Cipher Sms Protocol: A Secure Sms Transmission for confidential Data

[1]Nimmya Unnikrishnan,[2]Divya K V

[1] PG Scholar, Dept of CSE, Vidya Academy of Science & Technology, Thrissur, India

[2]Divya K V, Asst. Professor, Dept of CSE, Vidya Academy of Science & Technology, Thrissur, India

ABSTRACT

Presently, mobile handheld device has successfully replaced traditional telephone to become the most popular wireless communication tool .The use of sms application is not a new topic now a days.sms are short length text documents written in a colloquial style. Sms has changed the way people communicate. Sms is very popular way of communication between mobile phones and portable device users to send and receive simple text messages. This paper deals with a sms encryption for mobile communication on android message application. The transmission of sms during mobile communication is not secure, Therfore it is desirable to secure sms by additional encryption. In this paper a Cipher-SMS protocol is successfully designed in order to provide end-to-end secure communication through SMS between mobile users by using AES and MD5 encryption. SMS is the most popular data service. Sms technology is used in security sensitive fields such as e-banking and e-government. SMS is transmitted in the form of plaintext between mobile user (MS) and the SMS center. SMS contents are stored in the systems of network operators and can be read by their personnel. Sms does not offer a secure environment for confidential data during transmission. The above requirements can be accomplished by proposing a protocol called Cipher-SMS which provides end-to-end security during the transmission of SMS over the network.

Keywords

Cryptography, Authentication Server, Symmetric Key, Short Message Service, encryption.

1. INTRODUCTION

Sms is a text message service that enables the users to send sms to other users on the global system for mobile communication (GSM) network.sms uses store and forward service similar to SMTP mail service. Instead of mail servers SMS Centers (SMSC) are used to store the SMS messages before they are forwarded to the mobile user's service provider or another SMSC. Although the network connections between the SMSC and nodes in a GSM network are usually protected by Virtual Private Network (VPN) tunnels the sms messages are stored unencrypted at the SMC. This means that employees of SMSC operators, or others who can hack into the system can view all the sms messages passing through SMSC. Many SMSCs also retain a copy of the sms message for audit billing and dispute purposes .if an attacker manages to compromise the SMSC the attacker can also read the SMS traffic. The mobile communication has experience a great acceptance among the human socities.Short Message Service (SMS) has become one of the fastest and strong communication channels to transmit the information across the Worldwide. SMS is the most popular mobile data service.Due to its wide popularity SMS technology is used in various field applications. This also include security sensitive fields such as e-banking and e-government. Messages are transmitted as plaintext between mobile user (MS) and the SMS center (SMSC), using wireless network. SMS contents are stored in the systems of network operators and can be read by their personnel.SMS is sent as plaintext; unfortunately sms does not offer an secure environment for confidential data during transmission. So the traditional SMS service offered by various mobile operators surprisingly does not provide information security it is strongly required to provide end-to-end secure communication between end users. Security to the SMS is the main problem .Presently there is no scheme that provide complete sms security. SMS is a text messaging service component of phone, web, or mobile communication systems, using standardized communications protocols that allow the exchange of short text messages between fixed line or mobile phone devices. Users can used SMS to send or receive from a single person, or several persons, personal messages, email notifications, information services [1], school activity alerts, notification from teacher, job dispatches, and also stock alerts. With these usable application, SMS is now more and more common among mobile phone users. However the security issue [2] of SMS's is still an open challenging task. SMS is now a very common communication tool. The security protection of SMS messages is not yet that sophisticated and difficult to implement in practice. The confidentiality and integrity mechanisms are only specified as optional security measures that can be made available, but they are not mandatory requirements for SMS system implementation [3]. In this paper, there proposed the use of symmetric cryptography for SMS transfer securing The above requirements can be accomplished by proposing a protocol called Cipher-SMS which provides end-to-end security during the transmission of SMS over the network. The Cipher-SMS protocol achieved by using cryptographic algorithms of AES and MD5, The Cipher-SMS protocol prevents the SMS information from various attacks. Proposed SMS based framework provides efficient and more secure solution for SMS Transmission. Cipher-SMS is the first protocol completely based on the symmetric key cryptography of AES and hash cryptography of MD5 for cellular network.

2. PROBLEM STATEMENT

Sometimes, we send the confidential information like password, pass code, banking details and private identity to our friends, family members and service providers through an SMS. But the traditional SMS service offered by various mobile operators surprisingly does not provide information security of the message being sent over the network. In order to protect such confidential information, it is strongly required to provide end-to-end secure communication between end users. SMS usage is threatened with security concerns, such as SMS disclosure [4], man-in-the-middle attack [5], replay attack [6] and impersonation attack [7]. There are some more issues related to the open functionality of SMS which can incapacitate all voice communications in a metropolitan area [8], and SMS-based mobile botelnet [9] as Android botelnet [10]. SMS messages are transmitted as plaintext between mobile user (MS) and the SMS center (SMSC), using wireless network. SMS contents are stored in the systems of network operators and can be read by their personnel.

3. RELATED WORKS

In this section we briefly discuss the existing works of sms systems. The field of cryptography [11] can be divided into several techniques of study. There are two types of techniques in cryptography which are asymmetric key algorithm and symmetric key algorithm. Asymmetric key algorithm or sometimes called public key algorithm is usually based on complex mathematical problems. Symmetric key algorithm can be broadly grouped into block ciphers and stream ciphers [12]. Other symmetric key algorithms are cryptographic hash functions and Message Authentication Codes (MACs). Owning from suggestion of Garza-Saldana & Diaz Perez [12] that symmetric encryption could provide confidentiality to SMS, this paper perform an evaluation of three block cipher symmetric encryption techniques. This is done in order to find the most suitable block cipher symmetric encryption technique for securing SMS transmitted messages. Previously, various authors have proposed different techniques to provide security to the transmitted messages. An implementation of a public key cryptosystem for SMS in a mobile phone network has been presented in [13] but the security analysis of the protocol has not discussed. A secure SMS is considered to provide mobile commerce services in [14] and is based on public key infrastructure. A framework Secure Extensible and Efficient SMS (SEESMS) is presented in [15] which allows two peers to exchange encrypted communication between peers by using public key cryptography. Another new application layer framework called SSMS is introduced in [16] to efficiently embed the desired security attributes in SMS to be used as a secure bearer for m-payment systems and solution is based on the elliptic curve-based public key that uses public keys for the secret key establishment. An efficient framework for automated acquisition and storage of medical data using the SMS based infrastructure is presented in [17] and the results conclude that provide better security. However, implementation of framework always increases the overall overhead which is not much suitable for the resource constraints devices such as mobile phones. Thus, in this paper we compared our proposed protocol with the existing SMSSec and PK-SIM protocols. The reason for chosen these protocols for comparison is that these are the only existing protocols which do not propose to change the existing architecture of cellular networks. We wanted to compare our proposed protocol with some existing protocols devoted to provide end-to-end SMS security with symmetric key cryptography, but there is no such protocol exists. Both protocols are having two phases similar to the proposed protocol and are based on symmetric as well as asymmetric key cryptography while the proposed protocol is completely based on symmetric key cryptography. The SMSSec protocol can be used to secure an SMS communication sent by Java's Wireless Messaging API while the PK-SIM protocol proposes a standard SIM card with additional PKI functionality. Both protocols are based on client-server paradigm, i.e., one side is mobile user and the other side is authentication server but they do not present any scenario where an SMS is sent from one mobile user to another mobile user. The SMSSec protocol does not illustrate the security analysis

4. PROPOSED SYSTEM

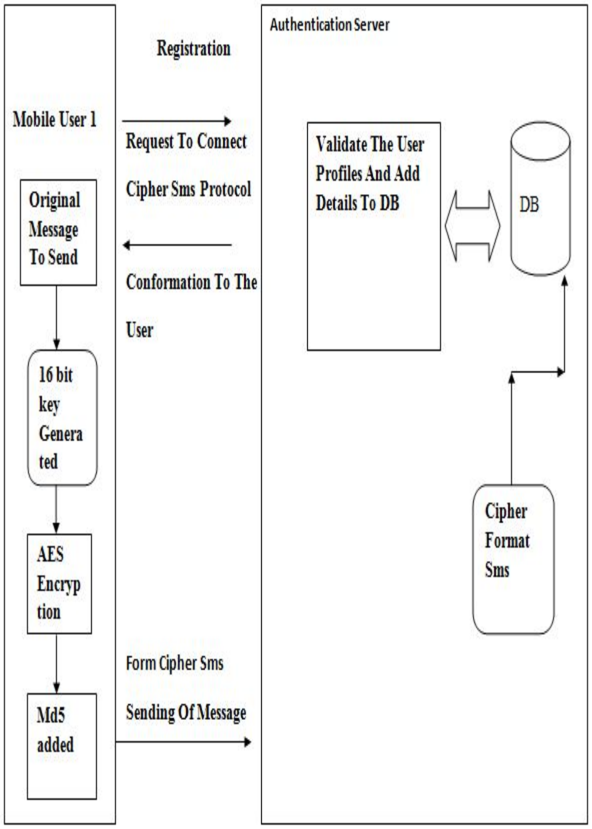
.

The Cipher-SMS provides end-to-end security during the transmission of SMS over the network. The Cipher-SMS protocol achieved by using cryptographic algorithms of

AES and MD5. The Cipher-SMS protocol prevents the SMS information from various attacks including SMS disclosure, over the air (OTA) modification, replay attack, man-in-the-middle attack, and impersonation attack. Proposed SMS based framework provides a low-bandwidth, reliable, efficient and cost effective solution for SMS Transmission. Cipher-SMS is the first protocol completely based on the symmetric key cryptography of AES and hash cryptography of MD5 for cellular network. This Cipher-SMS sends lesser number of transmitted bits, generates less computation overhead, and reduces bandwidth consumption and message exchanged as compare to existing protocols.

4.1 SYSTEM ARCHITECTURE

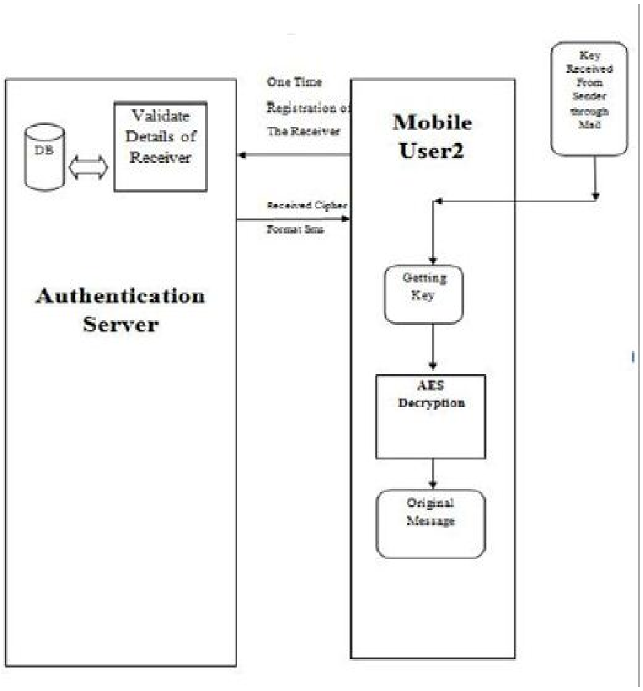
Architecture mainly consists of two parts: Sender side Architecture



Sender Side

Mobile user1 request to connect the cipher sms protocol to the authentication server for registraction.The authentication server first validate user profiles add details to the db.After validating it will send a conformation message to mobile user1.for producing cipher sms send sms content to mobile user2,when it reaches authentication server it under go AES encryption and generate cipher sms and it is stored in the database at that time MD5 algorithm produces a hash function. And finally send acknowledgement about cipher sms to mobile user1.

Receiver Side Architecture


DB
Validate Details of Receiver
Authentication Server
One Time Registration of The Receiver
Received Cipher Format Sms
Mobile User2
Key Received From Sender through Msd
Getting Key
AES Decryption
Original Message

Receiver Side

Receiver side mobile user2 request to the authentication server to connect cipher sms. Then authentication server validate the user profile and store in the database and replay with the conformation message to the mobile user with a telephone number. For receiving the msg mobile user2 send a key for decrypting the message. Then in Authentication server it undergo AES decryption using cipher sms and the key. And finally Receiver get the original message.

5. Modular Design

- User Profile
- Sms Communication
- Authentication Server
- Symmetric key

5.1 User Profile

The mobile device that receive the user details with some parameters that recognize the authenticate user. this restricts the non-owner users to see information about the SMS we send. in fig6, However, any mobile device using this service can get some additional profile examination has to be handled with some unique parameter. Through this function, the mobile device can allow authenticated profile owner that recognize the authenticate user. this restricts the non-owner users to see information about the SMS we send. However, any mobile device using this service can get some additional profile examination has to be handled with some unique parameter. Through this function, the mobile device can allow authenticated profile owner To access the data and send secure sms to others. This is to be explained in fig6.

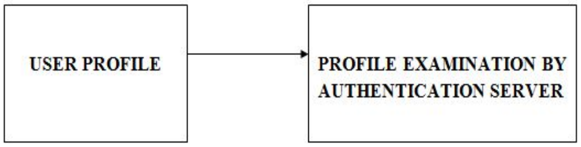


Fig1: User Profile

5.2: Sms Communication

In fig2,The Authenticated mobile user can send the SMS with some key to the server. The mobile who wants to send SMS must be registered with server. The mobile sends the SMS with certain key to server. The server can encrypt the original message using AES algorithm and the send SMS to receiver through base station and mobile station

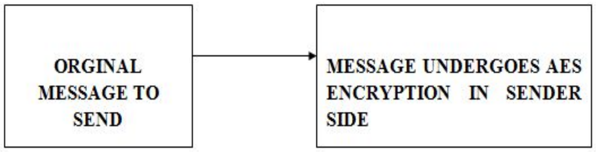


Fig2: Sms Communication

5.3Getting Key

In fig3,The Encrypted message can travel through base station. Receiver receives the message in secure inbox. Now the receiver wants to decrypts the message. So receiver requests the key using random number generator from server. Then server generates the random number and sends it to the receiver..receiver get the key from Gmail.

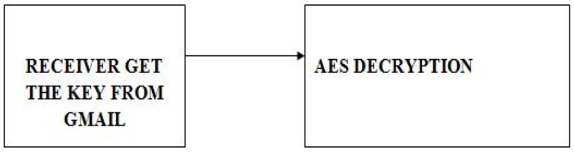


Fig3: Getting Key

5.4 Message Recovery

In fig4, The receiver get the original message from the mobile application

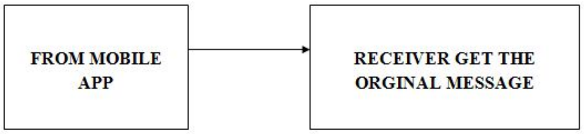


Fig4: Message Recovery

6. CONCLUSION

CipherSMS protocol is successfully designed in order to provide end to to end secure communication through SMS between mobile users. The analysis of the proposed protocol shows that the protocol is able to prevent various attacks.The transmission of symmetric key to the mobile users is efficiently managed by the protocol. This protocol produces lesser communication and computation overheads, utilizes bandwidth efficiently, and reduces message exchanged during authentication .A new symmetric key-based solution for secure SMS messaging (SSM). It is an application layer protocol that simultaneously provides theconfidentiality,integrity,authentication, nonrepudiation, public verification, and the forward secrecy of message confidentiality. It efficiently combines AES and digital MD5Algorithms and uses it has great computational advantages over the previously proposed symmetric key solutions while simultaneously providing the most feasible security services.

7. REFERENCES

[1] M. A. Hossain, S. Jahan, M. M. Hussain, M.R. Amin, and S.H. S Newaz, , “A Proposal for enhancing of short message services in GSM,” *IEEE /ASME Trans.security 2nd conference* on Anticounterfeiting, Security and Identification, ASID, Guiyang, China, 2008, pp. 235-240 .

[2] P. H. Kuaté, J. L. Lo and J. Bishop , “Secure asynchronous communication for mobile devices ,” Proceedings of the Warm Up Workshop for *IEEE Trans*. 2010,Cape Town,South Africa,2009,pp.5-8.

[3] J. J. Garza-Saldana and A. Diaz-Perez , “State of security for SMS on mobile devices ,” *IEEE Trans.* Proceedings of the Electronics, Robotics and Automotive Conference, Aug. 2008 pp 110-115.

[4] S. Ariffin, R. Mahmod, A. Jaafar and M.R.K. Ariffin , “Byte Permutations in Block Cipher Based on Immune Systems,” International Conference on Software Technology and Engineering ,3rd(ICSTE 2011.)ASME Press, New YORK,NY.,2011.

[5] D. Lisonek and M. Drahansky “SMS encryption for mobile communication ,” International Conference on Security Technology Hainan Island ,2008,pp 198-201

[6] B Schneider, “Applied cryptography protocols ,Algorithms And source cods in C,”John wiley and sons,,Inc.,NEW YORK,NY,USAA, *IEEE /ASME Trans. Mobile computing*, vol. 17, no. 3, pp. 397–403, 2nd edition 1995.

[7] W Stallings, “Cryptography and Network Security,” *IEEE /ASME Trans. Scurity*,Prentice Hall,New Jersey vol. 17, no. 3, pp. 397–403, Jun. 2006.

[8] S. Zhao, A. Aggarwal and S. Liu “Building secure user-touser messaging in mobile telecommunication networks ,” Proceedings of Wireless Telecommunications Symposium Pomona, CA, 2008 pp.151-157.

[9] J. P. Albuja and E. V. Carrera , “Trusted SMS communication on mobile devices ,” 11th Brazilian Workshop on Real-Time and Embedded Systems, Pernambuco, Brazil 2009, pp .165-170.

[10] X. P. Liu, W. Gueaieb, S. C. Mukhopadhyay, W. Warwick, and Z. Yin, “Guest editorial introduction to the focused section on wireless mechatronics,” *IEEE /ASME Trans. Mechatronics*, vol. 17, no. 3, pp. 397–403, Jun. 2012.

[11] S. Redl, M. W. Oliphant, M. K. Weber, and M. K. Weber “An Introduction to GSM ,” *IEEE /ASME Trans. networking*, vol. 17, no. 3, pp. 397–403, Jun. 2012.

[12] S. Ariffin, R. Mahmod, A. Jaafar and M.R.K. Ariffin , “Symmetric Encryption Algorithm Inspired by

Randomness and Non-linearity of Immune Systems ," *IEEE /ASME International Journal on Natural computing Research*, vol. 17, no. 3, pp. 397–403, Jun. 2012.

[13] Kahn, J., Yang, J. and Kahn, J. 2010 , "Mobile"Health Needs And Opportunities In Developing Countries. *Health Affairs* ," *IEEE /ASME International Journal on security*, 29,2(2010)252.

[14] J. Chen, L. Subramanian, E. Brewer , "SMS-Based Web Search for Low-end Mobile Devices ," *IEEE /ASME International Journal on security*, 16thMobiCom,2010,pp.125-135.

[15] Kuldeep Yadav , "SMS Assassin: Crowdsourcing Driven Mobilebased System for SMS Spam Filtering ," *IEEE /ASME International Journal on security*, Workshop HotMobile,2011,pp 1-6.

[16] K. Par ," Smartphone remote lock and wipe system with integrity checking of SMS notification ," *IEEE ICCE* 2011,pp 263-264.

[17] A. Santis, A. Castiglione, U. Petrillo ," An Extensible Framework for Efficient Secure SMS ," *IEEE /CISIS International Journal on security*, 2010,pp 843-850.

[18] M. Toorani, A. Shirazi , "SSMS-A secure SMS messaging protocol for the m-payment systems ," *IEEE /ISCC, International Journal on security*,2018,pp 70-75.

[19] P. Mondal, P. Desai, S. Ghosh , "An Efficient SMS -Based Framework for Public Health Surveillance ," *IEE/PHTInternational Journal on security*, ,2013,pp 1244-247.

[20] C. F. Lu, Y. S. Kan, H. Chiang, C. Yang , "Fast Implementation of AES Cryptographic Algorithms in Smart Cards ," *IEEE 37th ICCST, International Journal on security*, 2003,pp 573-579.