A Secure Model For Bluetooth Banking

Somayeh Izadi[1], Kamran Morovati[2], Saeed Zahedi[3], Reza Ebrahimi Atani[4]

[1] Department of Information Technology, University of Guilan, Rasht,
[2] Department of Computer Science, University of Pune, PhD candidate in security, Pune, India,
[3] Department of Information Technology, University of Guilan, Rasht,
[4] Department of Computer Engineering, University of Guilan, Rasht,

Abstract:

Nowadays, customers' needs are more or less centered on three main axes: to remove the time and location limitations and reduce costs. This is considered an organizational value and is seen in the perspectives and institutional missions of financial organizations. In this paper, a model of secure electronic payment based on Bluetooth mobile infrastructure with biometric authentication system is presented.

Keywords: Mobile Banking; e-payment; Bluetooth; fingerprint; minutia; Rabbit ;Hash

1. Introduction

Considering the financial policies of countries and even global policy based on human life being electronic, especially in financial matters, such as elimination of physical money, and replacement of credit cards and ..., make us pay more attention to the importance of time. The Bank which is a driving force of each country's economy should be able to help in co-operations and interactions with the simplest and most accessible equipments .Item Read phonetically Dictionary Customer investment security would be most important matter. These days the banks offer services such as paying and receiving the bills or account management.There are many papers in this area, but not as much as electronic banking, because still it is a new technology and needs more study. In the first section of this article we explain the stages in production of key, in the second section we will talk about text encryption and access to the encrypted text. In the third part we explain server database and identification of the main message of the text and finally in the fourth section outline the analysis of security models.

2. Key Generation

At first, according Figure 1, key will generate.

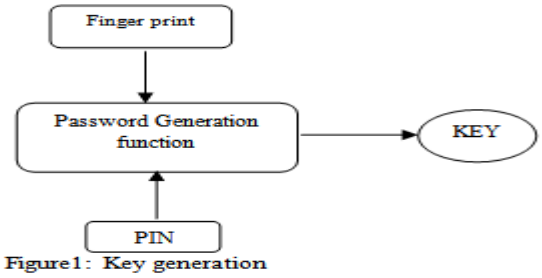

Figure1: Key generation

3. Finger print

A fingerprint is the feature pattern of one finger. It is believed with strong evidences that each fingerprint is unique. Two representation forms for fingerprints separate the two approaches for fingerprint recognition. The first approach, which is minutia-based, represents the fingerprint by its local features, like terminations and bifurcations. This approach has been intensively studied, also is the backbone of the current available fingerprint recognition products. We also concentrate on this approach in this paper.

The image segmentation task is fulfilled by a three-step approach:
1- Block direction estimation,
2- Segmentation by direction intensity
3-Region of Interest extraction by Morphological operations.

Dividing the image into small processing blocks (32 by 32 pixels) and performs the Fourier transform according to:

$$f(u,v) = \sum_{x=0}^{M-1}\sum_{y=0}^{N-1} \mathrm{f(x,y)} * \exp\left(-\mathrm{j}2\pi * \left(\frac{\mathrm{ux}}{\mathrm{M}} + \frac{\mathrm{vy}}{\mathrm{N}}\right)\right) \quad (1)$$

For u=0, 1, 2… 31 AND V=0, 1, 2… 31

In order to enhance a specific block by its dominant frequencies, we multiply the FFT of the block by its magnitude a set of times. Where the magnitude of the original FFT=abs

$$(f(u,v) = |f(u,v)|) \quad (2)$$

Get the enhanced block according to

$$G(x,y)=f^{-1}\{f(u,x) * |f(u,x)|^{x}\} \quad (3)$$

Where F-1(F (u,v)) is done by:

$$f(x,y) = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1} \mathrm{f(u,v)} * \exp\left(\mathrm{j}2\pi * \left(\frac{\mathrm{ux}}{\mathrm{M}} + \frac{\mathrm{vy}}{\mathrm{N}}\right)\right) \quad (4)$$

For x=0, 1, 2… 31 AND y=0, 1, 2… 31

The k in formula (2) is an experimentally determined constant, which we choose k=0.45 to calculate. While having a higher "k" improves the appearance of the ridges, filling up small holes in ridges, having too high a "k" can result in false joining of ridges. Thus a termination might become a bifurcation.

4. Author Function Hash:

Function is a function that creates a fixed length output for arbitrary input, in a way that it is impossible to find two different inputs with the same output. For the message M with the result of the HASH function is shown by H (M). In Table 1 new HASH algorithms are compared. Comparison of speed has been implemented on a 266 MHz Pentium system under C + + language.

Table1: Comparison Table for RIPEMD-160, SHA-1, MD5

	RIPEMD-160	SHA-1	MD5
Digest size	160 bit	160 bit	128 bit
Main processor unit	512 bit	512 bit	512 bit
N# steps	160(5steps 16pieces)	80(4steps 20pieces)	64(4steps 6pieces)
Message length	2 64 -1 bit	2 64 -1 bit	∞
Basic logic function	5	4	4
Additional constants used	9	4	64
Speed(Mbps)	13.6	14.4	32.4
Endianness	Little-endian	Big-endian	Little-endian

In this plan according to the comparison table and the user needs and equipment, we choose the MD5 algorithm. In this algorithm, K-bit message to the L segment is divided into 512-bit. If the end segment is not 512 bits, for completion of 512 bits, other bits are left zero. The first segment (Y_0) is coded by 128-bit vector IV and MD5 algorithm, and 128-bit Review (CV_1) is obtained and the operation would continue until eventually a Review of 128-bit is achieved.

Results of the MD5 algorithm are performed between fingerprint and PIN. Key is generated. Since the fingerprint and PIN information is provided to the destination database, meaning the bank; therefore, the production of the key in the bank is done similarly.

5. Producing And Sending The Encrypted Text

Figure 2 shows the steps and overview of the encrypted text creation. It should be mentioned that at this time the text message is hashed. The reason is to ensure message authenticity.

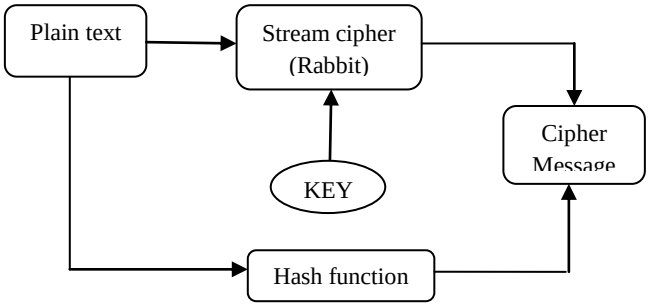

Figure2: cipher text generation

Rabbit is a synchronous stream cipher that was first presented at the Fast Software Encryption Since then, an IV-setup function has been designed, and additional security analysis has been completed.

No cryptographically weaknesses have been revealed until now. The Rabbit algorithm can briery be described as follows. It takes a 128- bit secret key and a 64-bit IV (if desired) as input and generates for each iteration an output block of 128 pseudo-random bits from a combination of the internal state bits. Encryption/decryption is done by XOR'ing the pseudo-random data with the plaintext/cipher text. The size of the internal state is 513 bits divided between eight 32-bit state variables, eight 32-bit counters and one counter carry bit. The eight state variables are updated by eight coupled non-linear functions. The counters ensure a lower bound on the period length for the state variables.

Rabbit was designed to be faster than commonly used ciphers and to justify a key size of 128 bits for encrypting up to 264 blocks of plaintext.

This means that for an attacker who does not know the key, it should not be possible to distinguish up to 264 blocks of cipher output from the output of a truly random generator, using less steps than would be required for an exhaustive key search over 2128 keys.

At this point the message (user`s raw text) by the function Hash, becomes encrypted the text and encrypted text messages followed by Rabbit stream cipher function has been done, sits ready to be sent. Bluetooth platform is selected. Bluetooth connects through radio frequencies. This frequency is selected because it is accessible free of charge worldwide and a permit is not required. This frequency band according to an international agreement is used only by scientific equipment, medicine and industry and is called ISM. Theoretically, Bluetooth bandwidth is one megabyte per second, which is close to 723 kbps.

1. Reasons for choosing this platform:
2. Restrictions on data transfer (Data) through wires
3. Low cost of Bluetooth Technology
4. Bluetooth data transfer speed
5. Bluetooth technology superiority versus infrared
6. No Bluetooth interference with other waves
7. Being automatic
8. Using less energy
9. Increasing the security by limiting the bank space for customers.

6. Review by the Bank

Encrypted messages are sent to the bank via Bluetooth. Every person’s bank already has the customer fingerprint. The associated PIN is also available to the bank. Therefore generating keys for the bank is easily possible. This is possible only if none of the components involved in the production of key gives it to secondary person.

Bank receives the encrypted text. The attached Hash function separated and then with the key as well as the current password algorithm Rabbit, decodes the received text message in order to access the main message of the client.

Figure 3 shows the Schema of what happens in the bank.

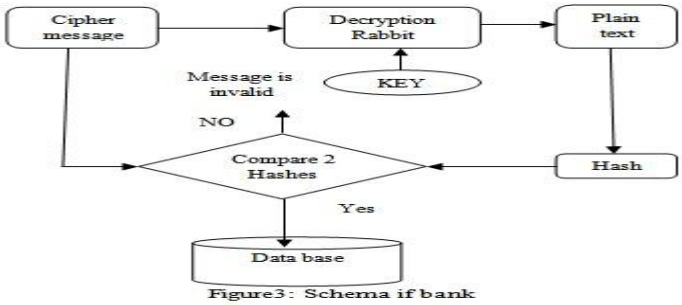

Figure3: Schema if bank

Although bank has applied unique security principles in the model, once again the text content of text message authenticity is checked. To do this, the text that has been achieved through decryption is Hashed again compares it with the Hash that was separated from the original message. This comparison assures the bank of the accuracy of the text considering the features of the function Hash. If the comparison of the two Hashes is positive and they correspond, the text message is stored in the server database. Figure 4 shows the full plan of the proposed model.

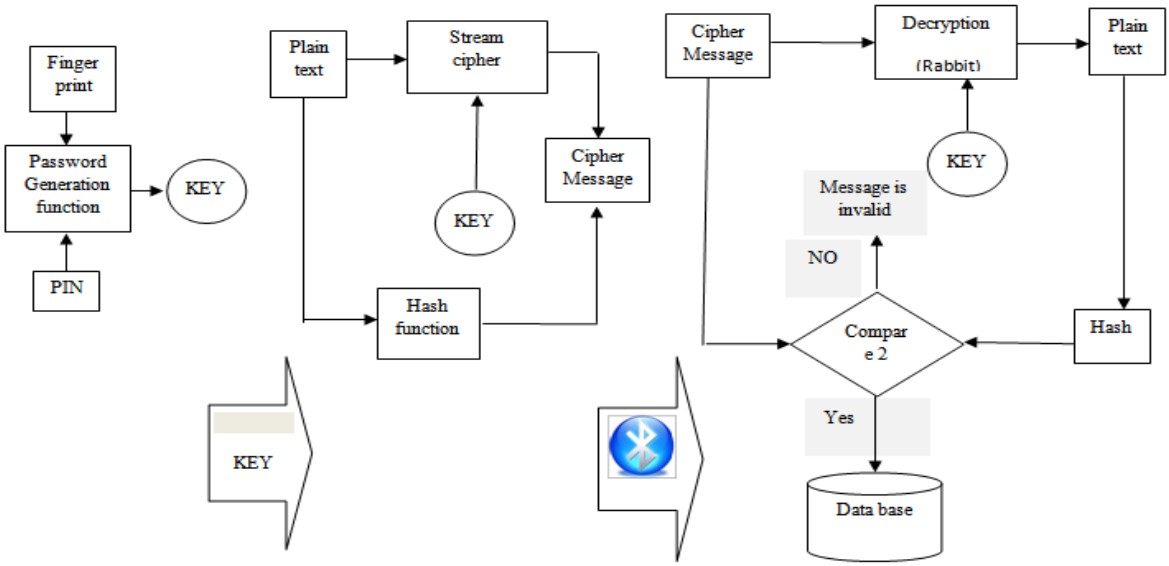

Figure4: schema of proposal model

7. Main Analysis of The Security In The Proposed Model

Integrity: The proposed model uses the Hash algorithms for creating abstract message about the message exchange. Review message is calculated by both the client and the server database.

Confidentiality: In Our proposal model Confidentiality get with fingerprint. As our assumption only the user and bank-server know the parameters for generation key. The level of security of the designed protocol depends on the strength of the encryption algorithm used.

Authentication: Unique identity of the fingerprint and PIN number to which only the bank and the customer have access, cause the customer not to be able to deny sending the message. Even if the phone or SIM card is stolen from clients, the thief or invader won't have access to the fingerprint and PIN of the customers.

Availability
The availability of our proposed model depends on three factors:

- ✓ Availability of the mobile phone: although Message decryption and calculating message digest can cost much of processing power but all selected algorithms for hash and encryption/decryption are light. Thus need to minimum resource for operation.

- ✓ Availability of the cellular network provider: If the cellular network is congested, the time to deliver the secured SMS message will be time-consuming.

- ✓ Availability of the bank server: Our proposed model guarantees minimum workloads of the server by discarding any message that causes the security verifications to return failed. This can decrease the workloads on the server side when the attacker tries to congest server with random messages. . On the other hand availability of the banks service depends on the number of transactions that the server can handle at once. Number of transaction depends on the hardware capability. If the server hardware can handle multiple incoming messages then the server can perform multiprocessing to accommodate for more requests.

Non-repudiation:
Unique identity of figure print and PIN is providing with customers and bank server.

8. Conclusion

The main goal of this paper is to present a security solution based on equipments and with regard to minimum fees to send bank messages. This model has tried to use the best algorithms and security templates for banking transactions according to the limitations of the phone. On the other hand, in this model there is no message size limit or common disorders and of course is very low cost and simple.

References

[1] J. Li-Chang Lo, J. Bishop, J.H.P. Eloff. SMSSec: An end-to-end protocol for secure SMS, Computers & Security, Vol. 27, 154 - 167, 2008.
[2] J. Golic. Cryptanalysis of Alleged A5 Stream Cipher Advances in Cryptography - EUROCRYPT 97, LNCS 1233, pp. 239-255, 1997.
[3] C. Berbain, O. Billet, A. Canteaut, N. Courtios, H. Gilbert, L. Goubin, A. Gouget, L. Granboulan, C. Lauradoux, M. Minier, T. Ptonin and H. Sibert, SOSEMANUK, a fast software-oriented stream cipher, eSTREAM,2005, eSTREAM project website.
[4] D. J. Bernstein. What output size resists collisions, in a XOR of independent expansions? ECRYPT Workshop on Hash Functions, 2007. See also http://cr.yp.to/rumba20.html.
[5] M. Boesgaard, M. Vesterager, T. Pedersen, J. Christiansen, O. Scavenius. Rabbit: A new highperformance stream cipher, Fast Software Encryption, Vol. 2887, Lecture Notes in Computer Science, pages 307-329. Springer, 2003.
[6] W. WUZHILI. Fingerprint Recognition, Bachelor of Science (Honors) in Computer Science, Hong Kong Baptist University, April 2002.
[7] M. Boesgaard, M. Vesterager, T. Christensen, and E. Zenner, The stream cipher Rabbit, eSTREAM, 2005, eSTREAM project website
[8] H. Wu, The Stream Cipher HC-128, eSTREAM, 2005, eSTREAM project website.
[9] D.Maio and D. Maltoni. Direct gray-scale minutiae detection in fingerprints. IEEE Trans. Pattern Anal. And Machine Intell., 19(1):27-40, 1997
[10] A. Farina, Z. M.Kovacs-Vajna, A . leone, Fingerprint minutiae extraction from skeletonized binary images, Pattern Recognition, Vol.32, No.4, pp877-889, 1999
[11] D. J. Bernstein. ChaCha, A variant of Salsa 20. See http://cr.yp.to/chacha.html.