International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-4, June 2015
ISSN: 2395-3470
www.ijseas.com

A Survey on Secure SMS Transmission and authentication at user end

SandeepKumar Laxman Sahu[1], HOD Prof Pragati Patil[2]

[1] Dept. name of organization: Computer Sc. and Engineering
Name of organization -Abha- Gaikwad Patil College of Engineering
NAGPUR, INDIA
[2] Dept. name of organization: Computer Sc. and Engineering
Name of organization -Abha- Gaikwad Patil College of Engineering
NAGPUR, INDIA

Abstract— *Short message service (SMS) is most important communication medium in many daily life applications, including healthcare monitoring, mobile banking, mobile commerce, and so on. when a SMS send an from one mobile phone(MS) to another MS (Mobile subscriber), the information contained in the SMS transmit as plain text. Sometimes this information may be confidential like account numbers, passwords, license numbers, and so on, and it is a major drawback to send such information through SMS while the traditional SMS service does not provide encryption to the information before its transmission, However telecom service providers are ensuring at server end some security provided as Using A3,A8 and Kc algorithms, but not providing during the message transformation .In this paper, we propose an efficient and secure protocol called User End secure SMS along with integrity key check, which provides end-to-end secure communication through SMS between end users. The working of the protocol is presented by considering two different scenarios. The analysis of the proposed protocol shows that this protocol is able to prevent various attacks, including SMS disclosure, over the air modification, replay attack, man-in-themiddleattack, and impersonation attack. . The protocol completely based on the symmetric key cryptography and retains original architecture of cellular network. The simulation generated in C#.net for execution system. SMS protocol is successfully designed in order to provide end-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. We consider all the transmission among various Authentication Server AS(Either Same location or different location) take place by encrypting the message with a symmetric key shared between each pair of AS. This protocol produces lesser communication and computation overheads, utilizes bandwidth efficiently, and reduces message exchanged ratio during authentication than AES.*

Keywords: *Authentication, over-the-air, security, SMS, Symmetric key, A3, A8, Kc*, Ik.

I. INTRODUCTION

All the confidential information like password, pass code, banking details and private identity to our friends, family members and service providers through an SMS. The traditional SMS service offered by various mobile operators surprisingly do not have 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, man-in-the-middle attack, replay attack and Impersonation attack. There are some more issues related to the open functionality of SMS which can incapacitate all voice communications in a metropolitan area, and SMS-based mobile. 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. The system should provide the encryption of the message at the user end through the server having less computational time and secured information transformation. SMS flow work as two types:

TYPE OF MESSAGE

1.1SMS MO-Used for Message Originating GSM Specific T21: ISDN Telephony

1.2 SMS MT-Used for Message Terminating GSM Specific T22: ISDN Telephony

2. Literature Survey

Existing AES symmetric key for data encryption and decryption. This system has claim this is first protocols based on encryption technique, *Neetesh Saxena et al [01]* proposed the SMS from one mobile phone to another, the information contained in the SMS transmit as plain text. Sometimes this information may be an efficient and secure protocol called EasySMS, which provides end-to-end secure communication through SMS between end users. The working of the protocol is presented by considering two different scenarios. Authors claim that EasySMS is the first protocol completely based on the symmetric key cryptography and retain original architecture of core cellular network. Protocol reduces of the bandwidth consumption and reduces of message exchanged time during the authentication process in comparison to SMSSec and PK-SIM protocols respectively a Protocol for End-to-End Secure Transmission of SMS.Brief SMS flow is given for the Existing system.

Ruth E. Anderson et al [02] In this paper at present our experiences with an SMS-based system for providing transit information based solely on existing cellular and GPS networks. The aim is to permit the development of information services that do not rely on a central authority or complex web hosting. We developed and applied our system to the network of privately-run marshrutka buses in Bishkek, Kyrgyzstan. However, our goal is to more broadly address issues of ad-hoc shared transportation systems in the developing world. A custom designed GPS-GSM unit is placed on a vehicle, and users can query our server over SMS with their own non-GPS enabled cell phones.

We report on the accuracy of our location naming approach and estimates of bus arrival times. In addition, we summarize interviews with bus drivers and bus riders relating their views of the system and outline directions for future work. This system is a grass roots solution to the persistent lack of transport information in developing countries. Above paper are most of uses for experiences with a Transportation Information System that Uses Only GPS and SMS.

Mauro Ricardo et al[03] A case study of a quiz game designed to be used using SMS technology; the study consists of monitoring the game adaption to the Mobile Deck concept. In the Mobile Deck concept, the SMSs are received and sent through an appropriate graphical user interface. System efficiency and game Improvement will be analyzed and discussed in this paper, in order to infer that the use of this proposed model is beneficial to the ecosystem of games based on SMS. The integration of the cited game to Mobile Deck concept was proved a success, providing a new way of playing games via SMS.In this paper Improving Games by SMS through the MobileDeck Concept without any data loss with secure concept. The application server (ASE) enables the external applications using the CIMD2 protocol to connect to the SMS Center kernel. The ASE communicates with the client applications using the CIMD2 the CIMD2 protocol allows each client to send and retrieve short messages and status reports in a flexible way by transferring data to and from the SMS Center. In this paper following points discussed and try to enhance some features.

- Receiving messages from the mobile stations and applications.
- Storing messages to the database (SMS) in SMSC.
- Support for real time charging with ECN(End Call Notification)
- Delivering messages to the destinations.
- Retrying to send messages at predetermined intervals if the first delivery attempt fails.
- Delivering a status report to the originator of the message when requested and storing the status reports to the database.
- Receiving alerts from the network.
- Forwarding alerts.
- Checking capacity license key.

Kuldeep yadav et al [04] proposed the reason to increase is used of SMS over mobile phones in developing countries, there has been a burst of spam SMSes. Content-based machine learning approaches were effective in filtering email spams. Researchers have used topical and stylistic features of the SMS to classify spam and ham. SMS spam filtering can be largely influenced by the presence of regional words. In this paper ongoing research, as an exploratory step, developed mobile-based system SMSAssassin that can filter SMS spam messages based on bayesian learning and sender blacklisting mechanism. Since the spam SMS keywords and patterns keep on changing, SMSAssassin uses crowd sourcing to keep itself updated. Using a dataset that,we are collecting from users in the real-world, we evaluated our approaches and found some interesting result.

SMS spam filtering is an important problem to solve and make use of the Information Communication Technologies (ICT) to the fullest. it have designed a bayesian based mobile Spam filtering application which satisfies most of design goals with accuracy Considering user perception about spam SMSes, it have provided a user oriented solution where different tabs in mobile application gives use freedom to receive SMSes which are spams but still useful to him/her. Reception of SMS does not cost in India even in the roaming, this kind of solution may work well. ICT-based systems, which have the following properties:

- Every visit is captured.
- Structured data is collected,
- Data are sent in real time, and
- The system allows CHWs

Lakshmi Subramanian et al[05] Proposed Short Messaging Service (SMS) based mobile information services have become increasingly common around the world, especially in emerging among user with low-end-mobile device.

This paper presents the design n and implementation of SMS Find, an SMS-based search system that enable users to obtained extremely concise and appropriate search responses for queries across arbitrary topics in one round of interaction SMS find the designed to complement existing SMS-based search Services that are either limited in the topics they recognize or involve a human in the loop.

The exceptional growth of the mobile phone market has motivated the design of new forms of mobile information services. With the growth of Twitter, SMS GupShup and other social messaging networks, the past few years have Witnessed a growing prevalence of Short-Messaging Service(SMS).

Brian DeRenzi1 et al[06] .In this paper having many benefits, many challenges, including super vision and support, make CHW programs difficult to maintain. An increasing number of health projects are providing CHWs with mobile phones to support their work, which opens up opportunities for real-time supervision of the program with secure and correct manner. Taking advantage of this potential, we evaluated the impact of SMS reminders to improve the promptness of routine CHW visits, first in a pilot study in Dodoma, Tanzania, followed by two larger studies with 87 CHWs in Dar es Salaam, Tanzania. The first Dar es Salaam study evaluated an escalating reminder system that sent SMS reminders directly to the CHW before notifying the CHW's supervisor after several overdue days. The reminders resulted in an 86% reduction in the average number of days a CHW's clients were overdue (9.7 to 1.4 days), with only a small number of cases ever escalating to the supervisor. However, when the step of escalating to the supervisor was removed in the second study, CHW performance significantly decreased. These are used for Improving Community Health Worker Performance through Automated SMS. This work makes the following contributions:

a. A randomized controlled study showing that an escalating reminder system causes a significant increase in CHW performance, with the average number of days clients are overdue dropping from 9.7 to 1.4 days (85.6%).

b. A second randomized controlled study showed that the step of escalating to supervisor is integral: removing that step from

the process and sending SMS reminders to only the CHW significantly decreases performance.

c. Lessons learned about the implementation of an automated reminder system and several ways to build upon our basic approach in the future. At the time of submission, this system is still running and has sent more than 25,000 SMS messages over the eight and half month period.

Melissa Densmore et al [07] Short message service (SMS, aka text messaging) is a low-cost and effective means of communication for organizations attempting to maintain contact with many people. In this paper we look at the deployment and of a bulk mobile text-messaging platform (Bulk SMS), conceived and commissioned by a health non-governmental organization (NGO) for use in communicating with the 100+ private health facilities. In this paper show how the platform emerged from existing practices, the features and expectations of the system, and the ways in which it was used. Common failure points include infrastructural limitations, human error, and unexpected use cases. We find that 1) the use of SMS as a media enables new w types of communication, and 2) SMS alone is not sufficient for maintaining relationships within the NGO program. The NGO was in constant communication with the HSPs. For each payment made, the project coordinator (PC) in Mbarara was required to secure confirmation from each of the HSPs that they successfully received the correct payment in their bank accounts. The project management office (PMO) also coordinated yearly training sessions, handled question regarding the treatment protocol, and settled disputes regarding unpaid claims. The PMO sales staff traveled to each of the HSPs once or twice a month to deliver blank claims to the HSPs as they ran out, pick up claim submissions, and relay messages from the NGO.

We are using above references for literature survey to implementation of SMS protocol is successfully designed in order to provide end-to-end secure communication through SMS between mobile networks to user end.

3 Authentication Principles

Authentication is a procedure used in checking the validity and Integrity of subscriber data. With the help of the authentication Procedure the operator prevents the use of false SIM modules in the network. The authentication procedure is based on an identity key, Ki,that is issued to each subscriber when his data are established in the HLR. The authentication procedure verifies that the Ki is exactly the same on the subscriber side as on the network side.

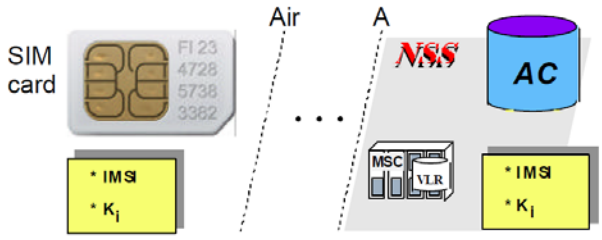

Fig 3.1 Authentication

Authentication is performed by the VLR at the beginning of every call establishment, location update and call termination (at the called subscriber side). In order to perform the authentication, the VLR needs the basic authentication information. If the mobile station was asked to Broadcast its K i, this would undermine the principle of authentication, because identification data would be sent across the air. The trick is to compare the K i stored in the mobile with the one stored in the network without actually having to transmit it over the radio air interface. The Ki is processed by a random number with a “one way” algorithm called A3 and the result of this processing is sent to the network. Due to the type of the algorithm A3, it is easy to get the result on the basis of Ki and a random number, but it is virtually impossible to get the Ki on the basis of the result and random number (hence the name “one way” algorithm). Since the security issue concerns confidentiality as well, the network uses more than one algorithm. These are introduced in the following sections.

The Authentication Centre generates information that can be used for all the security purposes during one transaction. This information is called an Authentication Triplet.

The authentication triplet consists of three numbers:

- **RAND**
- **SRES**
- **Kc.**

International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-4, June 2015
ISSN: 2395-3470
www.ijseas.com

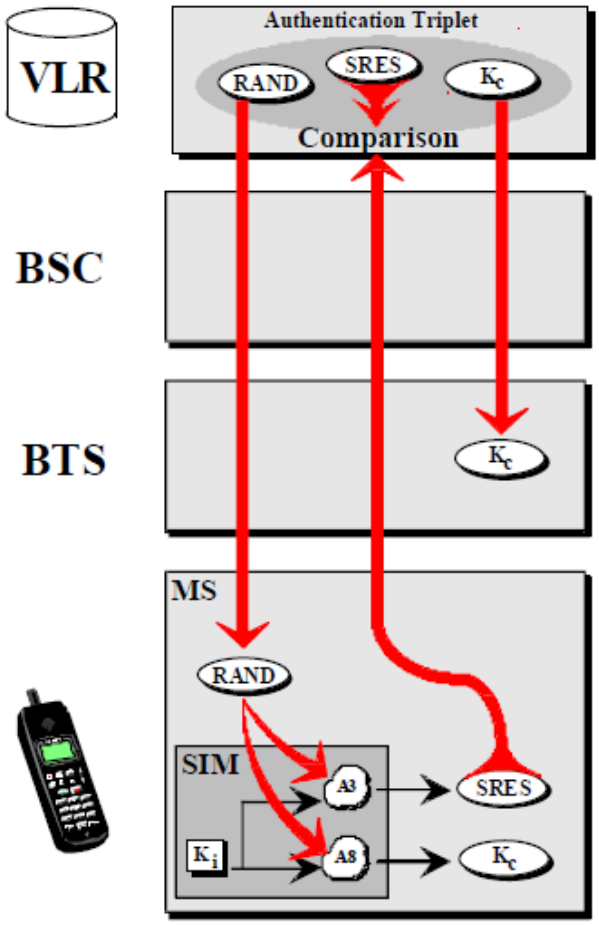

Fig 3.2 Authentication Procedure

4 Characteristics of the attacks during SMS transmission

In recent years, new applications, architectures, and technologies have been proposed for Authentication and encryption technique regarding SMS transformation applications for Cellular. Provide the enhance of the security at user end and less quarry time at user Side. It will protect in over the air:

3.1 Man-in-the-middle attack.

3.2 Replay attack.

3.3 Impersonation attack.

3.4 Private health facilities using SMS .

3.5 Participation in elections through SMS .

3.6 In Crime Scene Investigation.

3.7 In case of medical emergency/military/any disasters, it will work with less computational time and secure as well as reduce overheads.

Existing Security done at AuC end and it is done by VLR, AuC and MS jointly as disscussed with Authentication Procedure.

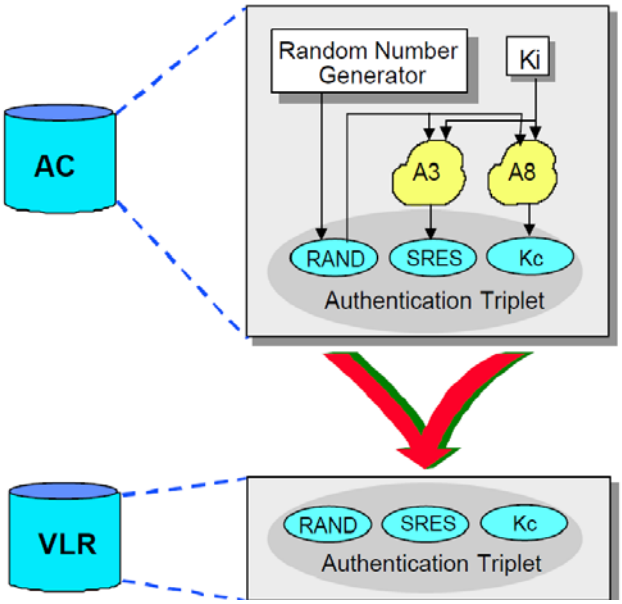

Fig 4.1: Security flow from AuC and VLR

5 Global Title Definitions in GMSC

GT(Globe Title Exp. In INDIA-+91-XXXX) analysis is also involved for successful SMS delivered to destination. Each service operator need to be open particular GT at their Gateway network element as per DoT/ITuT Guideline as this is very challenging task.GT Should be open in NP1(Numbering Plan-1) at each service provider end for smoothly successful message delivery.SMSC GT of each operator should be opened in operator Gateway MSC/GMSC.

6 Reason for Security

With the increasing use of SMS for communication and information exchange, care should be taken when sensitive information is transmitted using SMS. Users should be aware that SMS messages might be subject to interception. Solutions such as encrypted SMS should be considered if there is a need to send sensitive information via SMS.

7 Techniques Used for detection of attacks

The SMS protocol is able to prevent the transmitted SMS from various attacks over the network. It is assumed that the cryptographic functions used in the paper are not publically available and are secret. The capturing of any secret key SK is not possible because no secret key has been transmitted in any phase of the proposed protocol and always a delegation key DK1 is being transferred in the cipher mode whenever is required. Secret keys are also not publically available and are secret.

6.1) SMS Disclosure: In the EasySMS protocol, a cryptographic encryption algorithm is maintained to provide end-to-end confidentiality to the transmitted SMS in the network. Thus, encryption approach prevents the transmitted SMS from SMS disclosure through key verification.

6.2) Replay Attack: The proposed protocol is free from this attack because it sends one timestamp (like T1, T2, T3, T4 and T5) with each message during the communication over the network. These unique timestamp values prevent the system from the replay attack.
This attack can be detected if later previous information is used or modified. Additionally Kc algorithm verified in Air interface on BTS.

6.3) Man-in-the-middle Attack: In the SMS protocol, a symmetric algorithm is used for encrypting/decrypting end-to-end communication between the MS and the AS in both scenarios. The message is end-to-end securely encrypted/decrypted with DK1 key for every subsequent authentication and since attacker does not have sufficient information to generate DK1, thus it prevents the communication from MITM attack over the network.

6.4) Modification in SMS Transmission: The SMS protocol provides end-to-end security to the SMS from the sender to the receiver including OTA interface with an additional Strong encryption algorithm. The protocol does not depend upon the cryptographic security of encryption algorithm exists between MS and BTS in traditional cellular networks. This protocol provides end to end security to end users. It protects the message content being access by mobile operators as well as from attackers present in the transmitted medium. This section analyzes proposed protocol in various aspects such as mutual authentication, prevention from various threats and attacks, key management, and computation & communication overheads. Proposed algorithm: RC-4 for security.

SMS is now a very common communication tool. Security protection of SMS messages is not yet that sophisticated and difficult to implement in practice. Two different scenarios which provide end-to-end secure transmission of information in the cellular networks. First Scenario is illustrated in below Fig. Where both MS belong to the same AS, in other words share the same Home Location Register (HLR) while the second scenario is presented in Fig. where both MS belong to different AS, in other words both are in different HLR. There are two main entities in the SMS protocol. First is the Authentication Server (AS), works as Authentication Center (AuC) and stores all the symmetric keys shared between AS and the respective MS. In this paper, we refer AuC as the AS. Second entity is the Certified Authority/Registration Authority (CA/RA) which stores all the information related to the mobile subscribers. We assume that every subscriber has to register his/her mobile number with CA/RA entity and only after the verification of identity, the SIM card gets activated by this entity. Thus, this entity is responsible to validate the identity of the subscribers. We also assume that a symmetric key is shared between the AS and the CA/RA which provides the proper security to all the transmitted information between AS and CA/RA. It is considered that various authentication servers are connected with each other through a secure channel since one centralized server is not efficient to handle data all around. We consider all the transmission among various AS take place by encrypting the message with a symmetric key shared between each pair of AS. Both scenarios of this protocol are as follows. Secure SMS communications are two types: Both MS (SIM+ Equipment) belongs in same AS or different AS.

8. Conclusions and future scope

The SMS protocol can be successfully designed in order to provide end-to-end secure communication through SMS between mobile users at user end. The proposed protocol shows that the protocol is able to protect from 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 ratio during authentication than AES.We will use RC-4 for computation overheads reductions. In future can be introduced an integrity Key to make more secure system between Hop to Hop from MO user to MT users.

REFERENCES

[1] Press Release. (2012, Dec. 3). *Ericsson Celebrates 20 Years of SMS* [Online]. Available: http://www.ericsson.com/ag/news/2012-12-03-smsen_ 3377875_c

[2] 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.

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

[4] K. Yadav, "SMSAssassin: Crowdsourcing driven mobile-based system for SMS spam filtering," in *Proc. Workshop Hotmobile*, 2011, pp. 1–6.

[5] J. Chen, L. Subramanian, and E. Brewer, "SMS-based web search for low-end mobile devices," in *Proc. 16th MobiCom*, 2010, pp. 125–135.

[6] B. DeRenzi *et al.*, "Improving community health worker performance through automated SMS," in *Proc. 5th ICTD*, 2012, pp. 25–34.

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

[8] J. Hellström and A. Karefelt, "Participation through mobile phones: A study of SMS use during the Ugandan general elections 2011," in *Proc. ICTD*, 2012, pp. 249–258.

[9] I. Murynets and R. Jover, "Crime scene investigation: SMS spam data analysis," in *Proc. IMC*, 2012, pp. 441–452.

[10] K. Park, G. I. Ma, J. H. Yi, Y. Cho, S. Cho, and S. Park, "Smartphone remote lock and wipe system with integrity checking of SMS notification," in *Proc. IEEE ICCE*, Jan. 2011, pp. 263–264.

[11] A. Nehra, R. Meena, D. Sohu, and O. P. Rishi, "A robust approach to prevent software piracy," in *Proc. SCES*, 2012, pp. 1–3.

[12] N. Gligoric, T. Dimcic, D. Drajic, S. Krco, and N. Chu, "Applicationlayer security mechanism for M2M communication over SMS," in *Proc. 20th TELFOR*, 2012, pp. 5–8.

[13] S. Gupta, S. Sengupta, M. Bhattacharyya, S. Chattrejee, and B. S. Sharma, "Cellular phone based web authentication system using 3-D encryption technique under stochastic framework," in *Proc. AH-ICI*, 2009, pp. 1–5.

[14] P. Traynor, W. Enck, P. McDaniel, and T. La Porta, "Mitigating attacks on open functionality in SMS-capable cellular networks," *IEEE/ACM Trans. Netw.*, vol. 17, no. 1, pp. 40–53, Feb. 2009.

[15] Y. Zeng, K. Shin, and X. Hu, "Design of SMS commanded-andcontrolled and P2P-structured mobile botnets," in *Proc. 5th WiSec*, 2012, pp. 137–148.