International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

A Secure Protocol for SMS Mobile Banking

Amol B. Jawanjal[1], R. B. Joshi[2]

[1]Department of Computer Engineering, MMCOE Pune
Savaitribai Phule Pune University Pune India

[2]Department of Computer Engineering, MMCOE Pune
Savaitribai Phule Pune University Pune India

Abstract: ***Short Message Service (SMS) is most popular, cheapest and easy-to-use communication technology for mobile phone users. Using SMS, mobile user sends some confidential information such as password, account number, banking information in the form of plaintext from one mobile to another mobile. The hacker can easily read this information and privacy will not be maintained. Nowadays due to lack of security in SMS it is rarely used in many value added services such as mobile banking and e-commerce. For this purpose we provide a solution that provides end to end security to the message with authentication, confidentiality, integrity. Hence we present a secure model for SMS mobile banking services tailored to suit mobile cellular phone users.***

Keywords: Authentication, SMS, Mobile banking, Security

1. Introduction

Short message service (SMS) has become a very strong communication medium of transferring the information world-wide. On December 3, 2014, SMS service has completed its 22 years as on December 3, 1992, the world's first SMS was sent by Neil Papworth from the UK through the Vodafone network. The popularity of SMS is increasing day by day as it is being used in many data centric applications including railways enquiry, news alert, mobile banking, and health care applications. User sends confidential information using SMS. SMS channel is not secure to transfer confidential information SMS are send from base station to mobile station in encrypted format then the message store in SMS center .The SMS center check the recipient in home location register(HLR) or visitor location register(VLR) and message to specific recipient. The message stores in SMS center that message are read by network operator hence privacy will not be maintain.

Mobile banking system is one which provides all daily banking operations to customer with one click of his mobile handset with supported application. M-banking system has potential to provide access or delivery of very specific and highly necessary information to customer. Growth in the M-Banking is driven by various facilities like convenience of banking operations, greater reach to consumers and Integration of other m-commerce services with mobile banking. In M-banking there is no place restriction, it is highly penetration coefficient as growth of mobile phones are more than computers, it is fully personalized and private increasing transaction authenticity and is available all time to the user. The contents of SMS are stored in SMS center and it is visible to the network provider Staff it can modify he contain of the message and therefore, SMS is not an appropriate communication medium for secure communications. Most users do not realize how easy to hack the SMS message. A hacker can easily hack the SMS center and read the message contain.

SMS security has at least four security constraints to meet, as listed below

In confidentiality it prevents the unauthorized user to assess the private information. The encryption techniques are used to provide confidentiality to the message.

In integrity it is preventing anybody other that authorized par-ties from modifying the computer system assets like writing, changing status and deleting and creating files. The methods of attacking integrity we found replay, reordering and modification of messages.

In non-repudiation it provides security service that prevent participant from denial of message transmission service. The message can send by sender to the receiver. The receiver can prove the message coming from authorized sender. The most common technique used in non-repudiation is digital signature method.

In authentication it gives assurance to the communication party that it claims to be. For authentication purpose both communication party knows the common factor that authenticate the user.

2. Literature Survey

Various author suggesting various technique to provide end to end security to the SMS .the author provide framework and protocol that provide security to the SMS .The Survey is base on which technique is used to provide security to the SMS.

Neetesh Saxena, Narendra S. Chaudhary [1] it proposes a protocol that improves the authentication technique. In this it provide a technique that authenticate the user and provide end to end security .this protocol prevent various attack like Man-in middle, SMS Spoofing, Replay attack, SMS disclosure. Geovandro C.C.Pereira [2] in this paper it proposed a framework for secure SMS transmission. SMSCrypto encloses a tailored selection of lightweight cryptographic algorithms and protocols, providing encryption, authentication and signature services. For confidential purpose it used public key cryptography and for authentication purpose it use block cipher based Message

Licensed Under Creative Commons Attribution CC BY

Authentication Code (MAC) for generating a message and key-dependent tag appended to each SMS message Lokesh Giripunje[3] In this paper it proposed a framework for providing end-to-end security for transmission of SMS . In this framework it used existing GSM encryption algorithm A8 for maintaining confidentiality Mohsen Toorani, Ali Asghar Beheshti Shirazi[4]The main contribution of this paper is to introduce a new secure application layer protocol, called SSMS, to efficiently embed the desired security attributes in the SMS messages to be used as a secure bearer in the m-payment systems. SSMS efficiently embeds the confidentiality, integrity, authentication, and non repudiation in the SMS messages Johnny Li-Chang Lo [5] in this paper it proposed a protocol SMSSec that can be used to secure a SMS communication sent by Java's Wireless Messaging API. SMSSec has a two-phase protocol with the 1st handshake using asymmetric cryptography which occurs only once, and a more efficient symmetric nth handshake which is used more dominantly protocols is the ability to perform the secure transmission with limited size messages Hao Zhao, Sead Muftic [6] implemented a new secure mobile wallet application using J2ME for convenience and security of financial mobile transactions performed by the subscribers. AES and DES are used as an encryption methods and SHA-1, 2 are used to generate hashes/keys for authentication purpose. Separate authentication module, i.e., PIV is implemented as a separate java card applet to provide authentication service to all subscribers Harb [7] has used symmetric and asymmetric cryptography to develop secure mobile payment application model. It is suitable for online payment/ transactions; provides security with minimum cryptography keys and less encryption operations. SMS is used as a transport channel in order to send transactions to payer. 3DES session key is used to secure SMS communication b/w customer and bank. J2ME application generates encrypted SMS having payer's confirmation and sends it to payer's bank. Payers bank will decrypt SMS and send payee's mobile number to PG. Hassan Mathkour [8] proposed a new system, i.e., Secret Short Message Service (SSMS) to secure SMS messages transmission on mobile network. Their system can also protect the private data saved on mobile phone. AESRijndeal is used to perform encryption. Secret key is embedded in cipher text using hash. It is used to encrypt SMS message. Message decryption also uses the same secret key. Encrypted secret key is used for encryption and decryption. Bouncy-Castle J2ME cryptographic library is used for encryption with SHA-1 Neetesh Saxena [9] proposed a new approach to provide SMS security using encryption and digital signatures. Firstly, message is encrypted then digital signature is applied on the encrypted message. DES, AES, DSA, and RSA are used respectively in order to encrypt SMS message. Signature generation uses hash function to get message digest. DSA signature method is used to verify signatures. DES, Triple-DES, AES and Blowfish algorithms are implemented and AES is found to take less encryption/decryption time. Marko Hassinen [10] has used RSA algorithm to encrypt SMS messages used in mobile commerce, whereas keys are generated using SHA-1. Private keys are restricted to mobile devices. Authentication Server will then generate certificates for public keys. Lightweight Directory Access Protocol (LDAP) database is used to store/retrieve those certificates. These certificates are further used by mobile user to exchange encrypted SMS messages David Lisonk [11] proposed an application to encrypt SMS messages using asymmetric RSA cipher. OAEP padding scheme is used to avoid RSA from dictionary attacks. Private keys are stored in the application, whereas public keys are stored in mobile memory. Symbian OS is used as a programming environment since it requires less computational power. Key generation operation is tested on Nokia N80 by subtracting the actual start time of key generation from its final time. Analysis of several attacks on application is also conducted at the end. Alfredo De Santis [12] proposed a secure extensible and efficient SMS (SEESMS) application framework which allows two mobile peers to exchange encrypted SMS message in an efficient manner by selecting their level of security. ECIES and RSA are used for encryption. RSA, DSA, and ECDSA signatures are also used to validate contacts. After being registered with SEESMS on mobile, keys are exchanged b/w users to transmit secure SMS using HMAC. Users will then select energy efficient cryptosystem, encrypt SMS using it, and send to the receiver. Comparison of RSA, DSA, and ECDSA is conducted on the basis of energy efficiency on N95 mobile.

3. Proposed System

In proposed solution we provide a framework for secure end to end mobile banking. For this purpose we used symmetric encryption algorithm for encryption purpose we used MAES encryption algorithm. To make mobile banking first mobile user registers their mobile number to the respected bank. Bank verifies the detail of customer and to save the mobile number in the bank database and gives secure key to the customer in the format of SMS or in the letter or mail secure key to the respected customer email id. These secure key is stored in encrypted format in the database Customer detail save in database are used to generate one time password (OTP). Bank provide mobile application that is install in mobile handset for secure mobile banking that encrypt and decrypt the message and provide end to end security of message . The Secure message contain mobile id, MAC, encrypted message and transaction time .the client send its mobile id, MAC1 will be form using message and MPIN, and message will be encrypted using encryption algorithm and transaction time is the at the time request will be generated these all contain are send to the bank server.

Server decrypt the message and calculate MAC1' and check

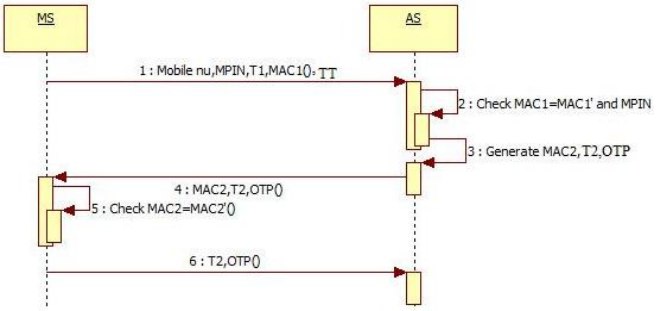

Figure 1: Communication between mobile station and bank server

MAC1'=MAC1 if it is correct then it check the MPIN if it is matches with the stored MPIN then it generate one time

Licensed Under Creative Commons Attribution CC BY

password(OTP) from the stored information of the customer. These OTP are stored into the database .the server send MAC2, OTP, and transaction time all these contain are send to the client. Client calculate MAC2' and check MAC2'=MAC2 if it is found correct then it send back replay with OTP and transaction time to the server. Server check the OTP with stored OTP if it is found correct then authentication of client is successful.

Encryption Algorithm: MAES

AES with 128-bit key has proved to be an efficient algorithm to encrypt the SMS but, its security cannot be remain maintained in the subsequent years. Various researchers have found attacks on AES with 128-bit key with some assumptions. Thus, we propose a variant of AES called MAES (modified AES) which is more secure with 256-bit key (as original AES) and 256-bit each block of data. The increase in length of each block improves the performance of MAES than the original AES. Various steps of the MAES algorithm are as follows:

1) Initial Round: AddRoundKeyeach byte of the state is combined with the round key using bitwise XOR.
2) Rounds:
   (i) SubBytes- a non-linear substitution step where each byte is replaced with another according to a lookup table.
   (ii) Shift Rows- a transposition step where each row of the state is shifted cyclically a certain number of steps.
   (iii) MixColumns- a mixing operation which operates on the columns of the state
   (iv) AddRoundKey.
3) Final Round (no MixColumns)
   (i) SubBytes
   (ii) ShiftRows
   (iii) AddRoundKey

On considering the best assembly code combinations and continuance memory usage, the order of SubByte and ShiftRow processes are swapped, to reduce the number of times in memory reads and writes, as well as increase the computation speed without compromising the actual result and this is done with MAES algorithm. Next, in AES, the MixColumns step is defined as a multiplication of columns with the matrix M. The matrix M used in the AES and its inverse matrix M, both are different and the calculation of inverse of a matrix increases the computation. Thus, we used an alternative matrix M1 because for new matrix, M1 = M inverse.

The performance of AES and MAES algorithms with one SMS size of plaintext and ciphertext pairs in bits and characters, where MAES generates 158 characters after ciphering the SMS of160 characters. Finally, we conclude that out of these algorithms, the MAES algorithm is more efficient to encrypt the SMS.

There are four main security constraints that can be maintained by any framework or protocol. The four constraints are confidentiality, integrity, non-repudiation, and authentication. The proposed solution will be maintain all the four security constraint confidentiality of the SMS will be maintain using symmetric encryption algorithm and integrity will be maintain using hash algorithm i.e. MAC that can check hash function and will be maintain integrity of the message. Non-repudiation will be maintain using one time password and Authentication will be done using various authentication pattern like mobile number, Secret key and one time password.

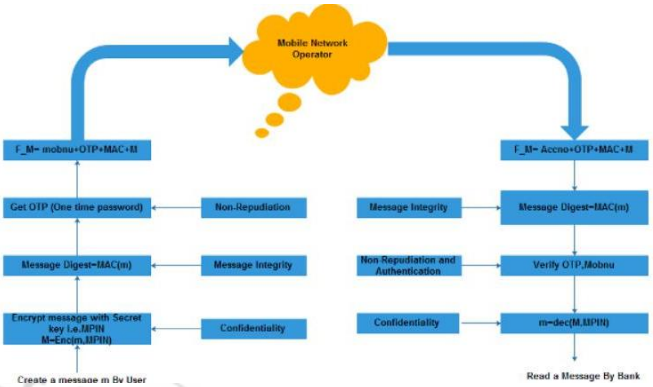

Figure 2: Security Service

4. Mathematical Model

A. Check Balance

Let

Esk = encryption with the MPIN

EAccP = encryption using session key

H = A hashing function that generates a digest on message m1

Ci = the Cipher text

Transaction Type = the number specifying the trans-action selected.

Accnu = Account identifier of the user

MPIN = user predefined personal identification number.

m1 and m2 = Plaintext Message.

Then

M1 = Esk[m1 + MPIN] M2 = H[m1 + MPIN]

M3 = Accno||Transaction Type||M1||M2

M4 = EAccP[< confirmation >]or[< Err.msg. >] in ciphertext

Where

Output M3 Send from Customer to server
Output M4 send response from bank server to customer.

B. Money Transfer

M1 = Esk[m1 + MPIN] M2 = H[m1 + MPIN]

Licensed Under Creative Commons Attribution CC BY

M3=Accno.||DestinationAccID||Transaction Type||M1|| M2
M4 = EAccP[< confirmation >]or[< Err.msg. >] in ciphertext

Where

Output M3 Send from Customer to server
Output M4 send response from bank server to customer.

5. Implementation

We have implemented proposed solution in java and android platform. At the server side we used java platform and for data storage we used oracle 11g and at the client side we developed an android application that can install in the client mobile that application run in android supported handset. An application can provide security to the SMS banking that can maintain integrity, authentication, non-repudiation and confidentiality.

6. Conclusion and Future Work

We have implemented a framework that provides secure mobile transaction using mobile banking application. All messages are sent from customer in encrypted format, bank decrypt the message and process the query and send response in encrypted format to the mobile .user decrypt this message using the banking application install in mobile. In the future work we analyze the encryption algorithm which is better than AES, we can use concept of SIM application toolkit where bank store application and encryption key on SIM.

Acknowledgment

We take this opportunity to thank Mr. Ram Joshi for their valuable guidance and for providing all the necessary facilities, which were indispensable in the completion of this paper. We are also thankful to all the staff members of the Department of Computer Engineering for their valuable time, support, comments, suggestions and persuasion. We would also like to thank the institute for providing the required facilities, Internet access and important books.

References

[1] Neetesh Saxena ,Narendra S. Chaudhary EasySMS: A Protocol For End-to-End Secure Trans-mission Of SMS IEEE Transactions On Information Forensics And Security, Vol. 9, No. 7,July 2014
[2] Geovandro C C.C.Pereira, Mateus A.S.Santos ,Bruno T. De Oliveira SMSCrypto: A lightweight cryptographic framework for secure SMS transmission The Journal of Systems and Software 86 (2013) 698 706.
[3] Nikhil Sakhare, Mithil Wasnik Secure System Of Short Message Service (SMS) For GSM Networks International Journal of Soft Computing and Artificial Intelligence, ISSN 2321- 404X Nov 2013.
[4] SSMS Mohsen Toorani, Ali Asghar Beheshti Shirazi A Secure SMS Messaging Protocol for the M-Payment Systems IEEE 2008.
[5] L.-C. Lo, J. Bishop, and J. H. Elo, SMSSec: an end-to-end protocol for secure SMS Computers and Security vol. 27, 2008, 154167.
[6] H. Zhao and S. Muftic, Design and implementation of a mobile trans-actions client system:Secure UICC mobile wallet, International Journal for Information Security Research, vol. 1,2011, 113-120.
[7] H. Harb, H. Farahat, and M. Ezz, SecureSMSPay: secure SMS mobile payment model, Proc.2nd International Conference on Anti-counterfeiting, Security and Identification, 2008. ASID,2008.
[8] H. Mathkour, G. Assassa, A. AlfiMuharib, and A. Jumah, A Secured Cryptographic Messaging System Proc. International Conference on Machine Learning and Computing (ICMLC), 2009
[9] N. Saxena and N. S. Chaudhari, Secure encryption with digital signature approach for Short Message Service, Proc. World Congress on Informa-tion and Communication Technologies (WICT), 2012.
[10] M. Hassinen, Java based public key infrastructure for sms messaging, Proc. 2nd International Conference on Information and Communication Technologies, 2006. ICTTA06., 2006, 88-93.
[11] D. Lisonek and M. Drahansky, Sms encryption for mobile commu-nication, Proc. International Conference on Security Technology, 2008. SECTECH08., 2008, 198-201.
[12] A. De Santis, A. Castiglione, G. Cattaneo, M.Cembalo, F. Petagna, and U. F. Petrillo,An extensible framework for efficient secure SMS,Proc. International Conference on Complex,Intelligent and Software Intensive Systems (CISIS), 2010, 843-850.
[13] F. Hao and P. Y. Ryan, Password authenticated key exchange by juggling Springer, 2011.
[14] A. K. Nanda and L. K. Awasthi, Joint Channel Coding and Cryptog-raphy for SMS, Proc.International Siberian Conference on Control and Communications (SIBCON), 2011.
[15] N. J. Croft and M. S. Olivier, Using an approximated one-time pad to secure short messaging service (SMS), Proc. Southern African Telecommunication Networks and Applications Conference. South Africa, 2005.
[16] J. Choi and H. Kim, A Novel Approach for SMS Security, International Journal of Security and Its Applications, vol. 6, 2012, 373-378
[17] S. Samanta, R. Mohandas, and A. R. Pais, Secure Short Message Peer-to-Peer Protocol, International Journal of Electronic Commerce, vol. 3, 2012.
[18] R. E. Anderson et al. Experiences with a transportation information system that uses only GPS and SMS, in Proc. IEEE ICTD, no. 4, Dec. 2010.
[19] J. Chen, L. Subramanian, and E. Brewer, SMS-based web search for low-end mobile devices, in Proc. 16th MobiCom, 2010, pp. 125135.
[20] I. Murynets and R. Jover, Crime scene investigation: SMS spam data analysis, in Proc. IMC, 2012, pp. 441452

Licensed Under Creative Commons Attribution CC BY