An Efficient and Secure Symmetric key used for EasySMS protocol

Nandini V, Student
Mtech 4th Sem (CSE)
SVIT, Bangalore, India
Nandiniv.v18@gmail.com

Deepak M
Assistant professor (CSE)
SVIT, Bangalore, India

***Abstract*—** SMS (Short Message Service) is a widely used communication between the end users. SMS is being used in our different applications. The Short Message Service (SMS) usually whatever we exchange the original format, sometimes we used to send the some secret message like our email password, pass code and bank password. We send SMS is in original format, our traditional SMS does not secure this trusted information, so the proposed protocol called EasySMS it will provide very secure and protect the trusted information between the end users.

Keywords- *component; Authentication, Security, Secrete Key, Mobile Phone*

*****

I. INTRODUCTION

Nowadays, the Short Message has become one of the most fast and strong communication in the world to transmit the message from two persons. The Short Message Service called SMS is a communication platform that sends the message through a mobile cellular network.

When the sensitive information in our messages (**SMS**), it is very difficult to protect the information from the eavesdroppers and also very difficult to identify the origin from the particular sender. The mobile phone communication is very good experience and a great acceptance from among all human society.

The GSM is airway traffic communication between the two mobile stations called Mobile Station (MS) and the Base Transceiver Station (BTS) is a encryption between two weak and stream cipher (A5/1 or A5/2). The authentication is a one sided and also unprotected.

Despite the increasing power of mobile devices with the advent of "Smart Phones", a significant fraction of mobile devices in developing regions are still simple low-cost devices with limited processing and communication capabilities.

A. Research Problem

Sometimes, we used to send trusted information to our family members like password, credit number also bank pass book number. This confidential information from one mobile phone to another through network. While sending the information over the network eavesdropper can read the information because that will be in the original format. SMS usage is threatened with security concerns, such as SMS disclosure, man-in-middle attack and replay attack. SMS messages are transmitted as plaintext between mobile user and the SMS center using wireless network.

B. Key Contribution

The above protocol called EasySMS is proposed to prevent and secure the end-to-end communication between the users, the protocol EasySMS is going to prevent the various attack are Man-in-middle attack, Replay attack, SMS disclosure and it is also message exchange during the authentication process, less computation overhead and reduces the bandwidth.

II. RELATED WORK

According to the various authors have proposed different types of techniques and security to protect information during transmiision of the message. An implementation of a public key cryptosystem for SMS in a mobile phone network has been presented, but the security for protocol is not discussed. Peer-to-peer exchange encrypted using public key cryptography by **A framework secure extensible and efficient SMS(SEEMS)**. Another protocol called SSMS is used to provide the application layer framework for the desired security attributes in SMS. **During the transmission of message to provide the security for the message by using bearer for m-payment**. Due to physical limitations of the mobile phones it is very neccesary to offer the protocol which would make minimum use of resources and would make better security.

The proposed protocol called **SMSSec** is used to protect SMS communication between a client and also used to the encryption between end users. The protocol SMS based framework provides a low-bandwidth, reliable, efficient solution for medical data acquistion. The shared session key generation is highly usage communication and it is also unsuitable for real eord application.

Thus in this proposed protocol **EasySMS** compared with two protocol called **SMSSec** and **PK-SIM** protocols.

III. EXISITNG SYSTEM

In Existing System, the SMS based framework provided a low-bandwidth, reliable, efficient and cost effective solution for medical data acquisition. The generated shared key for each session generated a huge overhead. This framework failed to prevent SMS against various attacks.

SMS messages are transmitted as plaintext between mobile user (MS) and the SMS centre (SMSC), using wireless network. SMS contents are stored in the systems of network operators and can be read by their personnel.

An attack model describes different scenarios for the possibilities of various attacks where a malicious MS can access the authentic information, or misguide the legitimate MS. Since, the SMS is sent as plaintext, thus network operators can easily access the content of SMS during the transmission at SMSC.

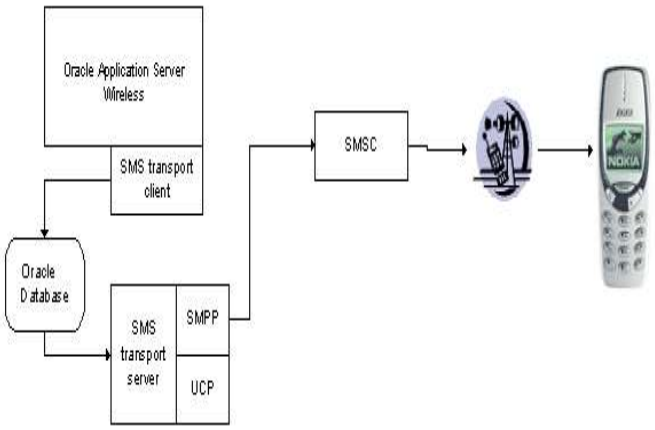

Fig1. Existing Architecture

IV. PROPOSED SYSTEM

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.

In order to overcome the above stated attacks, various cipher algorithms are implemented with the proposed authentication protocol. We recommend that the cipher algorithms should be stored onto the SIM (part of MS) as well as at AS. Since providing security needs to do some extra effort which is measured in terms of cost, thus providing or adding extra security means increasing more cost. Authors propose to include one more service as 'Secure Message' in the menu of mobile software developed by various mobile companies.

Mobile operators can add some extra charges to send secure message by their customers over the networks. Whenever a user wants to send a secure message to other user, the proposed protocol namely EasySMS is executed which makes available the symmetric shared key between both MS and then ciphering of message takes place using a symmetric key algorithm.

We propose a new protocol named EasySMS with two different scenarios which provide end-to-end secure transmission of information in the cellular.

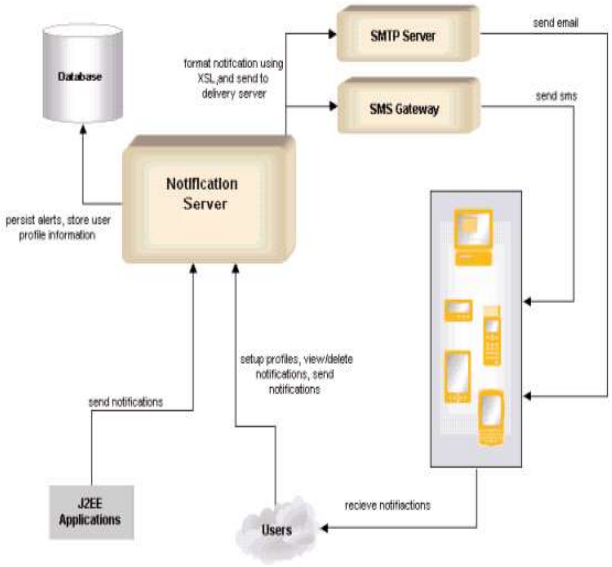

Fig2. Proposed Architecture

Is the Secret Key SK Safely Stored? Since the malicious user does not know the structure of cryptographic functions like f1() and f2(), so he/she can neither generate the correct MAC1 nor correct delegation key DK1. Further, the secret key SK is stored on the authentication server/centre as well as embedded onto the SIM at the time of manufacturing. Thus, it is almost impossible to extract the SK. The storage scenario of SK key we presented is same as nowadays used for the voice communication in the traditional cellular networks. If some service providers do not wish to use actual SK in the protocol execution.

The EasySMS protocol prevents the SMS information from various attacks including SMS attack, phone hijack, SMS spam, man-in-the-middle attack, and GSMA. This EasySMS sends lesser number of transmitted bits, generates less computation overhead, and reduces bandwidth consumption

and message exchanged as compared to SMSSec and PK-SIM protocols.

V. CONCLUSION

The EasySMS protocol is typically used to design for protection of various attacks and also provide end-to-end secure communication.

Symmetric key is efficiently managed by the proposed protocol called EasySMS and also it is communication overhead during execution, compared to SMSSec and PK-SIM protocol authentication of exchange of messages is less.

VI. REFERENCES

[1] H. Rongyu, Z. Guolei, C. Chaowen, X. Hui, Q. Xi, and Q. Zheng, "A PK-SIM card based end-to-end security framework for SMS," *Compute. Standard Interf.* vol. 31, no. 4, pp. 629–641, 2009

[2] M. Densmore, "Experiences with bulk SMS for health financing in Uganda," in *Proc. ACM CHI*, 2012, pp. 383–398.

[3] D. Risi and M. Teófilo, "MobileDeck: Turning SMS into a rich user experience," in *Proc. 6th MobiSys*, no. 33, 2009.

[4] 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.

[5] J. L.-C. Lo, J. Bishop, and J. H. P. Eloff, "SMSSec: An end-to end protocol for secure SMS," *Compute. Security*, vol. 27, nos. 5–6, pp. 154–167, 2008.