A NOVEL STRATEGY TO PROVIDE SECURE CHANNEL OVER WIRELESS TO WIRE COMMUNICATION

Prof. Dr. Alaa Hussain Al- Hamami,
Amman Arab University for
Graduate Studies
Alaa_hamami@yahoo.com

Dr. Mohammad Alaa Al- Hamami
Delmon University for
Science and Technology
drmah78@yahoo.co.uk

ABSTRACT

This research aims to provide secure channel for the communication over mobile network to access the internet. This could be done by divide the security between mobile phone and WAP. Mobile phone takes the plaintext from user then compresses it by Huffman compression method. After getting the compressed text then will be encrypted by elliptic curve taking in account the limitations of mobile phone. After transmitting the encrypted compressed text to WAP, WAP will translate the wireless communication to wire and will do the following procedures: decrypt and decompress the cipher text then get the plaintext for translating to internet. If the message will be transferred from the WAP to a mobile, the following process will be taken place: recompress and re encrypt the message by using elliptic curve. Finally the cipher text will be encrypted by either blowfish or twofish to strength channel security over the internet. The encrypted message will be transmitted with image hidden in it that contains information and the key of the used encryption algorithm (twofish or blowfish).

Keywords: Mobile devices, Wireless network, Encryption, Compression, and WAP.

1 INTRODUCTION

Mobile devices and wireless network is being used widely now days, wireless networks are available in most public places, this encourage the unauthorized used for those networks and devices. Wireless Access Protocol (WAP) is the protocol that allows Internet access from wireless devices and as more subscribers demand WAP services, the need for wireless Internet security will continue to grow.

1.1- WAP Philosophy

WAP stands for Wireless Access Protocol, a general term used to describe the multi-layered protocol and related technologies that bring Internet content to mobile devices such as PDAs and cell phones [1]. Such devices are referred to as thin clients because they have one or more constraints in the form of display, input, memory, CPU, or other hardware or usability limitations. The platform constraints and the slower (and more expensive) bandwidth of cellular and related networks make standard Internet protocols difficult to utilize. Using the growing set of WAP tools and protocols, however, the mobile Internet is quite capable tool. As previously stated, WAP refers to a wide range of technologies and protocols, all related to mobile Internet functionality. Many articles focus on the delivery of Wireless Markup Language (WML) content to mobile devices over a cellular or related technology network. However, the delivery of many protocols and technologies takes the same route-namely, through a WAP proxy server that bridges the gap between the wired Internet and the wireless service provider's network as shown in Figure 1.

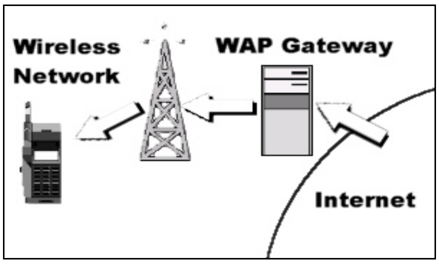


Figure (1): The WAP Gateway provides wireless networks with Internet access and optional content translation and filtering.

1.2- Steganography Philosophy [2]

Embedding information, which is to be hidden, into media requires two files. The first is the innocent-looking image that will hold the hidden information, called the cover media. The second file is the secret message that the information to be hidden as shown in Figure 2.

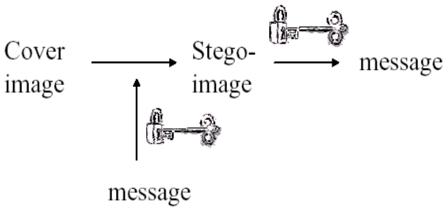


Figure 2: The Hidden Process in an Image.

A message may be plaintext, cipher text, images, or anything that can be embedded in a bit streams. The most media use is an image for hiding information. When combined, the cover media and the embedded message this will form a stego-object product. A stego-key (a type of password) may also be used in hiding process and then later may be used to decode the message.

1.3- Elliptic Curve Philosophy

It unlike earlier cryptosystem, an elliptic curve works with a finite Abelian group formed by the points on an elliptic curve defined over a finite field. The point addition operation in Elliptic Curve Cryptography (ECC) is the counterpart of modular multiplication in RSA and multiple addition of point (scalar multiplication) is the counterpart of the modular exponentiation. Menezes-Vanstone Elliptic Curve Cryptography (MVEC) is a cryptosystem that has no analogues for Discrete Logarithm Problem (DLP). Once one has a curve and a point on it, one is sure to succeed in embedding data into the system. That is not true for the elliptic curve analogues of DLP. In this system the finite field Fp, the elliptic curve E, and the “base point” B Є E (preferably, but not necessarily a generator of the curve) are public information. Bob randomly chooses secret integer d (1<d<N, where N is the number of points of E) and publishes the point dB. If Alice wants to send the message M (as any two number) to Bob, she will choose a secret random integer e (1<e<N) and sends the pair [(c1, c2), eB], where (k1, k2) = edB , (m1, m2) = M and c1 = m1*k1 mod q , c2 = m2*k2 mod q [3, 4].

Bob will then multiply the second point in the pair by d to find d(eB) ((k1, k2) = deB) and computes the inverse of each number in this point (i.e k1*k1’ = 1 mod q, and k2*k2’ = 1 mod q), and find the original message M = (m1, m2) as follows: m1 = c1*k1’ mod q, m2 = c2*k2’ mod q.

1.4- Blowfish and Twofish Philosophy [5, 6]

Blowfish, a new secret-key block cipher, is proposed. It is a ***Feistel network***, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. Although there is a complex initialization phase required before any encryption can take place, the actual encryption of data is very efficient on large microprocessors. Blowfish key expansion converts a variable-length key of at most 56 byte (448 bits) into several subkey arrays totaling 4168 bytes.

Twofish is a 128-bit block cipher that accepts a variable-length key up to 256 bits. The cipher is a 16-round Feistel network with a bijective *F* function made up of four key-dependent 8-by-8-bit S-boxes, a mixed 4-by-4 maximum distance separable matrix over GF(28), a pseudo-Hadamard transform, bitwise rotations, and a carefully designed key schedule. Twofish can be implemented in hardware in 14000 gates.

2 THE PROPOSED SYSTEM

The proposed system presents a strategy to provide secure channel over mobile communication to the internet. This strategy will be explained in detail by the following steps:

First Step: design the suitable WAP architecture for the strategy.

See Figure 3 .

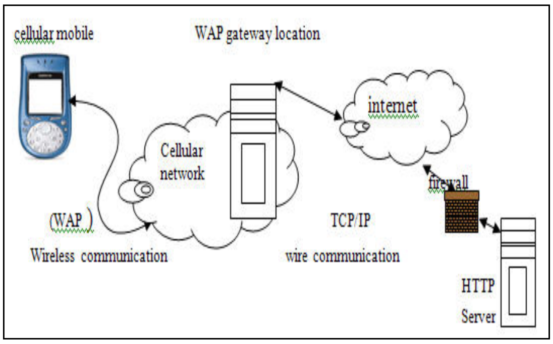


Figure 3 WAP infrastructures with specified WAP location.

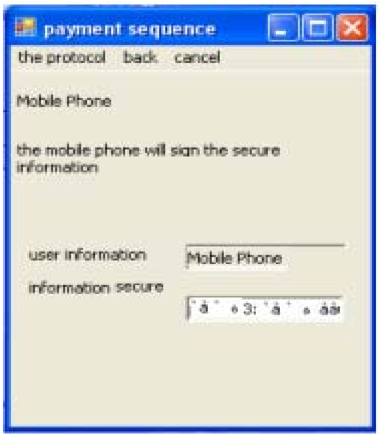
Figure 3 explains the proposed architecture. This architecture consists of mobile phone in mobile communication and WAP which will be put in the nearest point to mobile since the security with mobile communication is not strong because of the different limitations with mobile phones.

Second Step: mobile phone role.

Mobile phone will take the plaintext which represents credit card information or any other specified account information, putting them in file and then compress the file before encryption, also because of the mobile phone limitation. See Figure 4 which displays the compression process using Huffman method.

Figure 4 Huffman compressions with mobile phone.

Then take the compressed file to encrypt it by elliptic curve, see Figure 5.



Mobile Phone

the mobile phone will sign the secure information

user information: Mobile Phone

information secure: ˆâ˝ ‧3: ˆâ˝ ‧ ââ

Figure 5: elliptic curve with mobile phone.

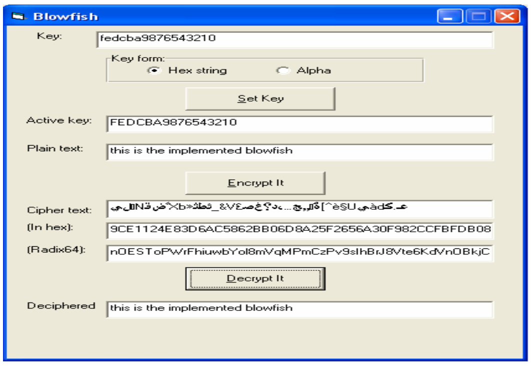
Using elliptic curve rather than RSA for the following reasons:

The principle of attractive of ECC compared to RSA is that it appears to offer equal security for a far smaller bit size, thereby reducing processing overhead. On the other hand, although the theory of ECC has been around for some time, it is only recently that products have begun to appear and that there has been sustained cryptographic interest in probing for weakness.

Finally transmit the compressed and encrypted information to WAP server.

Third Step: WAP server role.

After WAP received the encrypted and compressed information, it will decrypt and decompress the information. Then WAP converts the information from the mobile communication protocol to wire protocol and then compress the information (Huffman) and encrypt the information by using elliptic curve. Until now the security is pure over the internet so the proposed system supports the secure channel (Huffman and elliptic curve) over internet by strong encryption algorithm like blowfish or twofish. Figure 6 represents the blowfish implementation.



Key: fedcba9876543210

Key form: ● Hex string ○ Alpha

Active key: FEDCBA9876543210

Plain text: this is the implemented blowfish

Cipher text: ىلIINقضXb»ظثط_&V£عصغ؟د،...جو[^è§Uىàdكـع

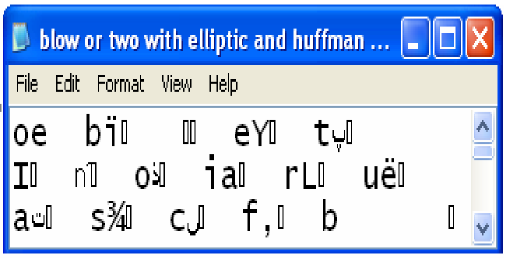
(In hex): 9CE1124E83D6AC5862BB06D8A25F2656A30F982CCFBFDB08

(Radix64): nOESToPWrFhiuwbYol8mVqMPmCzPv9slhBrJ8Vte6KdVnOBkjC

Deciphered this is the implemented blowfish

Figure 6: the complete proposed implementation of blowfish.

This means encrypting the compressed information by either twofish or blowfish. The encrypted information will be transmitted over the internet with an image (stego) which hides the type of encryption algorithm and 1000-bit. According to specific schema, it will take 448 bit for blowfish and 128 bit for twofish. This schema knows both WAP server and protected server. See Figure 7 which represents the file which contains the encryption information and the image that contains the 600 bit which represents the pool of the blowfish or twofish keys.



blow or two with elliptic and huffman ...
File Edit Format View Help

```
oe  bï    eY  tي
I  n  oي  ia  rL  uë
aيت  s¾  cل  f,  b
```

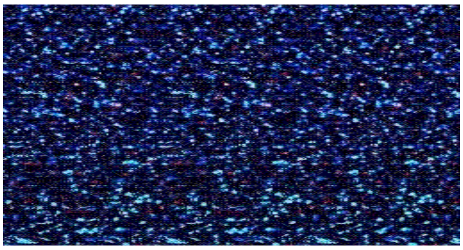


Figure 7: WAP will send the encryption file and image hiding the keys of blowfish and twofish

The specific schema of the key:

The 1000 bit will be selected randomly. For blowfish key 448:

- Divide these 1000 bit to ten 100 bit.
- First 100 bit takes from 30 to 80 bit and inverse them (50 bit).
- Second 100 bit takes from 5 to 55 and from 30 to 80 then exoring (XOR) them (50 bit).
- Third 100 bit takes first 10 bit, fourth 10 bits, sixth 10 bits, eighth 10 bit and the last 8 bit (48 bit).
- Fourth 100 bit take from 10 to 60 and from 40 to 90 anding (AND) them (50 bit)
- Fifth 100 bit takes from 20 to 70 bit and inverse them (50 bit).
- Sixth 100 bit take from 20 to 70 and from 50 to 100 then oring (OR) them (50 bit).
- Seventh 100 bit takes first 10 bit, fourth 10 bits, sixth 10 bits, eighth 10 bit and the last 10 bit. Each xored (XOR) with 0111001100 (50 bit).

- Eighth 100 bit take from 10 to 60 (50 bit)
- Ninth 100 bit take from 80 to 100 (20 bit)
- Tenth 100 bit take from 5 to 35 (30 bit)

The 1000 bit will be selected randomly. For twofish key 128:

- First 100 bit takes from 30 to 40 bit and inverse them (10 bit).
- Second 100 bit takes from 5 to 15 and from 10 to 20 then exoring (XOR) them (10 bit).
- Third 100 bit takes first 10 bit, fourth 10 bits and the last 8 bit (28 bit).
- Fourth 100 bit take from 10 to 30 and from 40 to 60 anding (AND) them (20 bit)
- Fifth 100 bit takes from 20 to 30 bit and inverse them (10 bit).
- Sixth 100 bit takes from 20 to 30 and from 25 to 35 then oring (OR) them (10 bit).
- Seventh 100 bit takes first 10 bit exoring (XOR) with eighth 10 bit (10 bit).
- Eighth 100 bit take from 72 to 82 (10 bit)
- Ninth 100 bit take from 82 to 92 (10 bit)
- Tenth 100 bit take from 34 to 44 (10 bit)

Forth Step: protected server role.

Now the protected server will receive the encryption file and image that contains the hidden information. First extract hidden information which represents type of encryption algorithm and the 1000 bit to extract the key of blowfish or twofish, then decrypt the encryption by the blow or two and decrypt the elliptic curve. Finally decompress the resulted decrypted file by using Huffman method.

3 CONCLUSIONS

- Placing a WAP gateway in the mobile communication network that due to mobile limitations which make the mobile phone unable to use what is efficient of security algorithms.
- Adding blowfish or twofish will strength the secure channel over the internet.
- Using the keys of blow and two encryptions online by creating schema for extracting them from 1000 bit. These bits which are hidden in image by using steganography will make the proposed system more immune against the attackers.

4 REFERENCES

1. Korhonen J.; **“Introduction to 3G mobile communication”**, second edition, Artech house, INC., 2003.

2. Nile F. Johnson and Suhil Jajodia, " ***Steganalysis of Images Created Using Current Steganographic Software*** ", in Proceeding of Information Hiding - Second International Workshop, Springer - Verlage, April 1998.

3. **“Standard for efficient cryptography; SEC1: elliptic curve cryptography”**, certicom crop, secg-talk@lists.certicom.com, 2000.

4. Murari A.; **“Software implementation of EEC”**, Oregon state university, 2003.

5. Schneier B., and Kelsey J.; **“Unbalanced fiestel network and block-cipher design”**, {Schneier,Kelsey}@counterpane.com , 2000.

6. Schneier B.; **“The blowfish encryption algorithm”**, counterpane-internet-security, Inc., 2000.