Strengthening the Encryption Mechanism in WEP Protocol

Jaspreet Singh
Department of Computer Science and Engineering
Chandigarh Engineering College, Landran (Mohali), Punjab, India

Sandeep Singh Kang
Associate Professor, Department of Computer Science and Engineering
Chandigarh Engineering College, Landran (Mohali), Punjab, India

Abstract: Wi-Fi is serving as a standard for broadband connectivity in homes, offices, and at many public locations. WEP is a security protocol for WLANs designed to give security equivalent to that provided on Wired Networks. It is a framework that uses RC4 encryption algorithm. Many flaws had been discovered in the RC4 algorithm by the experts. In the RC4 the encryption is performed by a 'bit-by-bit' 'exclusive or' operation with the secret key and if the key becomes known by unauthorized individuals, the key is compromised and data of the sender in the network can be interpreted by the hackers. In this paper we analyze some weaknesses on the RC4 stream cipher which is used by WEP Protocol and we proposes an public key encryption scheme Elliptic Curve Cryptography (ECC) in WEP which will overcomes the drawbacks of RC4 encryption Protocol and further we analyze the NAF and Block Method of Point Multiplication in ECC. The proposed ECC encryption will provide the secure encryption mechanism in the WEP Protocol.

Keywords WEP ; RC4 stream cipher; Elliptic Curve Cryptography

I. INTRODUCTION

Wired Equivalent Privacy (WEP) is a protocol for encrypting wirelessly transmitted packets on IEEE 802.11 networks [1].The WEP algorithm works on the basis of a secret key shared between a mobile device (e.g. PDA, cell phone, tablet PC) and an access point .Packets are encrypted using the key before transmission [2]. The security goal of WEP is data confidentiality equivalent to that of a wired LAN. When WEP is active in wireless LAN, packet is encrypted separately with RC4 cipher stream generated by a 64-bit RC4 key [3]. The encrypted packet is generated with a bit wise exclusive OR of the original packet and RC4 stream. The initialization vector chosen by the sender should be changed so that every packet won't be encrypted with the same cipher stream [3]. Private keys are also known as symmetrical keys. In private key encryption technology, both the sender and receiver have the same key and use it to encrypt and decrypt all messages [4].

1.1 WEP Encryption and Decr

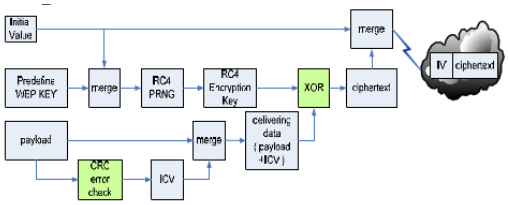

Figure 1: WEP Encryption Flowchart

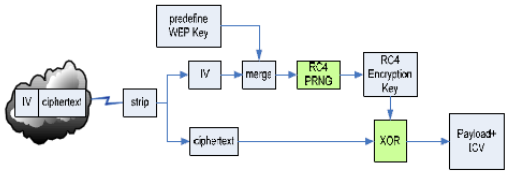

Figure 2: WEP Decryption Flowchart

Figure 1 and Figure 2 shows the WEP encryption and integrity checking mechanisms. Unfortunately, it is well-known that WEP is insecure and should not be counted on to provide any security [5]. The data frame is check summed (using the CRC-32) to obtain c(M), where M is the message. M and c(M) are concatenated to get the plain text P=(M, c(M)). RC4 key stream is generated by a function of the initialization vector IV and the secret key =RC4 (IV, K). The cipher text results from applying the XOR function to the plain text and the key stream. That is (M, c (M)) XOR RC4 (v, K) [7]. The receiver uses IV and WEP Key to generate the key stream. We use XOR key stream with cipher text to recover the plaintext P1. The P1 is then split into two parts as message M1 and check sum C1. c(M1) is then computed and compared with C1, if matches we receive it ,or refuse [7].

II. The Working of RC4 Encryption Algorithm

WEP algorithm implements RC4 encryption algorithm, but RC4 encryption algorithm has some weaknesses. So hackers can crack WEP key by using these weaknesses [7]. RC4 is a stream cipher, symmetric key algorithm. The same algorithm is used for both encryption and decryption as the data stream is simply XORed with the generated key sequence [4]

The algorithm can be broken into two stages: initialization, and operation. In the initialization stage the 256-bit state table, S is populated, using the key, K as a seed. Once the state table is setup, it continues to be modified in a regular pattern as data is encrypted. The initialization process can be summarized by the pseudo-code

The S-box is initialized using the key K as follows

```
j = 0;
for i = 0 to 255:
S[i] = i;
for i = 0 to 255:
j = (j + S[i] + K[i]) mod 256;
swap S[i] and S[j]
```

Once the initialization process is completed, the operation process may be summarized as shown by the pseudo code below:

Each next byte b of the key stream is produced using

```
i = j = 0;
for (k = 0 to N-1)
{
i = (i + 1) mod 256;
j = (j + S[i]) mod 256;
swap S[i] and S[j];
pr = S[ (S[i] + S[j]) mod 256]
output M[k] XOR pr
}
```

where [0..N-1] is the input message consisting of N bits [4]. Once the S-box is initialized with the key, the RC4 algorithm is a loop that updates the internal state of the S-box and returns a byte of keystream [7].

2.1 RC4 Steps

The steps for RC4 encryption algorithm is as follows:

1- Get the data to be encrypted and the selected key.
2- Create two string arrays.
3- Initiate one array with numbers from 0 to 255.
4- Fill the other array with the selected key.
5- Randomize the first array depending on the array of the key.

6- Randomize the first array within itself to generate the final key stream.
7- XOR the final key stream with the data to be encrypted to give cipher text. [4]

2.2 Drawbacks of RC4 Algorithm

The drawbacks of RC4 are as follow:

1. The key must remain secret and exchanging keys with someone must be done in secret.
2. Weak Keys: these are keys identified by cryptanalysis that is able to find circumstances under which one or more generated bytes are strongly correlated with small subset of the key bytes [1].
3. The RC4 algorithm is vulnerable to analytic attacks of the state table [1].

III. ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

Elliptic Curve Cryptography (ECC) is a public key cryptography. Elliptic curve cryptography was introduced by Victor Miller. The popularity of elliptic curve cryptography is due to the determination that is based on a harder mathematical problem than other cryptosystems [10]. In public key cryptography each user or the device taking part in the communication generally have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operation [8]. Only the particular user knows the private key whereas the public key is distributed to all users taking part in the communication.

3.1 Elliptic Curve in ECC

Elliptic curves are not ellipses. They are so named because of the fact that ellipses are formed by quadratic curves. Elliptic curves are always cubic and have a relationship to elliptic integrals in mathematics where the elliptic integral can be used to determine the arc length of an ellipse. An elliptic curve in its standard form is described by $y2 = x3 + ax + b$. For the polynomial, $x3 + ax + b$, the discriminant can be given as $D = - (4a3 + 27b2)$. This discriminant must not become zero for an elliptic curve polynomial $x3 + ax + b$ to possess three distinct roots. If the discriminant is zero, that would imply that two or more roots have coalesced, giving the curves in singular form. It is not safe to use singular curves for cryptography as they are easy to crack. Due to this reason we generally take non-singular curves for data encryption [9].

Each value of the ‘a’ and ‘b’ gives a different elliptic curve. All points (x, y) which satisfies the above equation plus a point at infinity lies on the elliptic curve. The public key is a point in the curve and the private key is a random number. The public key is obtained by multiplying the private key with the generator point G in the curve [8].

3.2 Plaintext Encryption by ECC

Encryption is the process of transforming plaintext data into Cipher text in order to conceal its meaning and so preventing any unauthorized recipient from retrieving the original data. Hence, encryption is mainly used to ensure secrecy .The encryption process involves taking each character of data and comparing it against a Key [4].

We describe the concept of plaintext encryption by defining a two-dimensional alphabetic table. It is worth noting that in the case of elliptic curve cryptography there is no specified rule and/ or algorithm to specify the letters of the English alphabet as well as special symbols. For this , a 6x5 table (Table 1) has been formed here for both the upper case and lower case letters of the English alphabet along with some of the other symbols like , , . , ? and space for illustration purpose only. Other symbols of punctuation marks and special characters can also be considered in a similar way. Such tables play some important role in ECC as two-dimensional plaintext co-ordinate representation requires to add with any point on the elliptic curve. Now, for any plaintext to be encrypted we add or multiply coordinates of a given character with selected points on the elliptic curve . For this purpose we consider the respective co-ordinates of the respective character. All the coordinate points should be on the surface of the elliptic curve [9].

We illustrate the process with the following examples:

	0	1	2	3	4
0	A a	B b	C c	D d	E e
1	F f	G g	H h	I i	J j
2	K k	L l	M m	N n	O o
3	P p	Q q	R r	S s	T t
4	U u	V v	W w	X x	Y y
5	Z z	,	.	?	

Table 1. Two-dimensional alphabetical table.

For the encryption plain text 'Boy', the two dimensional co-ordinate representations is

{P1, P2, P3}={(0,1),(2,4),(4,4)}

3.3 ECC Importance

As ECC is an Asymmetric encryption algorithm. So Asymmetric algorithm solve the problems by replacing single shared secret key with a pair of mathematically related keys: one public key that can be made publicly available and one secret private key [3]. They require only that the communication entities exchange keying material that is authentic (but not secret). Each entity selects a single key pair (e,d) consisting of public key e and private key d property that it is computationally infeasible to determine the private Key solely from knowledge of the public key [6].

The security due to ECC relies on the difficulty of Elliptic Curve Discrete Logarithm Problem. Let P and Q be two points on an elliptic curve such that kP = Q, where k is a scalar. Given P and Q, it is computationally infeasible to obtain k. If k is sufficiently large, k is the discrete logarithm of Q to the base P. Hence the main operation involved in ECC is related to the Point Multiplication i.e. multiplication of a scalar k with any point P on the curve to obtain another point Q on the curve [8][9].

3.4 Point Multiplication

In point multiplication a point P on the elliptic curve is multiplied with a scalar k using elliptic curve equation to obtain another point Q on the same elliptic curve i.e. KP=Q [10]

Point multiplication is achieved by two basic elliptic curve operations:

Point addition, adding two points J and K to obtain another point L i.e., L = J + K.
Point doubling, adding a point J to itself to obtain another point L i.e. L = 2J [10].

Point multiplication can be performed in ECC by using efficient methods for such as NAF.

3.5 NAF Method

As in the NAF No two consecutive digit are nonzero or non-zero values cannot be adjacent.

NAF method includes two parts for performing Point multiplication operations:

First is calculation of NAF for given input .
Second is computation of Point multiplication operation using NAF obtained.

Overall computation for Point Multiplication operation with NAF method can be made more effective by improving speed of calculating the NAF Part [10].

3.6 Block method of computing NAF

Block method improves the speed for computing NAF over the standard NAF Method. In Block method the procedure for converting the scalar k into signed binary representation is as follows [10]:

a) The first step is to partition the input into blocks of binary of equal size.

b) If there is an odd block at the end, sufficient padding bit will be appended to the left of this block to make all blocks equal in size.

c) Then get the index for each block of binary to extract the NAF value for each block from look up table

d) Perform the combine part for the blocks to get Final result in NAF [10].

IV. CONCLUSION

Now as the ECC is the Public key Encryption mechanism so it will solve problem which persist with the RC4 which is based on the symmetric key encryption . As the Problem with secret keys is that exchanging them over the Internet or a large network while preventing them from falling into the wrong hands. In the Asymmetric encryption, in which there are key pair of one is private key and one is public key .So it is infeasible for the hacker to get the key because if the hacker attacks the private key it is infeasible to get the cipher text until the hacker should have the pair of keys. So the Implementation of ECC technique in WEP makes it a more secure Protocol.

REFERENCES

[1] Lazar Stosic , Milena Bogdanovic ," RC4 stream cipher and possible attacks on WEP, (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 3, No. 3, 2012.

[2] Rajni Pamnani, Pramila Chawan , "Building a secured wireless LAN", International Journal of Recent Trends in Engineering, Vol 2, No. 4, November 2009.

[3] C. SAJEEV and G. JAI ARUL JOSE , "Elliptic Curve Cryptography Enabled Security for Wireless Communication , International Journal on Computer Science and Engineering Vol. 02, No. 06, 2010.

[4] Allam Mousa and Ahmad Hamad ,"Evaluation of the RC4 Algorithm for Data Encryption", International journal of computer and Application ,Vol 3, No 2 , June 2006.

[5] Jin-Cherng Lin, Yu-Hsin Kao, Chen-Wei Yang," Secure Enhanced Wireless Transfer Protocol" IEEE 2006.

[6] Marisa W. Paryasto, Kuspriyanto, Sarwono Sutikno and Arif Sasongko , "Issues in Elliptic Curve Cryptography Implementation", Internetworking Indonesia Journal , Vol 1 / No 1 2009.

[7] Peisong Ye and Guangxue Yue , "Security Research on WEP of WLAN" , Proceedings of the Second International Symposium on Networking and Network Security (ISNNS '10) Jinggangshan, P. R. China, 2-4, April. 2010.

[8] Elliptic Curve Cryptography – An Implementation Tutorial by Anoop MS.

[9] Tarun Narayan Shankar , G Sahoo , "Cryptography With Elliptic Curves", International Journal Of Computer Science And Applications Vol. 2, No. 1, April / May 2009.

[10] Harsandeep Brar and Rajpreet Kaur; Design and Implementation of Block Method for Computing NAF, International Journal of Computer Applications (0975 – 8887) ; Volume 20– No.1, April 2011.