Security for Short Message Peer-To-Peer Protocol

NADELLA PRIYANKA CHOWDARY[1], PAKANATI RAJITHA[2], MUVVA ANEESHA[3], JANJANAM MADHU BABU[4]
[1,2,3,4] *Computer Science and Engineering, Vasireddy Venkatadri Institute of Technology, Andhra Pradesh, India*

Abstract- ***Short Message Service (SMS) has become an extension of our lives and plays an important role in daily chores. SMS is a popular medium for delivering Value Added Services and are suitable for mobile banking, payment reminders, SOS calls, stock and news alerts, railway and flight enquiries etc. These types of messages are normally computer generated messages sent over Short Message Peer-to- Peer (SMPP) protocol. SMPP is an application layer protocol to send messages over TCP/IP connection. The Short Message Peer-to- Peer (SMPP) protocol is a telecommunications industry protocol for exchanging SMS messages between SMS peer entities such as short message service centers and/or External Short Messaging Entities. SMPP protocol has no security measures specified which allows fast delivery of SMS messages in bulk. Compromised messages or loss of messages can cause lot of revenue loss and fatal consequences. A secure SMPP protocol is proposed and implemented by introducing Transport Layer Security (TLS) with SMPP protocol specifications. A client tool is developed to securely connect to the server. Secure Short Message Peer-to- Peer protocol will enhance the security of fast growing messaging and telecommunication world.***

I. EXISTING SYSTEM

SMS text messaging is the most widely used data application in the world, with 2.4 billion active users, or 74% of all mobile phone subscribers. SMS is now a major revenue generator for wireless carriers. SMS are normally computer generated messages sent over Short Message Peer-to-Peer (SMPP) protocol. The Short Message Peer-to-Peer (SMPP) protocol is a telecommunications industry protocol for exchanging SMS messages between SMS peer entities such as short message service centers and/or External Short Messaging Entities. The message generated from ESME is in plain text which can be easily read and modified before it reaches SMSC.

PROPOSED SYSTEM: Short Message Service (SMS) has become an extension of our lives and plays an important role in daily chores. SMS is a popular medium for delivering Value Added Services and are suitable for mobile banking, payment reminders, SOS calls, stock and news alerts, railway and flight enquiries etc. These types of messages are normally computer generated messages sent over Short Message Peer-to-Peer (SMPP) protocol. SMPP is an application layer protocol to send messages over TCP/IP connection. SMPP protocol has no security measures specified which allows fast delivery of SMS messages in bulk. SMPP protocol lacks the basic elements of security that is confidentiality, integrity and endpoint authentication. Secure Short Message Peer-to-Peer protocol is a next step of SMPP to secure transfer of message from ESME to SMSC. SMPP is made secure by implementing it over Transfer Layer Security (TLS). Previously TLS was known as Secure Socket Layer (SSL). Transport Layer Security is cryptographic protocol that provides security for communications over networks such as the Internet.

The TLS protocol allows client/server applications to communicate across a network in a way designed to prevent eavesdropping and tampering. TLS uses the public-and-private key encryption system, which also includes the use of a digital certificate. A client tool is developed to securely connect to the server. Secure Short Message Peer-to-Peer protocol will enhance the security of fast growing messaging and telecommunication world. Secure SMPP is capable of satisfying security parameters of confidentiality, integrity and authentication.

OPERATING ENVIRONMENT

➢ Server-Side:

Processor	-	Pentium –IV
RAM	-	4 GB (min)
Hard Disk	-	1TB
Monitor	-	SVGA

➢Client-Side:

Operating System Windows XP	-	
Internet Speed	-	1.2Mbps
Storage	-	100MB

II. INTRODUCTION

SMS has achieved huge success in the wireless world. Billions of SMS messages are sent every day. SMS text messaging is the most widely used data application in the world, with 2.4 billion active users, or 74% of all mobile phone subscribers. SMS is now a major revenue generator for wireless carriers. It is the text communication service component of mobile communication systems that allow the exchange of short text messages between mobile phone devices. In everyday life most of the messages that we receive are generated from computers running SMS-based application connected to GSM (Global System for Mobile Communications) network. These messages are generated using Short Message Peer-to-Peer (SMPP) protocol over TCP/IP layer. This part of network is unsafe and vulnerable.

This project investigates on the security issues with message send using External Short Message Entity (ESME) over the communication channel. The investigation is aimed to uncover the security shortfalls of SMS using the GSM network and SMPP. The exposure of the security shortfalls has called for a new secure SMS protocol to be designed to enhance security of SMS.

III. PROBLEM DESCRIPTION:

Reliability on SMS-based services has increased a lot. Mobile banking, mobile customer services, railway enquiry system and many more such services use SMS as their primary mode of interaction with their customers. The intelligent application called External Short Messaging Entity (ESME) running on computers interacts with the users to give requested information. For instance: For enquiring the status of the train following transactions are performed. User sends a message to 139

User SMS: "Train <Train Number> <DOJ***DDMMYY> <Station Code>

The message travels through the GSM network to the SMSC which forwards the message to the ESME with the destination unique number "139". Here the message is parsed and checked for matching query. The response is generated after querying the database and forwarded to the receiver's mobile. The message generated from ESME is in plain text which can be easily read and modified before it reaches SMSC. Any wrong information received by the recipient can prove fatal for the user.

To exploit the popularity of SMS as a serious business bearer protocol, it is necessary to enhance its functionalities to offer the secured transaction capability. Data confidentiality, integrity, authentication, and nonrepudiation are the most important security services in the security criteria that should be taken into account in many secure applications. However, such requirements are not provided by the traditional SMS messaging. SMS spoofing and SMS spamming which are increasing rapidly are also addressed in this report.

Short Message Service (SMS)

SMS is a technology that enables the sending and receiving of messages between mobile phones. SMS first appeared in Europe in 1992. It was included in the GSM (Global System for Mobile Communications) standards right at the beginning. Later it was ported to wireless technologies like CDMA and TDMA. The GSM and SMS standards were originally developed by ETSI. ETSI is the abbreviation for European Telecommunications Standards Institute. Now the 3GPP (Third Generation Partnership Project) is responsible for the development and maintenance of the GSM and SMS standards.

As suggested by the name "Short Message Service", the data that can be held by an SMS message is very limited. One SMS message can contain at most 140 bytes (1120 bits) of data, so one SMS message can contain up to:

- 160 characters if 7-bit character encoding is used. (7-bit character encoding is suitable for encoding Latin characters like English alphabets.)

- 70 characters if 16-bit Unicode UCS2 character encoding is used. (SMS text messages containing non-Latin characters like Chinese characters should use 16-bit character encoding.)

SMS text messaging supports languages internationally. It works fine with all languages supported by Unicode, including Arabic, Chinese, Japanese and Korean.

Concatenated SMS Messages/ Long SMS Messages

One drawback of the SMS technology is that one SMS message can only carry a very limited amount of data. To overcome this drawback, an extension called concatenated SMS (also known as long SMS) was developed. A concatenated SMS text message can contain more than 160 English characters. Concatenated SMS works like this: The sender's mobile phone breaks down a long message into smaller parts and sends each of them as a single SMS message. When these SMS messages reach the destination, the recipient mobile phone will combine them back to one long message.

The drawback of concatenated SMS is that it is less widely supported than SMS on wireless devices

EMS (Enhanced Messaging Service)

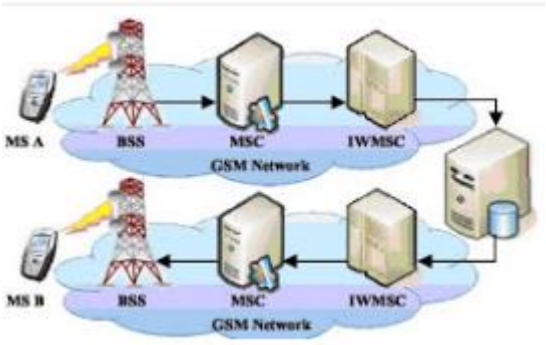
Besides the data size limitation, SMS has another major drawback -- an SMS message cannot include rich-media content such as pictures, animations and melodies. EMS (Enhanced Messaging Service) was developed in response to this. It is an application-level extension of SMS. An EMS message can include pictures, animations and melodies. Also, the formatting of the text inside an EMS message is changeable. For example, the message sender can specify whether the text in an EMS message should be displayed in bold or italic, with a large font or a small font.

The drawback of EMS is that it is less widely supported than SMS on wireless devices. Also, many EMS-enabled wireless devices only support a subset of the features defined in the EMS specification. A certain EMS feature may be supported on one wireless device but not on the other.

SMS Architecture:

SMS Architecture If any mobile user looking for the way how a SMS takes a rout to reach one user's mobile to another associate mobile user, So user should must aware about SMS architecture which plays a very important role. Anyone can easily find out the way by takes a look to understand GSM, illustrated figure below. At the beginning, if a user sends a SMS to his buddy, the SMS first deliver from the MS which is know as Mobile Station A to SM-SC(Short Message Service Center) Via the Base Station System (BSS), and then it catch up to the Mobile Station centre(MSC) and finally combine with Interworking MSC(IW-MSC). The use of Short Message Service Center (SM-SC) to carry ahead the SMS message to the GSM network through a definite GSM-MSC called the Short Message Service gateway MSC (SMS-GMSC). The SM-SC is allowed to link with several GSM networks and to several SM-GMSCs in a GSM network. The SMS-GMSC come across the contemporary MSC of the message acceptor and then step ahead the SMS message to that Mobile Station centre, pursue the Global System for Mobile Communication (GSM) roaming protocol. The MSC then Publish the SMS through the Base Station System (BSS) to the destination MSB.

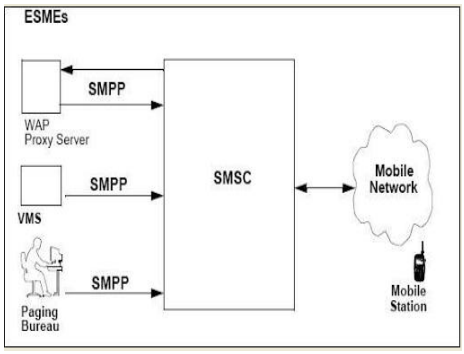
The SMS bearer service is the portion of the SMS system responsible for delivery of messages between the message center and mobile user equipment. The bearer service is provided by the SMS Transport Layer and the SMS Relay Layer. The SMS Transport Layer is the highest layer of the bearer service protocol. The Transport Layer manages the end-to-end delivery of messages. In an entity serving as a relay point, the Transport Layer is responsible for receiving SMS Transport Layer messages from an underlying SMS Relay Layer, interpreting the destination address and other routing information, and forwarding the message via an underlying SMS Relay Layer. In entities serving as end points, the Transport Layer provides the interface between the SMS Bearer Service and the SMS Teleservice. The SMS Relay Layer provides the interface between the Transport Layer and the Link Layer used for message transmission.



SMPP: SMPP is an open, industry standard protocol designed to provide a flexible data communications interface for the transfer of short message data between External Short Message Entities (ESME), Routing Entities (RE) and Message Centers. A Message Centre (MC) is a generic term used to describe systems such as a Short Message Service Centre (SMSC), GSM Unstructured Supplementary Services Data (USSD) Server, or Cell Broadcast Centre (CBC).

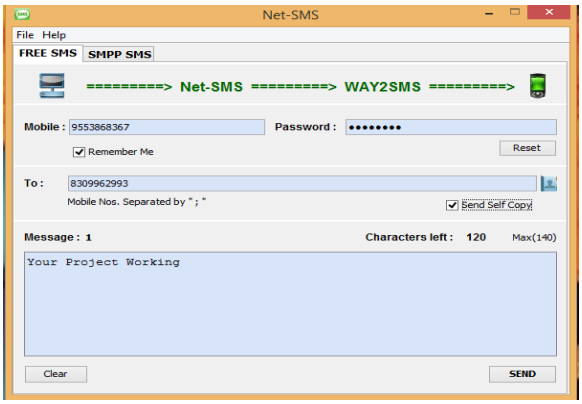
An ESME typically represents a fixed network SMS client, such as a WAP Proxy Server, E-Mail Gateway, or Voice Mail Server. It may also represent a Cell Broadcast Entity (CBE). The ESMEs are the starting points (the source) and the end points (the receiver) for SMS messages. They always communicate with a Short Message Service Center (SMSC) and never communicate directly with each other. An ESME can be a Mobile telephone. Depending on the role of the mobile phone in the communication we can talk about two kinds of SMS messages Mobile Originated (MO) messages and Mobile Terminated (MT) messages. MO messages are sent by the mobile phone to the SMSC. Mobile terminated messages are received by the mobile phone. The two messages are encoded differently during transmission.

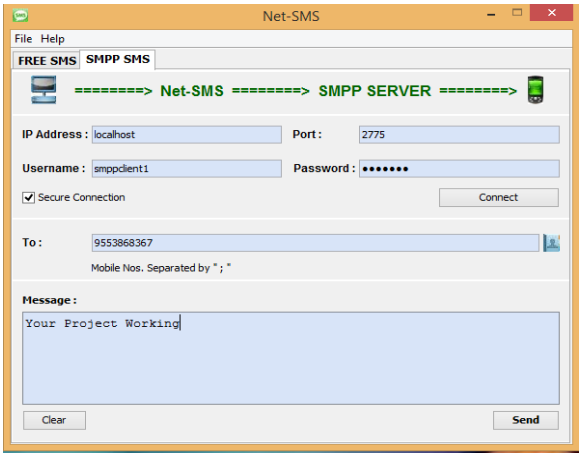
A Routing Entity (RE) is a generic term for a network element that is utilized for MC to MC, and ESME to MC message routing. A RE has the ability to emulate the functionality associated with both a MC and an ESME. To an ESME, a RE appears as a MC and to a MC, a RE appears as an ESME. A carrier may utilize REs to hide a network of Message Centers, presenting only the REs as the external interface point for ESMEs.



Security (TLS) with SMPP protocol specifications. Secure SMPP is capable of satisfying security parameters of confidentiality, integrity and authentication. A simple Secure SMPP protocol based client tool is implemented to send secure messages to SMSC. A little overhead performance cost is charged to send secure messages using Secure SMPP protocol as compared to normal SMPP protocol. Secure SMPP can be easily deployed to applications running in banks and other services.

IV. RESULT





The Client tool is named as Net-SMS. Net-SMS also consist of features where user can send messages using SMPP protocol as well as Secure SMPP protocol as discussed in previous section. Net-SMS is a very rich Java desktop based application. It is developed using Java Swing. Net-SMS can be proved to be very useful for any class of people who is in need to communicate too many people

REFERENCES

[1] GSM 03.40 Technical realization of the Short Message Service (SMS), Retrieved on May 05, 2010, from http://www.3gpp.org/ftp/Specs/html-info/0340.htm.

[2] The SMS Forum, Retrieved on May 15, 2010, from http://www.smsforum.net.

[3] SMPP Protocol, Open source, Retrieved on May 1 http://opensmpp.logica.com/.

[4] Short Message Peer to Peer Protocol Specification v3.4, Retrieved on April 10, 2010, from http://www.smsforum.net.

[5] Short Message Peer to Peer Protocol Specification v5.0, Retrieved on April 10, 2010, from http://www.smsforum.net.

[6] Short Message Service Center, Retrieved on May 17, 2010, from http://www.ozeki.hu/.

[7] Roshan D'Souza, Santhosh Kumar, Uttara Kumari, Protocol implementation for Short Message Service over IP