International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Improving the Security of SMPP Protocol using TLS

Akash R. Kotecha[1], H. P. Channe[2]

[1]Computer Engineering Department, Pune Institute of Computer Technology, Pune, India

[2]Professor, Computer Engineering Department, Pune Institute of Computer Technology, Pune, India

Abstract: ***In human life, Communication medium plays an important role in sharing the information. At many times, information is confidential so need to maintain the confidentiality of information is necessary. Short Message Service (SMS) has become an important way of communication for mobile users. SMS contains plain text which is transmitted to end user through layers of network. Nowadays, SMS is used widely for value added services and is suitable for versatile managing account, installment updates, SOS calls, stock and new cautions, route and flight enquiries so forth. These sorts of messages are generally created using computer application and are sent over Short Message Peer-to-Peer (SMPP) Protocol. SMPP uses TCP/IP connection to send messages over application layer. SMPP convention has no efforts to establish safety indicated which permits quick conveyance of SMS messages in mass. Sometimes messages may be lost in a network which may effect on the revenue loss or information leaked to third party. In this paper, we have proposed a way to secure the messages using Transport Layer Security (TLS) protocol. We have modified the structure of TLS for SMS submission.***

Keywords: Short Message Service, Short Message Peer to Peer, Transport Layer Security, Cryptography.

1. Introduction

Short Message Service (SMS) is the most used communication medium by mobile users. 80 percent of world population is using mobile phones with 90 percent coverage in year 2010 [8]. Most mobiles are used for making telephone calls. Another feature that is begun to fully exploit is SMS. First text message was sent in 1992. In SMS, User gets the notification of message state when queried about status of message i.e., Message is delivered or rejected. So it makes the communication very fast as compared to other communication medium. In a single message, 160 characters can be sent as a plain text. If it exceeds the size limit, then the message is divided in the size of 153 characters per segment and 7 characters are used for header information. When used sends a message from External Short Messaging Entity (ESME), it is first received by SMSC. SMSC store's the message until it is delivered to receiver in defined maximum attempts. After it reaches its maximum limit of tries to send a message, SMSC rejects the messages. SMSC works on Store and Forward technology. Once the message is delivered to receiver, SMSC gets a notification from receiver which tells about delivery of SMS. SMSC stores the messages for the audit and log purposes. As SMS is not encrypted, operator of SMSC can see those messages and can misuse them. Operator can also modify the messages. So this makes SMS vulnerable to third party attacks and misuse of the information.

Short Message Peer to Peer (SMPP) Protocol allows sending messages in bulk. This protocol works between External Short Messaging Entities (ESME) and Short Message Service Center (SMSC). This is an application layer protocol which makes it possible to send messages very fast. Now days, SMS is used widely for value added services such as enquiry, mobile banking and customer service. ESME which is intelligent application running on computer uses SMPP to send SMS to its users. Messages are of two types: Mobile Terminated (MT) and Mobile Originated (MO). Mobile Terminated messages are sent by SMSC to mobile. Mobile Originated messages are sent by mobile phones to SMSC.

SMS services are operated using push and pull messages. Push messages are those that the administrator decides to convey to a client's cellular telephone, without the client launching a solicitation for the data. For example, Push messages can be marketing messages, ATM messages indicating withdrawal of money or transaction. One time password is also an example of push messages. Pull messages are those that are started by the client, using a cellphone, for acquiring data or performing an exchange in the financial balance. Example of pull messages include account balance enquiry or information related to flight or train enquiry [1].

TLS provides end to end authentication and maintains confidentiality of data by encrypting the data using negotiated cipher. TLS process consists of 5 steps: 1) Fragmentation 2) Compression 3) Attaching MAC 4) Encryption 5) Attaching TLS header. In our proposed system we have removed Fragmentation and Compression steps so as task of sending SMS will become fast. In addition, we have used only efficient and more secure algorithms from the cipher suit of TLS.

The rest of the paper is organized with the sections as follows. Section 2 gives the literature survey of previous work done regarding the SMS security. Section 3 gives the problem statement. Section 4 gives the Mathematical Modeling of problem. Section 5 gives the Proposed System. Section 6 gives the conclusion and future work.

2. Related Work

Text messaging is used on a large scale to send information

or message to other people. We can do bunch of different things as a sender and receiver. SMPP Protocol provides an interface between External Short Messaging Entity (ESME), Routing Entities (RE), and Message Centers. The transport of operation between entities in the session is performed over a TCP/IP connection. The port usually used for this operation is 2775. Four types of operations are categorized as: 1) Session management 2) Message submission 3) Message delivery 4) Message broadcast 5) Ancillary operation [7]. Session management manages session between the SMSC and ESME. It also handles unexpected errors. Message submission deals with task of submitting the message to SMSC. Message delivery deals with delivering messages or delivery reports to ESME. Message broadcast deals with cell broadcast service within a message center. Ancillary operation deals with various operations such as replacing message content, cancelling message, querying message etc.

There are certain problems with SMPP protocol. First is Man-in-middle attack. In this the attacker makes an independent connection between the victims and relay messages making them believe that they are talking directly to each other over a private connection whereas attacker can control that conversation. Second is Zero confidentiality. There is no confidentiality of the information which is communicated over the connection. Information transmitted over the connection is sent as a plain text and it does not authenticate the receiver. So there is a vital loss of confidentiality. Third is Message Tampering. As the connection with SMSC is can be read by any attacker, it may lead to message adulteration and tampering. Fourth is No endpoint authentication. As the attackers can get the login id and password easily due to loss of confidentiality, he can misuse the service by showing himself as authenticate user.

Saurabh Samanta et. al. [1] discussed about a Secure Short Message Peer-to-Peer Protocol using TLS. They developed a client tool to securely connect to the server securely and authenticate the communication. It enhanced the security of SMPP Protocol. But there is an overhead performance cost is charged to secure the message.

Patrick Traynor et. al. [2] uses a combination of modeling and simulation to demonstrate the feasibility of targeted text messaging attacks. They developed five different techniques from resource provisioning and queue management. Techniques used in this paper can eliminate or extensively mitigate even the most intense targeted text messaging attack.

Chao-Wen Chang et. al. [3] proposed a secure short message communication protocol. Protocol proposed by this paper is an application level protocol build on standard SMS communication protocol using public key authentication and key agreement. The effective payload rate of proposed system can reach 91.4\%. Proposed system meet requirements as confidentiality, integrity, non-deniability, and identity authentication.

Dr. Shaimaa et. al. [4] proposed a model for encryption and authentication. It involves suitable encryption and decryption algorithm using asymmetric cryptography and suitable HMAC algorithm as a message digest. Proposed model provides the confidentiality, integrity and authentication using modified RSA-2048 and SHA-256.

Ning Lianju et. al. [5] studied some widely used protocols and discussed advantages and disadvantages of it. They proposed a new protocol to secure the SMS transmission. Proposed protocol improves both the structure and modules of previous protocols. Compared with others, proposed protocol is safer due to use of signature verification.

Abdullah A. Abdullah [9] proposed an approach consist of two steps, firstly, SHA-1 authentication is used to generate a message digest that is combined with previous message digest and a shared secret key to form initial key stream. Secondly, this key will be an input to mathematical equation which is one time pad to encrypt the original message text.

3. Problem Statement

To provide a secure connection between the server and client by using TLS protocol and authenticate the communication. SMPP is an application layer protocol and it is not intended to offer transport facility. It is therefore responsibility of underlying network connection will provide reliable data transfer.

3.1 Scope

- Our work is related to SMPP protocol
- We provide the secure connection between ESME and SMSC
- We will be targeting the Endpoint authentication issue and Confidentiality issue.

4. Mathematical Model

Input: Message in text format.
Output: Encrypted text message using TLS.
System:
$S = \{s, e, X, Y, f, f_f, c\}$
$X = \{Input\} = \{M, C_S\}$
$M = \{M_1, M_2, M_3, \ldots, M_{255}\}$
$Y = \{Output\} = \{E_M, D\}$
$D = \{Delivery\ Receipt\} = \{Message\_id, Submit\_date, Done\_date, Status, Text, TON, NPI\}$
$c = \{Connection\ Type\} = \{t, r, t_r\}$
$f = \{Functions\} = \{f_{nc}, f_a, f_s, f_e\}$
$f_f = \{Friend\ Functions\} = \{f_{en}, f_q, f_c, f_{re}\}$
Where,
M is Message. It can consist up to X characters depending upon the data coding used.
C_S is Cipher Suit.

An example of a cipher suite is TLS_RSA_WITH_DES_CBC_SHA, where TLS is the protocol version, RSA is the algorithm that will be used for the key exchange, DES_CBC is the encryption algorithm (using a 56-bit key in CBC mode), and SHA-1 is the hash function. Microsoft applications typically specify RSA as the key exchange algorithm, RC4 as the encryption method, and MD5 as the Message Authentication Codes.

E_M is Encrypted Message.
D is Delivery receipt received from SMSC.
c is Connection type which can be of transmitter, receiver or transceiver.

- Cipher Suit Negotiation function:
  f_{nc} : Send(C_S) -> SMSC
  It negotiates suitable cipher suit with server and client.
  Where,
  C_S= {CryptographicAlgorithm, key_sizes}.

- Function to authenticate SMSC:
  f_a: if (server_pk) is valid -> Ex(Secret_Key)
  This function validates server public key and if it is correct then it exchanges secret key with server.

- Function to encrypt SMS:
  f_e: encrypt(f_s, Secret Key)
  It encrypts the message using Secret Key.

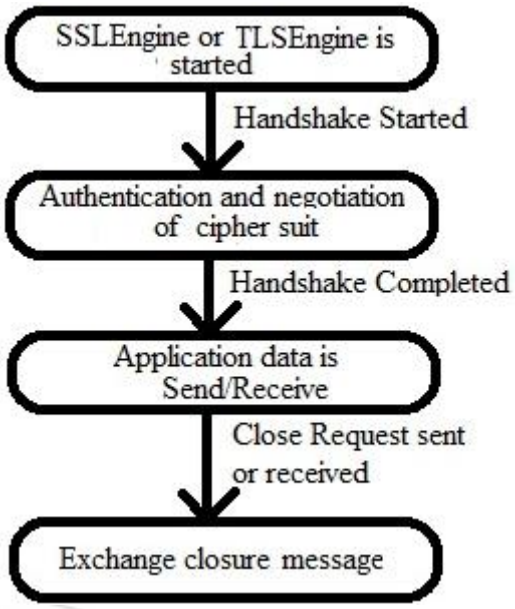
- Function to send SMS:
  f_s: SubmitSM(parameters)
  Where, parameters contain following fields,
  - Message_id is unique id allocated for every message.
  - Text contains first 20 characters of message body.
  - Priority contains the priority assigned to the message.
  - registered_delivery is a flag which tells whether to send delivery notification or not.
  - optional_parameters contains the additional parameters added by client.
  - TON is Type of Number.
  - NPI is Numbering Plan Indicator.
  - data_coding contains the encoding algorithm for text.

Success: Messages are securely transmitted over communication channel using SMPP protocol.
Fail: Messages are not sent to the SMSC securely.

5. Proposed System

SMPP protocol does not provide any security to the messages sent over the communication. In addition to that, Endpoint authentication is also not provided. Proposed system in this paper combines the SMPP and TLS to provide a more secure and reliable connection to send messages between server and client.

TLS is protocol that provides security for communication using cryptography over internet. TLS protocol as defined in RFC 5246. TLS maintains the confidentiality and provides endpoint authentication over the internet using cryptography. We have modified the header structure of TLS. In TLS Header, Compression Length, Minor Version, Major Version, and Content Type fields are present. As we are removing fragmentation and compression steps so we are removing the Compression Length field from the Header. In addition, we have only used more secure and efficient cipher suits from the TLS cipher suit.



6. Results

Results can be shown using the following graph. Overhead in existing system is upto 12%. Proposed system minimizes this overhead upto 10% by removing fragmentation, compression steps and modifying the header structure.

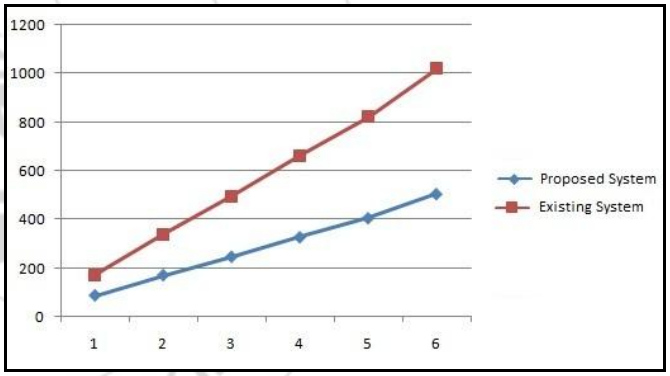


Figure 1: Comparison with existing system

7. Conclusion

Use of SMS has increased a lot. Now days, SMS is used widely for communicating the information to the people. The issue of security to maintain the confidentiality of SMS is very important. SMPP Protocol sends messages as a plain text and does not provide any kind of security to the message. So it is secured by using TLS protocol. In our project, We have reduced the overhead on sending a SMS. Overhead in our proposed system comes around 10%.

References

[1] S. Samanta, R. Mohandas, A. R. Pais, "Secure Short Message Peer To Peer Protocol," *International Journal of Electronic Commerce Studies*, Vol. 3, No. 1, pp 45-60, 2012.
[2] P. Traynor, W. Enck, P. McDaniel, Thomas La Porta, "Mitigating Attacks on Open Functionality in SMS-

Capable Cellular Networks," *IEEE/ACM Transactions On Networking*, Vol. 17, No. 1, February 2009.
[3] Chao-Wen Chang, Heng Pan, Hong-Yong Jia, "A Secure Short Message Communication Protocol," *International Journal of Automation and Computing* vol. 5, no. 2, pp. 202-207, April 2008
[4] Dr.Shaimaa H. Shaker, Dr.Hassan A. Jeiad, Fatimah A. Hassan,``Propose a model for Securing SMS," *International Journal of Scientific and Engineering Research*, vol. 5, no. 4, pp. 90-95, April-2014.
[5] Ning Lianju and Feng Xin, Lichi Sun, ``A Secure Protocol for Efficient SMS Transmission and Management," *Journal of Networks*, vol. 8, no. 9, pp. 2171-2178, September 2010
[6] Short Message Peer to Peer Protocol Specification v3.4
[7] Short Message Peer to Peer Protocol Specification v5.0
[8] Jeff Brown, Bill Shipman, and Ron Vetter, ``SMS: The Short Message Service," *IEEE Journals and Magazines*, vol. 40, no. 12, pp. 106-110, December 2007.
[9] Abdullah A. Abdullah, "Authenticated and Secure End-to-end Communication Channel using SMS Messages," *Raf. J. of Comp. and Math's*, vol. 6, no. 1, pp. 209-222, 2009
[10] Manoj Patil, Prof. Vinay Sahu, ``A Survey of Compression and Encryption Techniques for SMS," *International Journal of Advancements in Research* and Technology, vol. 2, no. 5, pp. 459-464, May-2013.
[11] Muhammad Waseem Khan, ``SMS Security in Mobile Devices: A Survey," *Int. J. Advanced Networking and Applications*, vol. 05, no. 02, pp. 1873-1882, 2013.
[12] Sean Turner, ``Transport Layer Security," *IEEE Computer Society*, vol. 18, no. 6, pp. 60-63, October 2014
[13] Amir Herzberg, Haya Shulman, ``Cipher-Suite Negotiation for DNSSEC: Hop-by-Hop or End-to-End," *IEEE Computer Society*, vol. 19, no. 1, pp. 80-84, February 2015
[14] Akash Kotecha, Prof H. P. Channe, ``A Survey: Security of SMS and Current Approaches," *International Journal of Computer Technology and Applications* vol. 6, no. 1, pp. 147-150, Jan-Feb 2015.

Author Profile

Akash R. Kotecha received B.E. degree in Computer Science Engineering from JNEC, Aurangabad and currently persuing his M.E. degree in Computer Engineering from Pune Institute of Computer Technology, Pune. His interest is in security.

Prof. H. P. Channe is an Assistant Professor in Computer Engineering Department at Pune Institute of Computer Technology, Pune. Her interest is in networks and security.