresponding to T1 and T2 respectively So, we can show that

C1 XOR C2 = T1 XOR T2.
Indeed, C1 XOR C2 = (T1 XOR KS) XOR (T2 XOR KS) = (T1 XOR T2) XOR (KS XOR KS) = T1 XOR T2.

This property means that if any person knows C1 and C2 (they can be easily obtained by eavesdropping) and T1, he can guess T2 by simple XOR. However, he would find some difficulties before being able to decrypt exchanged messages. One question becomes imperative: "is it possible to avoid reuse of initialization vectors?" The answer is no. The number of values of iv is limited. An access point sending frames of 1500 Bytes with a rate of 5 MB/s (about 45% of the maximal bandwidth), will inevitably reuse some iv in less than 12 hours

The attacker should also detect reuse of initialization vectors. This is very simple to do since ivs (Initialization Vector) are transmitted as clear text. Now that the attacker has two or more encrypted messages corresponding to some iv, he has to find one original message to be able to decrypt the others using only XOR operations.

C. Security Holes Analysis

Once the RC4 cipher text is decrypted, none of the security services can be guaranteed. CRCs are not signed by definition. Thus, the attacker can decrypt, then modify or even forge his own messages, then recomputed the corresponding CRC, and impersonalize some communication entity. Thereby making data integrity and authentication services obsolete.

All WEP weaknesses (Hassan etal ,March 2005) come from four main conception flaws:

- The initialization vector is transmitted as clear text. Beside the fact that this weakens the power of encrypting, attackers are in a position to detect every iv reuse.
- The key is rarely renewed. Key (k) updating techniques are completely leaved as implementation details. Thus, manufacturers are free to use the techniques that they find suitable. The worst, an implementation that doesn't plan key renewing is within the norm.
- Data Source Authentication. The WEP has not planed a mechanism to ensure data source authentication. As mentioned above, using CRCs allows attackers to forge their own messages, and send them as coming from a known entity (this hole is called impersonation). Using Message Authentication Code (MAC) would be an efficient solution to this problem. MACs are usually used to guarantee data source authentication. Another solution is to secure enough the privacy mechanism, so that nobody will be able to access the CRC. This is what WEP intended to do but failed to achieve.
- Security services are all implemented using only one mechanism. All the security scheme is based

upon the strength of the mechanism of data privacy service. Thus, once the privacy of data is broken, all other services data integrity and access control are directly broken.

3. Enhanced WEP (eWEP)

eWEP is a communication protocol which is free from the attacks defined above section. The proposed protocol provides data Integrity, authentication and replay detection. This table shows some symbols, which are used in procedure 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

A. Procedure for Enhanced WEP

The following steps are involved at sender side

Step 1: The sender S produces the message M.
Step 2: SHA-1 to generate the hash code of the message M, i.e. H1.

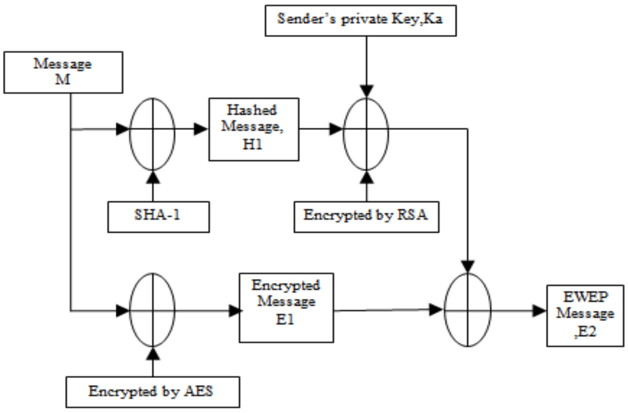

Fig. 2 Process on sender side in eWEP

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) .
Step 5: The Encrypted Hashed message Step-3 is appended with the encrypted message E1from step-4 .(Encrypted message appended with Signature). i.e.. E2= E1+ Encrypted H1 so E2 is send by sender S.
Step 6: The receiver uses RSA with sender's public key, Kb to decrypt the encrypted H1into hash code H1. (only signature is decrypted with public key, Ua).

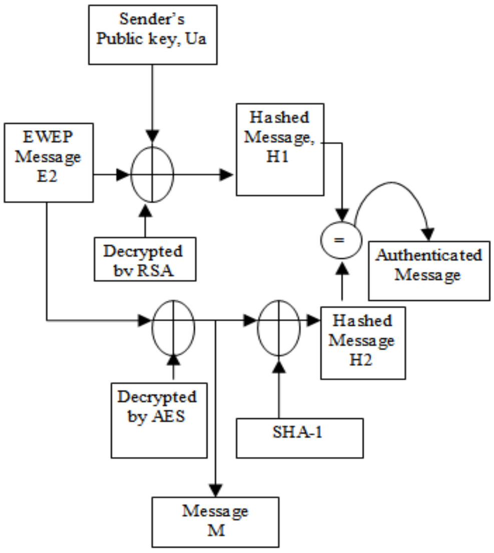

Fig.3 Process on Receiver side In eWEP

Step 7: At the receiver end , the encrypted message, E2 is decrypted by using AES
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 comparison between H1 and H2. (for message authentication).
Step 9: If comparison of H1 and H2 is successful i.e. the message M1 authenticated

B. Encryption Process

In eWEP we encrypt the message M with AES and i.e is called E1.

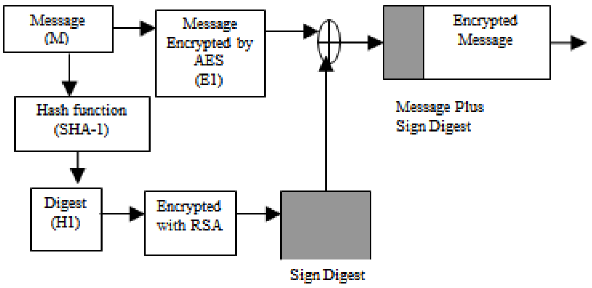

Fig. 4. Encryption Process of eWEP

Here we are using AES for the Encrypt the Original message. On the other hand we also use the concept of digital signature. So first we generate the digest of the message. Digest is generated by using the Hash function (SHA-1). SoSHA-1 is produce the digest H1.i.e. fixed in the length. Now by the using the RSA with private key of sender we encrypt this digest .i.e. is called sign digest. Now appended this sign digest with the encrypted message (E1) which is shown in the fig. 4

So. The sender send the encrypted message (E2) with the digital signature like this: E2 = E1+Sign Digest.

This E2 is send by the sender.(Atul Kahate) (Wiliam Stalling)

C. Decryption process

In the above section we see the Encryption process of eWEP.But now we see the Decryption process of eWEP. On receiver side, Encrypted message is received with the sign.

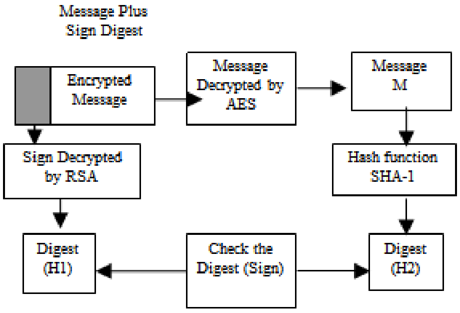

Fig. 5 Decryption process in eWEP

Now sign and the Encrypted message is handle separately. Here sign is decrypted by the RSA with public key of sender. So this is generate digest i.e. H1.

But encrypted message is decrypted by the AES which is produce the original message m. now for checking the authentication of message again apply Hash function on it, which is generate the digest H2. if H1 and H2 is successfully compare then message is without any error .otherwise message have error . So as we encrypt and decrypt in the **eWEP** (Estlake D etal,2001)(Atul Kahate)(William Stalling)

4. Security services of eWEP

Message Authentication

In the eWEP, has been used concept of digital signature which provides the message authentication. On the receiver side we compare digest of signature and digest of the message received. If the output will same then message has been authenticated.

Data Integrity

With the using the Digital signature, it also provide the data Integrity. Data integrity is checked with digest. If digest has not been changed then message has not been changed i.e. data integrity has been provided

Access Control

As in WEP, access control in eWEP depends strongly on efficiency of data integrity service. So, every frame that isn't integre, is considered non authenticated and is rejected.

Nonrepudiation

Digital signature also provides nonrepudiation for a message. We know the sender encrypt the digest with help of private key of sender using RSA. But on receiver side this encrypted digest is decrypted by public key of sender using RSA.

Data Privacy

Digital signature can not provide the privacy, so for providing privacy to message, we are using another layer of encryption/decryption the message. Data Privacy provided by using **AES algorithm**)(Atul Kahate)(William Stalling)

5. Comparison Performance of eWEP &WEP

This section describes, the Comparison between WEP and eWEP.

	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

Conclusion

In this paper, Security holes of WEP have been reviewed. An Enhanced Version of WEP has been proposed. This proposed protocol address a digitally signed authentication mechanism to achieve authentication, uses AES to provide confidentiality and hashing to provide integrity. In the future work, Computational complexity of eWEP will be analyzed and its performance calculated.

References

Hassan, Challal(March 2005), "Enhanced WEP: An efficient solution to WEP threats

BorscM.; Shinde(25 Jan 2005)."wireless Security Privacy" Personal Wireless Communications ICPWC,IEEE International Conference.

Kaufman, C.; Perlman, R., and Speciner, M. Network Security: Private Communication in a Public World, 2ndEdition Prentice Hall.

Eastlake, D. ; Jones, P. September (2001). US Secure Hash Algorithm 1 (SHA1), RFC 3174

I. M. S. Fluhrer ; A. Shamir (Aug. 2001). Weaknesses In the key scheduling algorithm of RC4. 8th Annual Workshop on Selected Areas in Cryptography

Atul Kahate , "Cryptography and network Security ", Tata McGraw –Hill, ISBN 0- 07-049483-5

William Stallings (2004) Cryptography and Network Security Principles and Practices, Pearson Education,Page(s) 312-340