International Journal of u- and e- Service, Science and Technology
Vol.8, No.2 (2015), pp.365-374
http://dx.doi.org/10.14257/ijunesst.2015.8.2.35

Financial Transaction Security Using Mobile SMS

Manoj Kumar Jain[1] and Anjana Jain[2]

[1]*Tata Consultancy services Bangalore*
[2]*Tech Mahindra, Bangalore*
[1]*Manoj.kumarjain@gmail.com*, [2]*Anjanajain2003@gmail.com*

Abstract

Almost every business uses SMS for various reasons to increase sales and brand exposure and Mass alert to everyone. 80% of cell phone users carry their phone all the time. Sending a text message to their cell phones is the perfect way to alert them of any urgent information, such as a change of appointment, or product ready for pickup etc. Mass alert are an ideal way for school districts to send alerts to parents regarding school closings, changes in schedules etc.

The short message service (SMS) is one of the highly used and well-tried mobile services with global availability within all GSM/CDMA networks. The existing SMS is limited to the transmission of secure plain text between different mobile phone subscribers and server for different purpose. SMS does not have any built-in procedure to authenticate the text and offer security for the text transmitted as data [5], because most of the applications for mobile devices are designed and developed without taking security into consideration [6] [7], But we can use SMS service to protect our financial transaction by enable or disable the account apply some security on SMS. It will help to control fraud on financial traction by ATM or online fund transfer. In this paper detail an overview of SMS transmission and how to apply security on SMS to transfer from one point to another point.

Key words*: Refer the Acronyms section in this paper*

1. Introduction

The point-to-point SMS provides a mechanism for transmitting "short" messages to and from wireless handsets. This service makes use of a short message service center (SMSC) which acts as a store and forward system for short messages. The wireless network provides transport of short messages between the SMSCs and wireless handsets. In compare to existing text message transmission services (such as alphanumeric paging), the service elements are aimed to provide guaranteed delivery of text messages to the endpoint [1, 2, 3].

A differentiating characteristic of the service is that a vigorous mobile handset is able to receive or submit a short message at any time, self-governing of whether or a voice or data call is in progress. SMS also guarantees delivery of the short message by the network. Temporary failures are identified, and the short message is stored in the network until the target becomes available [3, 4].

SMS is considered by out-of-band packet delivery and low-bandwidth message transfer. Initial applications of SMS focused on excluding alphanumeric pagers by permitting two way general purpose messaging and notification services, primarily for voice mail. As networks technology matured, a diversity of services were introduced like electronic mail and fax integration, paging integration, interactive banking, and information services such as stock

ISSN: 2005-4246 IJUNESST

quotes. Wireless data applications include downloading of SIM cards for activation, debit, and profile editing purposes. Now days, SMS is playing vital role in banking, advertisement sector and validation Purpose. In this paper, we are consider, the application SMS to control fraud applying security mechanism.

2. Network Elements and Architecture

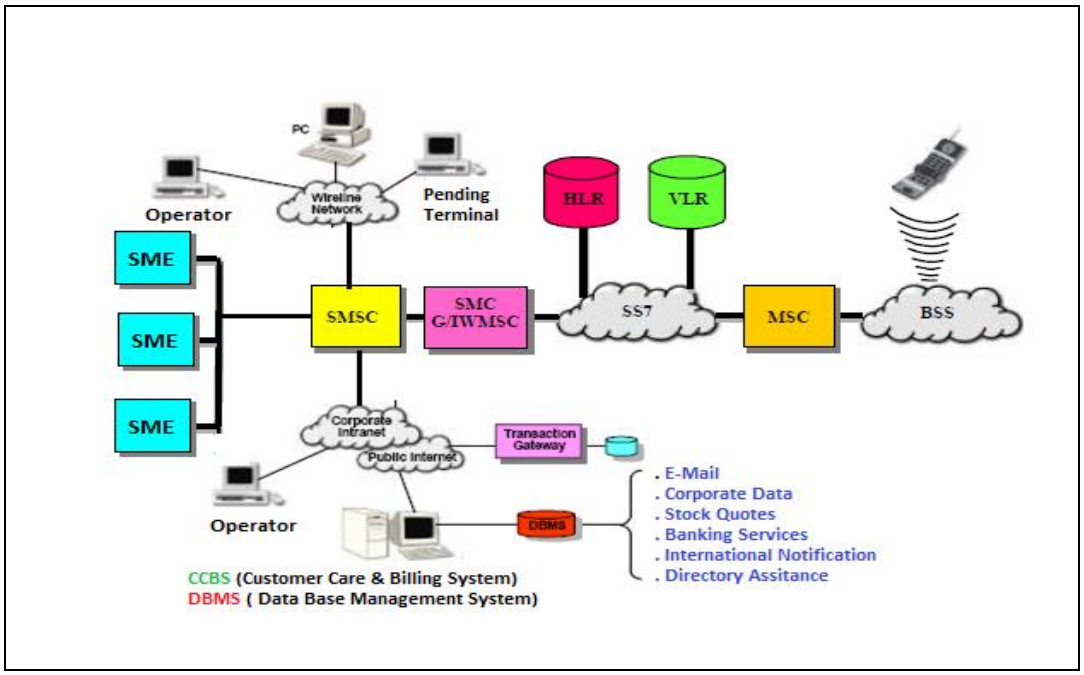

Figure 1. Network Elements and Architecture

2.1 Short Messaging Entities: Short messaging entity (SME) is an object which may receive or send short messages. The SME may be located in the fixed network, a mobile station or another service center.

2.2 Short Message Service Center: Short Message Service Center (SMSC) is liable for the relaying, store-and forwarding a short message between an SME and mobile station.

3.3. SMS-Gateway/Interworking Mobile Switching Center: The SMS gateway (SMS-GMSC) is an MSC capable of receiving a short message (SM) from an SMSC, interrogating a home location register (HLR) for routing information, and delivering the short message to the "visited" MSC of the recipient mobile station. The SMS interworking MSC (SMS-IWMSC) is an MSC proficient of receiving a short message from the mobile network and submitting it to the suitable SMSC. The SMSGMSC/ SMS-IWMSC are typically incorporated with the SMSC.

2.4 Home Location Register: The home location register (HLR) is a database used for stable storage and management of subscriptions and service profiles. Upon interrogation by the SMSC, the HLR provides the routing information for the indicated subscriber. The HLR also enlightens the SMSC, which has previously initiated failed short message delivery attempts to

a specific mobile station, that the mobile station is now recognized by the mobile network to be accessible.

2.5 Mobile Switching Center: The mobile switching center (MSC) performs the switching functions of the system and controls calls to and from other telephone and data systems.

2.6 Visitor Location Register: The visitor location register (VLR) is a database that contains temporary information about subscribers. This information is needed by the MSC in order to service visiting subscribers.

2.7 The Base Station System: All radio-related functions are performed in the base station system (BSS). The BSS consists of base station controllers (BSCs) and the base transceiver stations (BTSs) and its primary responsibility is to transmit voice and data traffic between the mobile stations.

2.8 The Mobile Station: The mobile station (MS) is the wireless terminal capable of receiving and originating short messages as well as voice calls. The wireless network signaling infrastructure is based on Signaling System No 7 (SS7). SMS makes use of the mobile application part (MAP) which defines the methods and mechanisms of communication in wireless networks, and uses the services of the SS7 transaction capabilities application part (TCAP). An SMS service layer makes use of the MAP signaling capabilities and enables the transfer of short messages between the peer entities.

3. Signaling Elements

The mobile application part (MAP) layer defines the operations necessary to support the short message service. Both American and international standards bodies have defined a MAP layer using the services of the signaling system No. 7 transaction capabilities part. The American standard is published by Telecommunication Industry Association and is referred to as IS-41. The international standard is defined by the European Telecommunication Standards Institute and is referred to as GSM MAP. The following basic MAP operations are necessary to provide the end-to-end short message service:

• **Routing information request:** Before attempting short message delivery, the SMSC needs to retrieve routing information in order to determine the serving MSC for the mobile station at the time of the delivery attempt. This is accomplished by way of an interrogation of the HLR which is accomplished via the use of the SMS request and send Routing Info for Short Message mechanisms in IS41 and GSM respectively.

• **Point-to-point short message delivery:** The mechanism provides a means for the SMSC to transfer a short message to the MSC which is serving the addressed mobile station and attempts to deliver a message to an MS whenever the MS is registered, even when the MS is engaged in a voice or data call. The short message delivery operation provides a confirmed delivery service. The operation works in tandem with the base station subsystem while the message is being forwarded from the MSC to the MS. Therefore, the outcome of the comprises either success (i.e., delivery to the mobile) or failure caused by one of several possible reasons. The point-to-point short message delivery is accomplished via the use of the Short Message Delivery-Point-to-Point (SMD-PP) and forward Short Message mechanisms in IS-41 and GSM respectively.

• **Short message waiting indication:** The operation is activated when a short message delivery attempt by the SMSC fails due to a temporary failure and provides a means for the SMSC to request the HLR to add an SMSC address to the list of SMSCs to be informed when the indicated mobile station becomes accessible. This short message waiting indication is realized via the use of the SMS notification indicator and set message waiting data mechanisms in IS41 and GSM respectively.

• **Service center alert:** The operation provides a means for the HLR to inform the SMSC which has previously initiated unsuccessful short message delivery attempts to a specific mobile station, that the mobile station is now recognized by the mobile network to be accessible. This service center alert is accomplished via the use of the SMS notification and alert service mechanisms in IS41 and GSM respectively. In GSM networks, the type of messaging service is identified by the protocol identifier information element which identifies the higher level protocol or interworking being used. Examples are telex, group 3 telefax, X.400 messaging, ERMES, and voice telephone. In IS41 networks, the service type is distinguished by use of the teleservice identifier. Basic teleservices include the following:

- Cellular messaging teleservice (CMT)
- Cellular paging teleservice (CPT)
- Voice mail notification teleservice (VMN)

CMT differs from the CPT due to the inclusion of a reply mechanism which enables a user or network acknowledgment to be selected on a per message basis. The user acknowledgment includes a response code which paves the way for powerful interactive services between SMCs.

Many service applications can be employed combining these service elements. Besides the obvious notification services, SMS can be used in one-way or interactive services providing wireless access to any type of information anywhere. Leveraging new emerging technologies combining browsers, servers, and new markup languages designed for mobile terminals, SMS can enable wireless devices to securely access and send information from the Internet or intranets quickly and cost-efficiently.

A generic network infrastructure for realizing the innovative SMS services is depicted in Some of the potential applications of SMS technology, utilizing both MT-SM and MOSM where appropriate:

• **Notification services:** Notification services are currently the most widely deployed SMS services. Examples of notification services using SMS contain the following:

I. **Voice/fax message notification:** which indicates that voice mail messages are present in a voice mailbox; e-mail notification, which indicates that e-mail messages are present in an e-mail mailbox; and reminder/calendar services, which enables reminders for meetings and scheduled appointment.

II. **E-mail interworking:** Existing e-mail services (*e.g.*, SMTP, X.400) can be easily assimilated with SMS to provide duplex e-mail to short messaging.

III. **Paging interworking**: Paging services (*e.g.*, TAP, TNPP, TDP) assimilated with SMS would allow digital wireless subscribers to be accessible via existing paging interfaces.

IV. **Information services**: A wide variety of information services can be provided by the SMS, comprising weather reports, traffic information, entertainment information (*e.g.*, cinema, theater, concerts), financial information (stock quotes, exchange rates, banking, brokerage services etc), and directory assistance.

4. Mobile-Terminated Short Message Sequence Flow Diagram

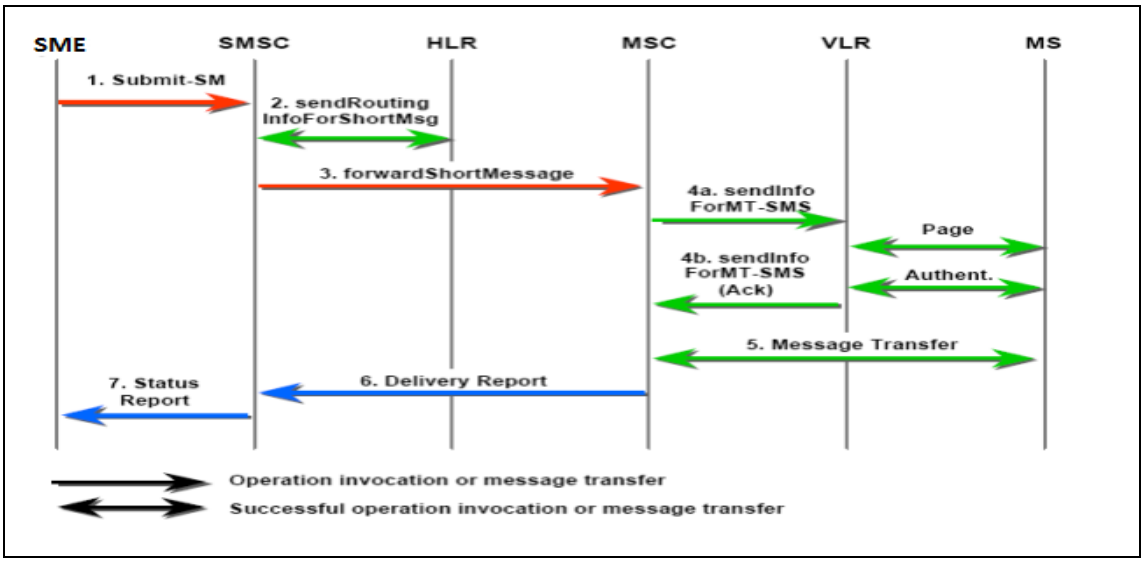

Figure 2. MT-SM Scenario

a) The short message is submitted from the SME to the SMSC.
b) After completing its internal processing, the SMSC interrogates the HLR and receives the routing information for the mobile subscriber.
c) The SMSC sends the short message to the MSC using the forward Short Message operation.
d) The MSC retrieves the subscriber information from the VLR. This operation may include an authentication procedure.
e) The MSC transfers the short message to the MS.
f) The MSC returns to the SMSC the outcome of the forward Short Message operation.
g) If requested by the SME, the SMSC returns a status report indicating delivery of the short message.

4.1. Mobile-Originated Short Message Sequence Diagram Flow

Figure 4 depicts the successful MO-SM scenario. For convenience, the GSM method is shown. However, the IS41 method is similar.

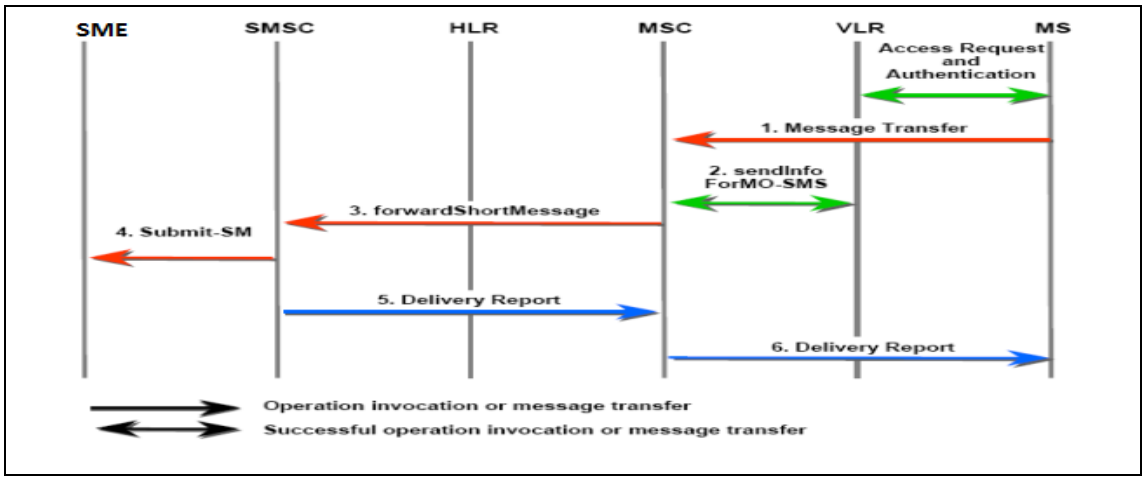

Figure 3. MO-SM Scenario

a) The MS transfers the SM to the MSC.
b) The MSC interrogates the VLR to verify that the message transfer does not violate the supplementary services invoked or the restrictions imposed.
c) The MSC sends the short message to the SMSC using the forward Short Message operation.
d) The SMSC delivers the short message to the SME.
e) The SMSC acknowledges to the MSC the successful outcome of the forward Short Message operation.
f) The MSC returns to the MS the outcome of the MO-SM operation.

5. Implementation

Unprotected communication channels pose serious security vulnerabilities. Thus, it is importantly pertinent that both the mobile applications and the service provider must apply some reliable protective techniques to avoid these assailable vulnerabilities [6, 7]. To avoid security vulnerabilities, the authentication of account we can divided by two part- Public key, private key and code for enable/disable.

Public key user will generate by account holder and register with the bank and account holder will get private key from bank. Public key and private key can we generate by using any of key generating tool. But message send to server in encrypted format and server will decrypt and process based on request. In this process, server first do authentication of user based on public key and private key after that process the request.

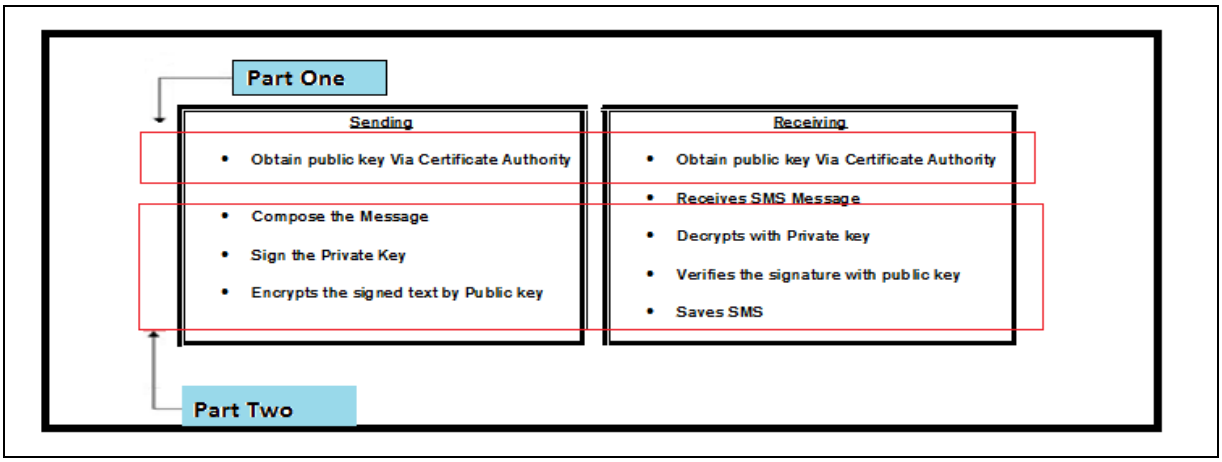

Figure 4. A: Securing SMS Transmission Parts

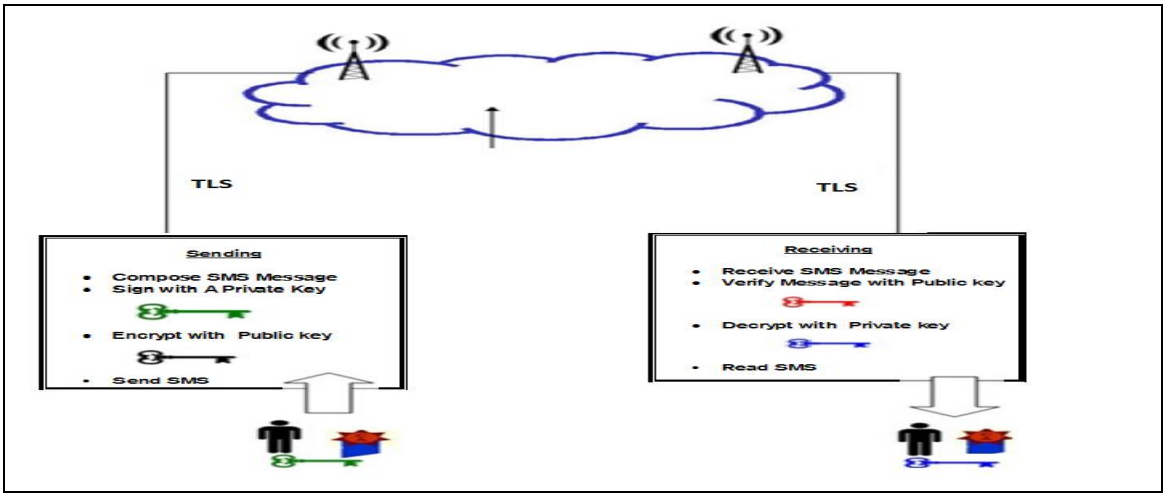

Figure 4. B: Securing SMS Transmission Overview

6. Conclusion

Purchase fraud occurs when a criminal approaches a merchant and proposes a business transaction, and then uses fraudulent means to pay for it, such as a stolen or fake credit card. As a result, merchants do not get paid for the sale. Merchants who accept credit cards may receive a chargeback for the transaction and lose money as a result.

The use of Internet services or software with Internet access to defraud wounded or to otherwise take advantage of them, for example by pocketing personal information, which can even lead to identity shoplifting. A very common form of Internet fraud is the distribution of scoundrel security software. Internet services can be used to present fraudulent solicitations to potential victims to conduct deceitful transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme. In this paper, we have discussed about application SMS to protect your account to defraud victims.

References

[1] Abomhara M, Khalifa O, Zakaria O, Zaidan A, Zaidan B, Alanazi H (2010). Suitability of Using Symmetric Key to Secure Multimedia Data: An Overview. J. Appl. Sci., 10: 1656-1661.
[2] Aziz Q (2006). Payments through Mobile Phone. Emerging Technologies, 2006. ICET '06. International Conference on. pp. 50-52.
[3] Beller MJ, Chang LF, Yacobi Y (1993). Privacy and authentication on a portable communications system. IEEE J. Selected Areas Commun., 11: 821-829.
[4] Hassinen M (2005). SafeSMS-End-to-End encryption for SMS messages. pp. 359-365.
[5] Hwu JS, Chen RJ, Lin YB (2006). An efficient identity-based cryptosystem for end-to-end mobile security. IEEE Trans Wireless Commun., 5: 2586.
[6] Jumaat NB, Zakaria O, Gani A (2008). GSM Mobile SMS/MMS using Public Key Infrastructure: M–PKI. WSEAS Trans. Comput., 7: 1219-1229.
[7] Zheng Y (1996). An authentication and security protocol for mobile computing. pp. 249-257.

Acronyms

AC Authentication Center
AIN Advanced Intelligent Networks
BSC Base Station Controllers
BSS Base Station System
BTS Base Transceiver Station
CDMA Code Division Multiple Access
CMT Cellular Messaging Teleservice
CPT Cellular Paging Teleservice
GMSC Gateway Mobile Switching Center
GSM Global Standard for Mobiles
HLR Home Location Register
MAP Mobile Application Part
MIN Mobile Identification Number
MO-SM Mobile-Originated Short Message
MS Mobile Station
MSC Mobile Switching Center
MT-SM Mobile-Terminated Short Message
SM Short Message
SMD-PP Short Message Delivery Point-to-Point
SME Short Message Entity
SMS Short Message Service
SMSC Short Message Service Center
SMS-GMSC Gateway Mobile Switching Center
SMS-IWMSC SMS Interworking Mobile Switching Center
SMTP Simple Mail Transfer Protocol
SS7 Signaling System 7
TAP Telocator Alphanumeric Protocol
TCAP Transaction Capabilities Application Part
TDMA Time Division Multiple Access
TDP Telocator Data Protocol
TNPP Telocator Network Paging Protocol
VLR Visitor Location Register
VMN Voice Mail Notification

Author

Dr. Manoj kumar jain is Solution Architect in Computer Science at Tata Consultancy Services, Bangalore, India, His current research interests include Fuzzy Logic, Genetic Algorithm, Big Data, Data Mining, Software Engineering.

Anjana Jain is Software Quality auditor in Tech Mahindra, Bangalore, India. Her research interest include Quality and Analytics.