

IMPLEMENTING SECURITY IN MOBILE COMMUNICATION

Dinesh Sripuram¹, KalyanChakravarthyPottimurthy², Nikhil Nimmagadda³,

Rohitha Saguturu⁴, PraneethBhumireddy⁵

^{1,2,3,4,5}Department of CSE, KL University, Andhra Pradesh, India

¹sripuramdineshreddy@gmail.com

Abstract: These days everyone is using Short Message services(SMS) to remove the difference between far and near because there exist a guaranteed delivery, people use these SMS on their daily basis for connectivity. As Technology play a key role in present era not only living people although information Technology are also utilizing these services. But these exist some data loss by attackers technically known as threads they try to steal the data and used as unauthorized person some these threads are Man in the Middle, Denial of Service (dos), SMS Spoofing etc[1]. Therefore to resist these attacks in mobile systems we have planned a structure which can secure both man and computerized data. This construction can be achieved Through HTTPS for secure key exchange. By using authentication and confidentiality we try to send reply message by utilizing Message Digest (MD5) and try to achieve Integrity so that we can safe guard the data from attacks.

Keywords: SMS, Integrity, confidentiality, authentication, HTTPS, Man-In-The-Middle Attack.

1. Introduction

Generally most of us today using SMS as a daily routine but technically SMS are distinct as wireless services which is worldwide acknowledged for broadcast of alpha numeric records between two mobile users. These days mobile numbers can be measured as customer secondary uniqueness and service providers use it to switch over a vital in sequence[1]. Even though SMS are computerized messaging, complete SMS prospective was not reached because there exist

safety weakness in carry as well as cargo space maintaining which would be attacked by Man In The Middle (MIME) in the direction of performing the unauthorized actions on behalf of original user. As we are using GSM Network architecture there are some point need to be know about the transmissions and their security issues in segment II and segment III. The presented safety solutions are discussed in segment IV. The key defense thread that is Man In The Middle (MITM) assault is discuss in segment V can be solved by SSL and HTTPS as solutions to MITM[1]. In this we thought about each and every part of message transmission that is held by achieving Integrity. The networks are one that played a key role in data transmissions because they are widely connected throughout the world depend on technology these networks are also get updated from past such as 1G,2G,3G,3.5G,4G. The latest updated version of networks is 4g-Long Term Evolution (LTE), but we are doing this project on 2G networks i.e. Global System for Mobile Communications (GSM) which is combination of both Time Division Multiple Access (TDMA) and Frequency Division Multiple Access (FDMA).

2.GSM Architecture and Work Flow

In this segment we are going to know about the hardware components that are being employed in this network. GSM Architecture and Network Component is definite by following SMS operation over set of connections.

2.1. Structural Component Description

SMS has fail-safe delivery and similar accessibility to know how this is done we have to

look deeper imminent, machinery involved in SMS communication are describe beneath.

2.1.1 Mobile Station (MS):- Mobile phone position is defined as back-to-back visual display unit device that is used to obtain and store up the short message services. The term mobile station is used for mobile phones and GSM modems.

2.1.2 Short Message Service Centre (SMSC):- SMSC is SMS member of staff serving at table reside inside operator system accountable for storage, reception as well as forwarding and deliverance of SMS among end users[6].

2.1.3 Base Station System (BSS):- BSS is element of mobile system which is accountable for traffic management along with signaling to structure switching system and base system. They transmit the voice and data signals from one end user to another end user over a precise geological region.

2.2 SMS Transmission

At present we can distinguish how the operations of MS, SMSC and BS are being executed and show how SMS is being communicated between two subscribers.

- i) Mobile System send message to nearest base station using regular broadcast and response control called on-The-Air interface.
- ii) From Base location these SMS are forward to nearest SMSC by the help of signaling synchronization channel SS7.
- iii) Basis SMSC sends the data to determined SMSC.
- iv) After querying target position, SMSC send the data message to nearest base station of the destination by using synchronization channels SS7. By using On-The-Air interface, SMS arrive at its target and then a release report is initiated back to the correspondent.

2.3 Modes of Sending

SMS can be sent in many modes mainly they are of three types building block mode, manuscript mode, PDU mode. Each approach has its own payback and drawbacks.

2.3.1 Block mode: In block mode they might loss of data happens when we try to send long message such as 64 bit data so to avoid these loses we try to split the data into blocks and send them from source to destination.

2.3.2 Text mode: In this text mode we convert the message of size equal to 160 characters into ASCII values of 7 bit representation, This mode also requires a special parameter like SMSC digit before distribution and getting messages.

2.3.3 PDU mode: In this method the message be compressed into some packet data units and these packets can be compressed up to a certain limit so that large amount of message can be sent at a time with more flexibility.

2.4 Imperfection

SMS was calculated without any safety considerations when compare to right to be heard calls which shares hush-hush key at initial stages. Security might not be a key obligation primarily but today SMS hold some important data like passwords, bank accounts, ATM pins, Emails, reset codes etc. most of the messages are transmitted through networks, monitor by organization and still alter before deliverance to avoid this problem several researchers proposed a frame work to establish confidentiality for communications but still there might exist man in the middle assault.

3. Security Issues

Security can be achieved by three main aspects they are authentication, confidentiality and integrity lets discuss in brief about them

3.1 Authentication: This states the guaranteed of data that was sent by the original sender before sending data it verifies and gives permissions only to the particular sender to transmit the message to the destination this process is known as authentication[2].

3.2 Confidentiality: The process which uses to cover the information to avoid the external attacks that happens during the transmissions[3] and this hiding can be achieved only by encryption techniques so that only the one who sends and the one who receives can understand the message inside it contained.

3.3 Integrity: It is a process of Transmitting the flow of data over a secured channel so that we can safeguard it from external manipulations there are different methods to check data integrity[4] such as secure hash algorithm (SHA), message digest (MD5).

4. Current Security Solution

Security threads may occur either on transportation or capacity layers as identifiers, to notify these arrangements are proposed.

4.1 Transportation layer

Global system for mobile communication networks uses A5 algorithm to encrypt voice communications before transmissions over a network but some of researchers suggest that there are some new algorithms that can encrypt voice and upgraded protocols to encrypt SMS[5] but we can use these technique because it suggested up gradation if GSM in fractures throughout the world which is not possible.

4.1.1 Proposed Application Layer Solution

Security is applied on this application layer because any message that is transmitting from sender to receiver it has to cross a set of networks to reach the destination during this transmission attack may happened and can modify the content of message. Proposed frame work for secure factor messages on applicant layers as per follows

- Mainly, sender side and client side has to maintain a secret key for secure communications whenever sender tries to send the data first they communicate and set a path for secure transmission and employ some encryption standards to avoid data leakages.
- Second method in this both the client and server side are engaged by the another party(third) to get the keys for encryption & decryption of messages this another party(third) is knows as public key infrastructure and was proposed for securing messages efficiently.

4.2 Man In The Middle Attack

This is a process where a person can obstruct conversation in the middle of sender & receiver and may control the content. There exist many solutions to avoid this man in the middle attack mostly we use third party verification that gives ensure for authentication of clients before correspondence begins.

4.2.1 Resisting Man In The Middle assault

Many safety communications begin with replace of keys moreover by straight sharing or

through allocation only when the transmission path is secured then only we can able to avoid MITM this could be achieved thought by verifying the third party authentications. Instead of using the same channels for keys distribution we have to use multiple channels to transmission of keys so that the attacker cannot able to guess the next step. We also employ HTTPS methods because as we are using GSM networks that are easily accessible to MITM he can able to get the rid of it in order to avoid this we have to maintain a secure protocol such as like HTTPS over GSM networks.

5. HTTPS& SSL

5.1 SS(secure socket) LAYER

SSL may be definite as Cryptographic protocol to may able to supply safety contact above internet. In favor of verification & key interactions it use asymmetric and identical encryptions in favor of privacy and reliability it relays on communication digest system (MD5).

SS Layer is use to supply message among two end systems and is implement above Transport layers. SS Layer consists of two protocols. SSL evidence procedure is use for greetings, Key switch and different armed forces to top coat protocol such as HTTPS. SS Layer use certificate to confirm back-to-back legitimacy by certificate power.

5.1.1 Hyper Text transport Protocol Secure (HTTPS)

HTTPS is as request detailed execution of protocol in excess of SS Layer[1]. It is wont to safety message among server and client in excess of net, with security by an intermediary identified as certification authority. HTTPS provide protection beside MIT assault by enable 2 manner coding which discourage meddling, eavesdrop as well as information fake. For facilitate HTTPS examine to a web site, hosting group wants to pay for certificate as of certification ability for necessary web site. Web page requirements HTTP knowledge over port 80 and port 443.

5.2 MITM Attack on SS Layer

The only attacks that can be done on SSL are SSL stripping and SSL sniffing attacks

5.2.1 SSL Sniffing Attacks

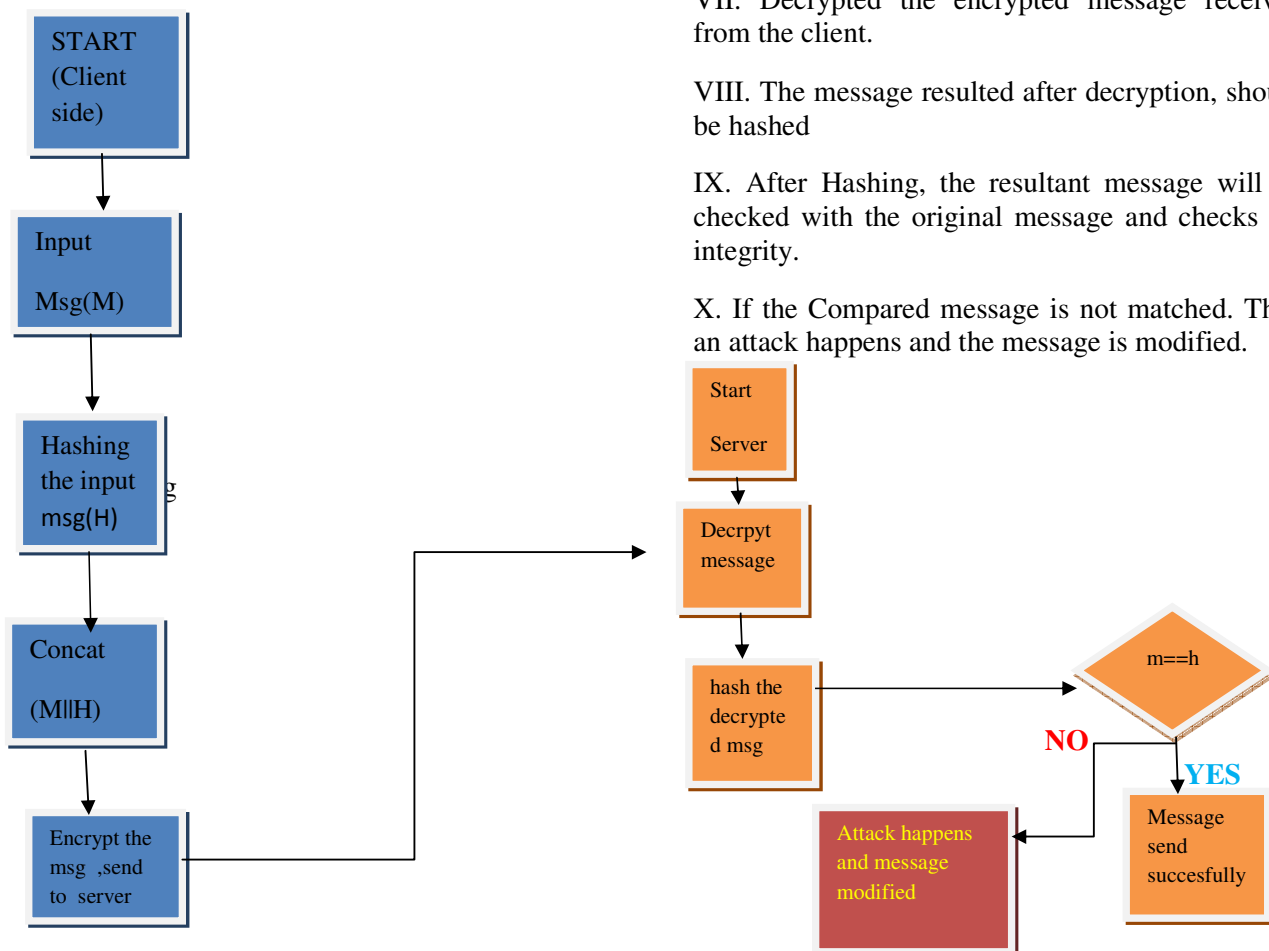
In SS Layer, man-in the middle sniff recognition packet of SS Layer message, sender reply SS Layer credential to receiver that is

intercept by man in the middle and a self signed credential is forward to receiver. customer page associates shopper concerning for solid certificate[6], excluding immobile several folks be set up ignore the alert and continual their schedule procedure, lacking knowing the truth that their non-public data is perceptible toward Associate in Nursing eavesdropper.

5.2.2.SSL Stripping Attacks

In SS Layer attacks, eavesdropper system redirect check among receiver and sender. while consumer requirements a few web site mistreatment straightforward communications protocol request, sender sends back control to customer browser. MIT catch this demand and redirect to HTTP Secure on its engine, anything contented as of sender is acknowledged in excess of HTTP Secure, is transformed to communications protocol information and send to consumer by MIT, receiver cant observe this attacks except he was convinced that he should take delivery of a safety sheet.

6. Methodology



6.1 Algorithm

The below algorithm is used to check the integrity of the message while communicating between client and server.

****CLIENTREQUESTS****

I. Establish the connection between client and server.

II. Input the message from client side.

III. The input string message should be reversed and stored in the array named mid[].

IV. The input string and the mid[](Reverse of the string array) should be concatenated.

V. The obtained concatenated message should be encrypted and send to the server.

****SERVERRESPONSE****

VI. Server receives the encrypted message from client side.

VII. Decrypted the encrypted message received from the client.

VIII. The message resulted after decryption, should be hashed

IX. After Hashing, the resultant message will be checked with the original message and checks for integrity.

X. If the Compared message is not matched. Then an attack happens and the message is modified.

7. Results and Analysis

```
dinu@Dinesh8547:~/Desktop$ ./a.out
Enter Input data :
Hi welcome to the project
Encrypting the Message ...
Data sent to server is: MnX|jqhtrj%yt%ynj%uwtojhyyhjotwukjnykty%jrthqj|%M
Received data from Server
Decrypting Message....
Received Message is:message recieved is "welcome to the project"
Enter Input data :
sucess
Encrypting the Message ...
```

Inputs from Client Side

```
dinu@Dinesh8547:~/Desktop$ ./a.out
Server is Running.
Message is received :
Decrypting Message....
Message Recieved is:Hi welcome to the project
Enter the reply:message recieved is "welcome to the project"
Encrypting the Message ...
Data sent to client is rjxxflj%wjhnj{ji%nx%}|jqhtrj%yt%ynj%uwtojhy''
Message is received :
Decrypting Message....
Message Recieved is:sucess
ssecusp e
Enter the reply:█
```

Message received from client to server

Acknowledgement

The work proposed in the paper is supported by Mr.P.KalyanChakravarthy and says how to attain integrity by using the concepts of confidentiality and authentication during the transmission of messages.

9. Conclusion

In this paper, there are severe safety issue connected to SMS. So, here planned a original come up to safeguard SMS from MIMT attack integrity has been presented by avoiding the attacks such as man-in-the-middle, Denial of service(Dos) attacks this is dynamically proven by establishing the socket connection between client and server and uses a special technique(hash technique) to transmit the messages. this is employed in GSM networks because now-a-days most of the transmissions are being done in 2G network known as GSM. By using connection between client and server the message is integrated successfully.

References

[1] Muhammad Murad Khan, MajidBakhtiari, SaeidBakhtiari "An HTTPS approach to Resist Man in the Middle Attack in Secure SMS Using ECC and RSA" in 2013th International Conference on Intelligent Systems Design and Applications (ISDA).

[2] David Lisoněk, Martin Drahansky "SMS Encryption for Mobile Communication" in 2008 International Conference on Security Technology.

[3] NeeteshSaxena, Member, IEEE, and Narendra S. Chaudhari, Senior Member, IEEE "EasySMS: A Protocol for End-to-End Secure Transmission of SMS" in 2014, IEEE transactions on information forensics and security.

[4] Minta Thomas, Panchami V "An Encryption Protocol for End-to-end Secure Transmission of SMS" in 2015, International Conference on Circuit, Power and Computing Technologies [ICCPCT]

[5] Jayasri .J , Logeshwari . N, "ARM Based Electronic Notice Board all the way through Zigbee with Room Lights Control via PIR Sensor" in 2016, International Innovative Research Journal of Engineering and Technology.

[6] Prof. Rashmi Ramesh Chavan , Prof ManojSabnees, "Secured Mobile Messaging" in 2012, International Conference on Computing, Electronics and Electrical Technologies [ICCEET] .

[7] A. Hossain, S. Jahan, M. Hussain, M. R. Amin, and S. Newaz, "A proposal for enhancing the security system of short message service in GSM," in 2nd International Conference on Anticounterfeiting, Security and Identification, 2008. ASID 2008, pp. 235-240.

