SECURE SYSTEM OF SHORT MESSAGE SERVICE (SMS) FOR GSM NETWORKS

[1]LOKESH GIRIPUNJE, [2]NIKHIL SAKHARE, [3]MITHIL WASNIK

[1]KDK College of Engineering, Nagpur, India
[2,3]Rajiv Gandhi College of Engineering and Research, Nagpur, India
Email:-lokeshgiripunje@gmail.com ,nikhilsakhare.06@gmail.com, mithilwasnik@rediffmail.com

Abstract—The mobile communications has experienced a great acceptance among the human societies. The Short Message Service (SMS) is one of its superior and well-tried services with a global availability in the GSM networks. In the GSM, only the airway traffic between the Mobile Station (MS) and the Base Transceiver Station (BTS) is optionally encrypted with a weak and broken stream cipher A5. 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 non-repudiation are the most important security services in the security criteria that should be taken into account in many secure applications. The proposed system provides the end to- end security in any SMS message outgoing or incoming to the Subscriber Identity Module (SIM).

Index Terms— MS, SMS, BTS, GSM, SIM, Protocol

I. INTRODUCTION

The GSM network with the greatest worldwide number of users, succumbs to several security vulnerabilities. SMS is a very popular wireless service throughout the world. It is the transmission of alphanumeric message between two parties. It enables the communication between the mobile subscribers and external systems such as paging, electronic mail and voice-mail systems. It will be the most attractive and effective service for future commercial use. SMS is a part of GSM networks that allows the alphanumeric message up to 160 characters to be sent and received via the network operator's SMS center to the mobile subscribers. If the subscriber is not reachable, then SMS are stored in the GSM operator's SMS center and delivered when it is reachable. The existing SMS is the transmission of just plaintext. It can be easily read by the intruder or even the persons of the operator. Therefore, it is not secured enough for future m-commerce or mobile banking. So security is one of the main concerns for these businesses.[1] In this work, the security of SMS in GSM network has been discussed especially for the use of SMS as such business tool. Here, we have introduced the complete security solution. In this system we have a security scheme for improving the SMS security.[2]

A. Architecture of SMS in GSM Network

The basic network architecture of SMS in GSM network is shown in Fig. 1. Here we have considered the communication between the mobile subscriber and the bank which is providing such m-commerce facilities.

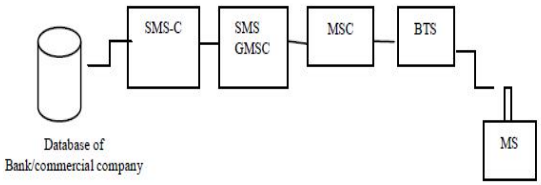

Fig.1SMS Architecture in GSM

- *SMS-C:* SMS Center
- *SMS GMSC:* SMS Gateway Mobile Switching Center
- *MSC:* Mobile Switching Center
- *BSS:* Base Station System

SMSC is responsible for the relaying, storing, and forwarding of a short message between an SME and mobile device. The SMSC must have high reliability, scalability, subscriber capacity and message throughput. Another factor to be considered is the ease of operation and maintenance of the application, as well as the flexibility to activate new services and upgrade to new software releases. SMS-C may connect to several GSM network through SMS GMSC which locates the current MSC of the message receiver and forwards the message to that MSC. This MSC broadcasts the message toSpecific BSS (in specific location area) with the help of Home Location Resistor (HLR) and Visitor location resistor (VLR). Then Base Transceiver Stations (BTS) page the destination Mobile station (MS). SMS can be stored in Subscriber Identity Module (SIM) or in the memory of the Mobile equipment (ME).[1]

B. SMS Security in & M-Commerce

SMS will play a very vital role in the future banking or commercial purpose because of its simplicity and cheapness. Upcoming payment system will be based on the mobile device by using SMS. Money can be debited or credited from the bank through the SMS

by using the GSM network. But some security related services of SMS should be available when we go for such m-commerce or m-banking. The service includes:

1) Confidentiality:

Only the valid communicating parties can view the SMS.

2) Integrity:

The SMS cannot be tampered by the intruders. The system should be able to find out such alteration.

3) Non-repudiation:

No party can deny the receiving or transmitting the data communicating between them.

4) Authentication:

Each party has to have the ability to authenticate the other party.

5) Authorization:

It has to be ensured that, a party performing the transaction is entitled to perform thattransaction or not.[4]

Our security proposals ensure all of these services. No such work ever done which can provide allthese security services.

C. Various Threats on SMS in GSM

There many threats can come to account for m-commerce via SMS. Sometimes the passwords for a bank account need to be sent. If any intruder read the SMS, he or she can gain the password as it is in plaintext. Encryption technique would be required to solve this attack. The SMS can also be altered or modified. Another problem is repudiation. Any sender can deny sending his or her SMS. Commercial companies can also deny the SMS receiving. Digital signature can provide the solution of these threats. So various threats or attacks can be generalized in 4 ways:[1], [10]

1) Interception
2) Interruption
3) Modification
4) Fabrication

D. Introduction of Android Operating System

The Linux kernel provides core system services to the Android software stack. These services include device drivers, networking, and file system, memory, power, and process management. Google patched the kernel with kernel enhancements, such as specific drivers and utilities, to support Android. The next level up in the software stack contains the Android native libraries. These libraries are written in C/C++ and used by various system components in the upper layers. Next is the Android runtime, consisting of the Dalvik virtual machine (VM) and the core libraries. The Dalvik VM runs the Dalvik executable (.dex) files that are designed to be more compact and memory efficient than Java class files. The core libraries are written in Java and provide a substantial subset of the Java 5 standard edition packages as well as some Android-specific libraries, which are needed for accessing the capabilities provided by the hardware, operating system, and native libraries. The application framework layer, written fully in Java, includes tools provided by Google as well as pro-prietary extensions or services. The top layer is the application layer, which provides such applications as a phone, Web browser, and email client. Each Android application is packaged in an .apk archive for installation. The .apk archive is similar to a Java standard jar file in that it holds all code and non-code resources (such as images and manifest) for the application. Android applications are written in Java based on the APIs provided by the Android software development kit. Every Android application runs in its own Linux process, with its own instance of the Dalvik VM. The application is also assigned its own user ID at installation time. Therefore, in principle, the code of two applications can't run in the same process or harm each other. The Dalvik VM relies on Linux for its underlying functionality (for example, process isolation, threading, and low-level memory management).

II. LITERATURE SURVEY

Before moving on to the secure system foe SMS in m-commerce it is necessary to consider some of the existing systems and architectures. In general the system uses different encryption techniques for SMS security.

A. SSMS - A Secure SMS Messaging Protocol for the M-Payment Systems

The main contribution of this paper is to introduce a new secure application layer protocol, called SSMS, to efficiently embed the desired security attributes in the SMS messages to be used as a secure bearer in the m-payment systems. SSMS efficiently embeds the confidentiality, integrity, authentication, and non-repudiation in the SMS messages. It provides an elliptic curve-based public key solution that uses public keys for the secret key establishment of a symmetric encryption. It also provides the attributes of public verification and forward secrecy. It efficiently makes the SMS messaging suitable for the m-payment applications where the security is the great concern. It will be a network independent solution and does not need any change in the network's infrastructure. The security of SMS messaging at the application layer is considered in some literature. The TS 03.48 standard that was designed for the SIM Application Toolkit (SAT) can also be used for providing the end to- end security in any SMS message outgoing or incoming to the Subscriber Identity Module (SIM).[11]

B. Enhancing the Security System of Short Message Service in GSM

In this work, the security of SMS in GSM network has been discussed especially for the use of SMS as such business tool. Here, they introduced the complete security solution. Both the encryption and digital signature has been incorporated with the transmission of SMS. Encryption can be done with the existing GSM encryption algorithm, A8. Then the encrypted message will create hash and finally it will be digitally signed. This signed encrypted will be transmitted.

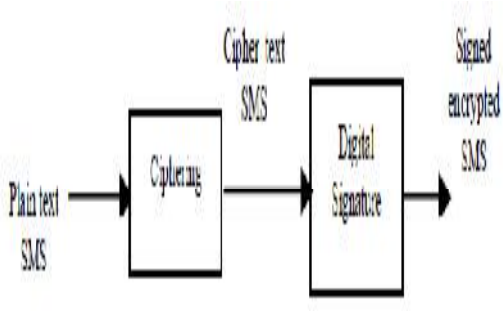

Fig. 2GSM SMS security system

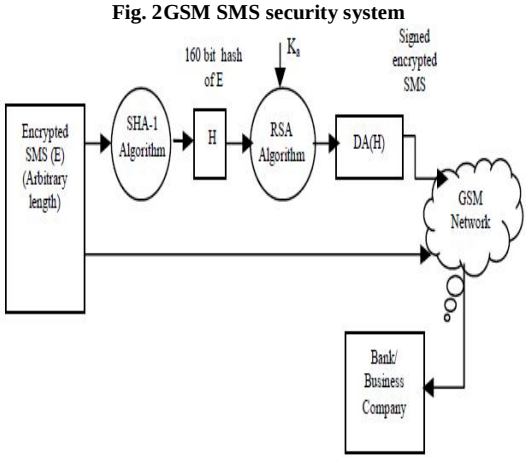

Fig. 3 Digital Signature Mechanism for SMS

In this scheme, some overhead of the SMS will be included while transmitting. This will limit the maximum characters can be sent as 130 instead of 160. Its major disadvantage using RSA for signing the hash is that it requires keys of at least 1024 bits for good security, which makes it quite slow.

III. METHODOLOGY

This section describes the methodology for total security solution for SMS in m-commerce. In our work, the authentication and the authorization procedure of the subscribers while connecting to the GSM network will be done according to the standard existing procedure. Our concern is to provide secure end-to-end communications. It has to be kept in mind that we can keepthe SMS secured even from the network operator. The main concept of our proposal is that we will do the ciphering on SMS first, and then the signature will imposed. This signed encrypted SMS will be finally transmitted.

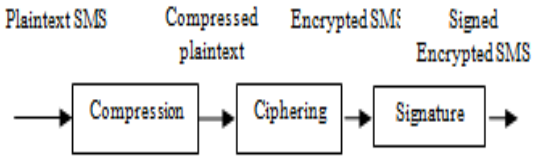

Fig. 4 Overall Security Scheme for SMS

A. Authentication

The authentication feature ensures to a very high level of probability that the user is who they claim to be. The purpose of the authentication is to protect the network against unauthorized use. It also enables the protection of the GSM PLMN. Subscriber authentication is performed at each registration, at each call set-up attempt (mobile originating or terminated), and before performing some supplementary servicessuch as activation or deactivation of the mobile. Authentication is not mandatory prior to IMSI attach and detach procedures. The frequency with which a particular PLMN applies the authentication procedure to its own subscribers is its own responsibility. However, a PLMN shall apply the authentication procedure to visiting subscribers as often as this feature is applied to those subscribers in their home PLMN. The authentication procedure is performed after the subscriber identity (IMSITTMSI) is known by the network and before the channel is encrypted. A very simple authentication method is the use of a password (or a PIN code).

B. SMS Compression

Plaintext SMS is first compressed with RLE (Run Length Encoding). It is a lossless algorithm that only offers decent compression ratios in specific types of data. RLE is probably the easiest compression algorithm there is. It replaces sequences of the same data values within a file by a count number and a single value. Suppose the following string of data (17 bytes) has to be compressed: ABBBBBBBBBCDEEEEF Using RLE compression, the compressed file takes up 10 bytes and could look like this: A *8B C D *4E F As you can see, repetitive strings of data are replaced by a control character (*) followed by the number of repeated characters and the repetitive character itself. The control character is not fixed; it can differ from implementation to implementation. If the control character itself appears in the file then one extra character is coded.RLE encoding is only effective if there are sequences of 4 or more repeating characters because three characters are used to conduct RLE so coding two repeating characters would even lead to an increase in file size.
It is important to know that there are many different run-length encoding schemes. The above example has just been used to demonstrate the basic principle of RLE encoding. Sometimes the implementation of RLE is adapted to the type of data that are being

compressed. This algorithm is very easy to implement and does not require much CPU power. RLE compression is only efficient with files that contain lots of repetitive data. These can be text files if they contain lots of spaces for indenting but line-art images that contain large white or black areas are far more suitable. Computer generated color images (e.g. architectural drawings) can also give fair compression ratios.

C. SMS Ciphering

The security methods standardized for the GSM System make it the most secure cellular telecommunications standard currently available. The confidentiality of the communication itself on the radio link is performed by the application of encryption algorithms and frequency hopping which could only be realized using digital systems and signaling. But unfortunately, there is no such system for encrypting SMS. The security mechanisms (for voice and data communication) of GSM are implemented in three different system elements; the Subscriber Identity Module (SIM), the GSM handset or MS, and the GSM network. We want to treat the SMS as the voice or data in GSM network. In this system, SMS encrypted by using (AES) Advanced Encryption Standard. AES does not use a Feistel structure. Instead, each full round consists of four separate functions: bytesubstitution, permutation, arithmetic operations over a finite field, and XOR with a key.[4]

1) General Security

AES has no known security attacks. AES uses S-boxes as nonlinear components. AES appears to have an adequatesecurity margin, but has received some criticism suggesting that its mathematical structure may lead to attacks. On the other hand,the simple structure may have facilitated its security analysis during the timeframe of the AES development process.

2) Software Implementations

AES performs encryption and decryption very well across a variety of platforms, including 8-bit and 64-bit platforms, and DSPs.However, there is a decrease in performance with the higher key sizes because of the increased number of rounds that areperformed. AES high inherent parallelism facilitates the efficient use of processor resources, resulting in very good softwareperformance even when implemented in a mode not capable of interleaving. AES's key setup time is fast.

3) Restricted-Space Environments

In general, AES is very well suited for restricted-space environments where either encryption or decryption is implemented (but notboth). It has very low RAM and ROM requirements.

4) Hardware Implementations

AES has the highest throughput of any of the finalists for feedback modes and second highest for non-feedback modes. For the192 and 256-bit key sizes, throughput falls in standard and unrolled implementations because of the additional number of rounds. Forfully pipelined implementations, the area requirement increases, but the throughput is unaffected.

5) Other Versatility and Flexibility

AES fully supports block sizes and key sizes of 128 bits, 192 bits and 256 bits, in any combination. In principle, the AES structure can accommodate any block sizes and key sizes that are multiples of 32, as well as changes in the number of rounds thatare specified.

D. Signature on SMS

Message integrity means that the message has not been altered or destroyed by any attackers. And non-repudiation means that a receiver must be able to prove that a received message came from a specific sender. The sender must not be able to deny sending a message that he or she, in fact, didsend. Signature will provide us this security service. So we need signature after ciphering the plaintext SMS.Here we are applying signature in the form of ASCII characters.We are appending one character at start and one character at end of encrypted SMS.This pair of ASCII character acts as a signature for a set of senders and receivers. The subscriber will send signed encrypted message the bank/commercial company vi**a the GSM network.**

E. Verifying the Digital Signature

At the receiver end, after receiving signed encrypted message, the bank/commercial company first of all it will check for signature.Signature of both sender and receiver is same since the software installed contain same signature for each pair.So,the SMS is processed further if and only if the signature is same otherwise SMS is rejected (SMS not from Authenticated user). If signature is matched it assures that message has been verified as original. That means four measures of security (authenticity, authorization, integrity and non-repudiation) are preserved. But signature is not matched, then it can be said that there must be some data modification or alteration. This comparison also gives the guarantee that the transmission of SMS has been done by the true sender and received by the true receiver. The comparison also clarifies that the sender can never deny the SMS sending since he/she cannot deny the signature.

F. Deciphering SMS

After verifying the signature on SMS, the receiver will decrypt it by using the AES decryption algorithm.

G. Decompression of SMS

After decryption of SMS, it is decompressed using same RLE algorithm. Finally, we obtained our plaintext.

IV. WORKING OF PROJECT

At first plaintext of SMS is compressed with Run-length encoding (RLE) data compression algorithm. Then the compressed message is encrypted with the help of AES encryption technology, and then at last simple signature is appended to encrypted text. This compressed signed encrypted will be transmitted. After installing the application, it will appear in home screen of emulator/phone.To use the application just click/touch the icon of application SMS App. On click it will open an UI, write the number of recipient and your message. Click Send SMS button to send SMS.

V. RESULTS AND DISCUSSION

Snapshot of emulator and real time implementation shows that the system provides complete security solution for SMS.

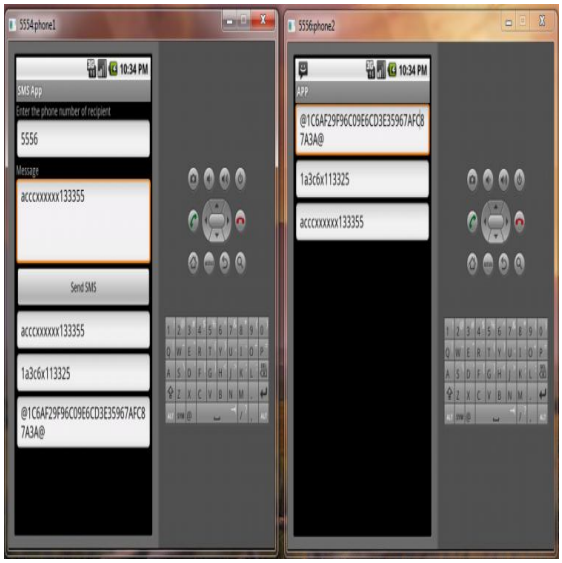

Fig. 5Snapshot of both emulators (phones) after the successful delivery of SMS.

Figure above shows that the plaintext SMS transmitted from sender phone is received exactly same on receiver phone. The limited memory capacity of SIM and the slow processing power of MS have to be considered. Another thing we have to consider that the secured SMS communication should be real time or should have a minimal accepted delay. That's why instead of using any algorithm which causes for ciphering we can use the AES algorithm. Instead of using the digital signature, we just appended ASCII characters which act as signature. In our system, no hardware implementation is needed. All schemes can be served by the software or system modification.

CONCLUSION

In the future, the use of SMS will have verities of dimensions such as for m-commerce, m-banking etc. due to its cheapness and availability. For these feasible future businesses through SMS, we have to provide the total security of it. In this work, a security scheme is given that will improve the security of SMS. In the proposal, the plain SMS will be compressed first, then encrypted and then it is appended signature. So by these themes, a total SMS security solution achieved. It is an application that simultaneously provides the confidentiality, integrity, authentication, no repudiation, public verification, and the forward secrecy of message confidentiality. It efficiently combines encryption and signature for encrypting the short messages via a symmetric encryption. Since it deploys symmetric encryption algorithm, it has great computational advantages over the previously proposed public key solutions while simultaneously providing the most feasible security services. It has great advantages to be used in the real m-payment applications and whenever the secure SMS messaging is important. However, its structure does not reply on the SMS messaging and is suitable for any other store and-forward technology.

FUTURE WORK

In the future, the practical implementation and the proposed scheme will incorporate. Various kinds of latest encryption algorithms and the hash functions are yet to be analyzed. We will try to integrate the channel coding and the encryption procedure so that it will give errorless secured fastest SMS transmission. I have also planned to research with the SMS security in 3G system. Errorless Data transmission with security is important in wireless environment. In the future, we will try to integrate secured transmission (SMS encryption) with joint channel coding.[7]

REFERENCES

[1] Md. Asif Hossain1, Sarwar Jahan, M. M. Hussain, M.R. Amin, S. H. Shah Newaz, "A Proposal for Enhancing Security System of SMS in GSM", May 2009 IEEE, pp:1-6.

[2] Alfredo De Santis, Aniello Castiglione, Umberto Ferraro Petrillo, "An Extensible Framework for Efficient Secure SMS", 2010 International Conference on Complex, Intelligent and Software Intensive Systems,May 2010,pp:843-850.

[3] Pan Tiejun , Zheng Leina ,Fang Chengbin ,Huang Wenji,Fang Leilei, "M-commerce Security Solution Based on the 3rd Generation Mobile Communication", International Symposium on Computer Science and Computational Technology, 2008 IEEE, pp:364-367.

[4] William Stallings, "Cryptography and Network Security Principles and Practices, Fourth Edition", Prentice Hall, 2006.

[5] Asha Mehrotra, "GSM System Engineering", The Artech House Telecommunications Library, INC., 2006.

[6] Do Van Thanh, "Security issues in Mobile eCommerce" International Conference on Security in Mobile eCommerce, 2000 IEEE, pp: 412-425.

[7] Ashok Kumar Nanda, Lalit Kumar Awasthi, "Joint Channel Coding and Cryptography for SMS", 2011 International Siberian Conference on Control and Communications SIBCON, April 2011, pp: 51-55.

[8] Ashok Kumar Nanda, Lalit Kumar Awasthi, "Encryption Based Channel Coding Algorithm for Secure SMS", World Congress on Information and Communication Technologies, 2011 IEEE, pp: 1282-1287.

[9] M. Ayoub Khan, Ir. M K Awang, R Chowudhury, Y. P. Singh, "A public key infrastructure (PKI) for signaling short message in GSM", proceedings of the ICCCE'06, Malaysia, vol. 1, May 2006,pp:97-102.

[10] Andrew S. Tanenbaum, "Computer Networks", fourth edition, Pearson education, 2006.

[11] Mohsen Toorani, Ali Asghar Beheshti Shirazi, "SSMS - A Secure SMS Messaging Protocol for the M-Payment Systems", International Symposium on Computer Science and Computational Technology, 2008 IEEE, pp:700-705.

★★★