Volume : 4 | Issue : 3 | March 2015 • ISSN No 2277 - 8179

Mobile User Communication Over Wireless Network Based on Crypto-Random Method

Engineering

KEYWORDS : Mobile user, Crypto-Random, Encryption, Decryption.

B.Bala Abirami Anna University, S.A Engineering College, Dept of Computer Science and Engineering

N.Valli Anna University, S.A Engineering College, Dept of Computer Science and Engineering

ABSTRACT

Mobile communication is a process of sending data, messages, files or speaking over a mobile network. Mobile user (Mu) communicates with other user through Short Message Service (SMS) also. Formal as well as informal information can also send by SMS. Highly secured, confidential SMS messages are transmitted as plaintext between Mobile User 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. Since, the SMS is sent as plaintext, therefore network operators will simply access the content of SMS during the transmission at SMSC. In this paper, a new method called Crypto-Random method is proposed inorder to avoid such hacking. It uses cryptographic techniques on the confidential messages and the intermediate unauthenticated users cannot reveal the original confidential information.

INTRODUCTION

Nowadays the most excellent way to send any information in mobile network is through SMS, because of its fast, robust and uninterrupted nature; but at the same time, it is highly insecure. There is a chance for the SMS content to be read by the mobile operators which is send by the mobile users. The conventional communication service does not provide any type of safety issues to the SMS. Various applications such as health care monitoring [3], finance, banking and military services send their highly secured confidential information through SMS. In all these applications SMS plays a major role because the user can get their SMS anywhere in the world.

According to a new report, mobile phone penetration will rise from 61.1% to 69.4% of the global population between 2013 and 2017 [10]. SMS contents are subjected to various attacks such as SMS disclosure, OTA modification, Man-In-The-Middle (MITM) attack, Masquerade, play back attack. The mobile users can send their private, commercial, confidential information through SMS. Bank transactions such as One Time Password (OTP), Pin Number send by banks or organizations via SMS messages for authorizing or confirming high-risk on-line transactions leads to loss, modification of message content by the hackers. This is the research problem in mobile communication to transmit SMS across the network.

There are some protection issues related the open functionality of SMS, because the messages are transmitted as a plain text among the sender and receiver across the network. There is a chance for the intruders or hackers to read the confidential message. In this paper Crypto-Random model is proposed. It uses an efficient encryption and decryption method for SMS communication using AES cryptographic algorithm. The process of transforming plain text of SMS to cipher format SMS for data security is also proposed. After forming cipher text of the secure SMS, it is encoded with a random key. Android mobile phone is used to implement this method, which is used to transmit the confidential messages.

This paper comprises of the following sections. Introduction is given in first section. The second section gives the proposed system model, next it deals with advantages of the proposed system. The last section concludes the paper with future work.

CASE STUDY

SYSTEM ARCHITECTURE

This section case study deals with the system architecture of the Crypto-Random method. This comprises of three components Mobile user1 (sender), Mobile user2 (Receiver) and the Authentication server. The design model narrates how the user creates the secret message and the process of forwarding and authenticating. It comprises of two sides (1) Sender side Architecture (2) Receiver side Architecture. It is clearly shown in Figure (1) and Figure (2)

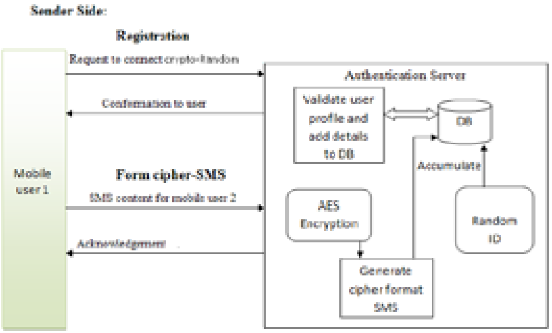

Figure.1: Sender side Architecture

The above figure illustrates the Sender side Architecture. In Registration phase, the Mobile user1 send a request signal to connect to the Authentication server. The Authentication server validates the user profile and adds detail about the user in its database. After that it sends a conformation request to the sender. Then the sender sends a confidential message to the receiver through the Authentication server. It performs encryption to the confidential message using AES.The AES uses 192 bit keys for encryption. Then it generates a random key and it is accumulated with the cipher format SMS. Now it is ready to send to the receiver.

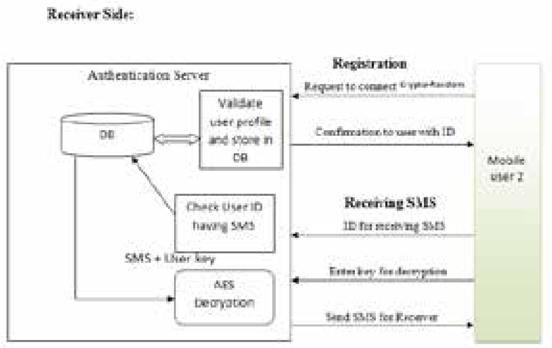

Figure.2: Receiver side Architecture

Figure 2 illustrates the Receiver side Architecture. In Receiver side, the receiver must also perform registration with the Authentication server. The mobile user2 who is the receiver sends a request to connect to the crypto-Random protocol. The Authentication server checks in its database and sends a conformation request to the receiver. The receiver sends a valid user id to receive the confidential message. The Authentication server checks in its database. If it matches means, it will decrypt the message and send it to the receiver.

The Crypto-Random method uses three techniques
(i)User validation: The Sender and Receiver have to register their details with the Authentication server. The Authentication server updates the necessary details in its database. Thus the Authentication server validates the correct user and it is used to identify the unauthorized user. (ii)Message creation and display: The message creation is done by the sender using a mobile App which is installed in their android mobile phone. The receiver after receiving the message it can be viewed as a message in encrypted (alphanumeric) format, if they know the key value only the original message is displayed to them.

(iii)Encryption and Decryption: The Authentication server gets the original confidential message from the sender. It checks for validity and performs Encryption using AES-192 symmetric key cryptographic algorithm. Then it generates a random key using Random key generator and both these are accumulated and it generates a secure cipher format SMS.

Decryption takes place in the receiver side. The Authentication server in the receiver side checks for receiver validity and if it matches with the details in database means it will perform decryption of the confidential message and send it to the receiver.

ADVANTAGES OF PROPOSED SYSTEM

This section focuses on the advantages of the proposed system. The Crypto-Random method uses cryptographic algorithm of AES-192 and a random number generator (OTP).It provides a high degree of

(i)Authentication: The Crypto-Random method provides authentication to the mobile user. This is done by the Authentication server. It will allow only the authenticated users to communicate in the mobile network.

(ii)Data Confidentiality: This method provides a high degree of data confidentiality to the message that is transmitted across the network. It uses highly secured encryption and decryption method to transmit the confidential messages.

(iii)Avoids various attacks: It avoids various attacks such as SMS disclosure, OTA modification, Man-In-The-Middle (MITM) attack, Masquerade and play back attack.

CONCLUSIONS

Crypto-Random method is implemented in smartphones as an app, it is effective because of its low expenditure and its easy execution process. It is applied in application layer and provides a high grade of confidentiality to the transmitted messages. This method uses AES-192 which provides high security to the confidential messages. It shows that this method is able to avoid many attacks. For the future work this can be implemented with picture, Audio, Video and needs to use high compression technique.

REFERENCE

J. L.-C. Lo, J. Bishop, and J. H. P. Eloff, “SMSSec: An end-to-end protocol for secure SMS,” Comput. Security, vol. 27, nos. 5–6, pp. 154–167, 2008. | [2] M. Toorani and A. Shirazi, “SSMS—A secure SMS messaging protocol for the m-payment systems,” in Proc. IEEE ISCC, Jul. 2008, pp.700-705. | [3] K. Yadav, “SMSAssassin: Crowdsourcing driven mobile-based system for SMS spam filtering,” in Proc. Workshop Hotmobile, 2011, pp. 1–6. | [4] I. Murynets and R. Jover, “Crime scene investigation: SMS spam data analysis,” in Proc. IMC, 2012, pp. 441–452. | [5] C. H. Kim, “Improved differential fault analysis on AES key schedule,” IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 41–50, Feb. 2012. | [6] S. Wu and C. Tan, “A high security framework for SMS,” in Proc. 2nd Int. Conf. BMEI, 2009, pp. 1–6. | [7] Neetesh Saxena and Narendra S. Chaudhari, “EasySMS: A Protocol for End-to-End Secure Transmission of SMS” IEEE Trans. Inf. Forensics and Security, vol. 9, no. 7, pp. 1157–1168, July. 2014 | [8] A. Medani, A. Gani, O. Zakaria, A. Zaidan and B. B. Zaidan “Review of mobile short message service security issues and techniques towards the solution” Scientific Research and Essays Vol. 6(6), pp. 1147-1165, 18 March, 2011. | [9] Manoj Patil, Prof. Vinay Sahu “A Survey of Compression and Encryption Techniques for SMS” International Journal of Advancements in Research & Technology, Volume 2, Issue 5, May-2013. | [10] http://www.emarketer.com/Article/Smartphone-Users-Worldwide-Will-Total-175-Billion-2014/1010536#sthash.c6k9wEjj.dpuf | [11] I. Murynets and R. Jover, “Crime scene investigation: SMS spam data analysis,” in Proc. IMC, 2012, pp. 441–452 | [12] R. E. Anderson et al., “Experiences with transportation information system that uses only GPS and SMS,” in Proc. IEEE ICTD, no. 4, Dec.2010