# Study of SMS Encryption Techniques

Meghana Madhusudanan
Dept.Computer Engg,
Ramrao Adik Institute of Technology
Navi Mumbai,India

Puja Padiya
Dept.Computer Engg,
Ramrao Adik Institute of Technology
Navi Mumbai,India

## ABSTRACT

Short Message Service (SMS) provides a very convenient way for users to communicate and also gives other facilities. Hence, it is very popular among the users of mobile phones or other portable devices. Use of SMS has a wide importance in every field, be it notifications, advertisements or for personal communication. Though people use it in large scale, there is a lack of knowledge among people regarding its security. The users are unaware of how much the transmission of messages must be trusted. In this paper, a comparative analysis of the latest schemes used for SMS message security in modern mobile devices is done.

## General Terms

Encryption, Cryptography

## Keywords

SMS, Elliptical Curve Cryptography, Sensor encryption, gesture algorithms, Compression, GZIP

## 1. INTRODUCTION

Short Message Service (SMS) has become an extension to our lives. SMS is a popular medium for delivering Value Added Services. Used for mobile banking, stock alerts, railways and flight enquiries etc [1]. These types of messages are computer generated. They are sent over SMPP protocol. SMS has a future scope in business such as M-Commerce, mobile banking etc. There are various techniques discussed where the SMS is encrypted using a common public key and the SMS gateway acts as mediator [2]. A method also discussed to secure an SMS message. This is done using onetime keypads that uses shared information between the communicating entities and the GSM network [1]. Another paper discussed a technique which uses hybrid application security with compression [3]. Another method given, encrypts the data using sensors. Sensors use accelerometer, multi-touch gestures, GPS sensors etc [4]. A technique is described based on Elliptical Curve Cryptography [5]. The paper is structured as: Related work is given in section II. Methods to secure SMS are described in section III, comparative analysis in section IV, followed by conclusion.

## 2. RELATED WORK

There exists some related work [6-7] which describes techniques for encrypting SMS. The author in paper [6] focuses on a technique called public Key Infrastructure (PKI) which uses pairing of key for secure communication encryption. A novel secure mobile content delivery method is introduced [7] where networked devices in a neighbourhood can discover each other. They can transfer media contents in a convenient method instead of regular transfer method using unfriendly manual operations of connection and file transfer. The paper [9] reviews digital signature and its use to secure SMS. The author gives a brief view on the various hash algorithms implemented in digital signatures for eg, MD5 algorithm, SHA-1, SHA-2. A new scheme is proposed in this paper [10] where, initially plaintext of SMS is converted into cipher text with the help of existing GSM encryption technology. The cipher text is formed. It is then digitally signed. It is done using public key signature. The communication is secured by using public key. In paper [11], the identity validation of the contacts is implemented. It is done through ECDSA signature scheme.

## 3. METHODS TO SECURE SMS

This section describes few of the SMS securing techniques

### 3.1 Using an approximated one-time keypad to secure Short Messaging Service (SMS).

This technique is one of the very secure techniques. SMS message which is transported is secured using this approach. This method is used even if it is transported through any medium. The physical underlying architecture is unaltered. Only the intended users are able to view the message. Every message denoted by m, is encrypted using an encryption method denoted by E where the output obtained is a cipher text. A hash function is used as transformation function. The input is of variable size. But the output has a fixed size given as h=H(X). The following requirements must be satisfied in order to use one-time keypad

- Each key k is used only once.
- The key k used to encrypt a message m is at least as the size as m.
- Each key is random and unpredictable. These are the necessary points to be considered when using this method. It has certain practical problems. It is called as key distribution problem, where each time prior to communication, a new random key must be issued and once a key is generated, it must be distributed among all communicating parties. Generation of one-time key pad is as follows.

$$k1 = SHA1(IMSI; TMSI; IMEI; LAI) \quad (1).$$

where k1 is obtained from SHA1 Hash. The inputs are IMSI, IMEI and LAI. The TMSI is the only variable input. The key is an approximated one-time pad. A TMSI is just for one-time use for the generation of one-time keypad. Once it is used, it is discarded. The serving GSM network allocates a new TMSI number. It is transmitted to the MS in cipher text. For each new SMS message sent, a new approximated one-time pad is produced, which is k1. The remaining keys are generated as follows.

$$ki = SHA1(ki1) \quad (2).$$

where (i = [2; 7]).

### 3.2 Novel approach for SMS security

SMS possesses two properties. The first property is that it can be monitored. Another important property is that, it is one-way communication. The scheme can be designed for two way communication. This would double the cost. There are two issues to design an encryption for an SMS. In this paper, an SMS gateway is employed. It acts as a third party entity. It is done to send messages among devices. The messages are encrypted by a common public key. It is then stored on the devices. In this scheme, the SMS gateway transforms these messages encrypted by the personal public key of a node. It is done without decrypting the messages. The scheme consists of 2 phases. They are initialization and communication phases.

1) Initialization.: This phase generates the parameters for authentication, encryption, or decryption of messages. Let G1 be an additive group. Another group G2 be a multiplicative group. And e be a bilinear map. H1 :{0,1}*G1 be a transform map. Let Øi be a unique mobile identification for the device of the i-th user. Let σ be a secret key for SMS gateways and m be the number of devices registered. It is assumed that v-th user is registered and P is a element of G1.

Step1:. Generates and distributes a common public key.

$$\sigma P \prod_{k=0}^{m} \emptyset k \tag{1}$$

Step2: Generates a private key of v-th user .

$$\frac{P \prod_{k=0}^{m} \emptyset k}{\emptyset v} \tag{2}$$

Step3: A mobile device stores both keys namely, common

public key and the private key K.

$$(G_1;G_2;ế;H_1;\ P;CPK;\ ḳ) \tag{3}$$

2) Communication: This phase is used to send messages. It causes these issues. Hence this scheme stores the common public key. Let CPK be the common public key. Let alpha and beta be the cellphone numbers of Alice and Bob. When Alice wants to send a message following steps are performed. Step1:. Alice's device encrypts the message using the common public key.

$$C1= è(H1(\beta), \frac{CPK}{\emptyset\alpha}).\ M \tag{4}$$

Step2: Alice sends the encrypted message. Also sends Bob's cellphone number to an SMS gateway.

Step3: The SMS gateway trans-shapes. It forwards the message received from Alice. It uses the cellphone number included.

C2 = C1.Øa/σ.Øa.

Step4: Upon receiving the message, Bob decrypts it by using his own private key, K

$$M = \frac{C2}{\acute{e}(H1(\beta),ḳ\beta)} \tag{5}$$

$$M= (\ ế(H1(\beta); CPK). M)/e(H1(\beta)\frac{P \prod_{k=0}^{m} \emptyset k}{\emptyset v}) \tag{6}$$

In order to monitor messages, SMS gateways can decrypt messages irrespective of the intended recipient. Hence, the given scheme derived the common public key. It is derived from a secret key of a serve. It also uses the identifications of alldevices.

## 3.3 Application-Layer security mechanism for M2M communication over SMS

The Security approach is used for M2M over SMS communication: (1) Each device can have an initial secret which is known by the devices itself.

(2) The signature is calculated as follows:.

S = H(Device IMEI + secret + (payload)) where H is MD5 or SHA1 hashing algorithm. Therefore, the signature is not always the same. It provides a content integrity check.

(3) Sender calculates the signature (2). Adds it in

the SMS. Then hash it again: signature + (compression( payload)) where GZIP is used as a compression algorithm.

(4)The device uses the same signature calculation as (2). Message is authenticated. It is accepted if signatures (3) (4) matches.

The message signature can be calculated. It uses MD5 or SHA1 hash. [7]. Before the payload can be sent, it should be encoded using Base64.

## 3.4 Securing SMS using Cryptography.

The author uses the concept of ECC to encrypt the message. It is sent over a common channel. The sender writes a message. Then gives the receivers number. And when he sends the message, the ECC algorithm is triggered on both the devices. The keys are shared among the devices. And the encryption takes place at the senders end. After encryption, the message is sent to the receiver. He decrypts it using his key. Each character in the message has to be converted into bytes. This is done during encryption. Then the bytes are converted into points of the form (x, y). Then the points have to be encoded. Encoding is done by mapping each of them with each point on the elliptic curve. Then the entire encoded points have to be converted into bytes. These bytes are then converted to strings. This is done because SMS can carry only string values. The domain parameters are a six tuple: T = (P, a, b, G, n, h). An elliptic curve over a field K is a curve. It is defined by an equation of this form. y2 = x3 + ax + b. where a, b K and 4a3 + 27b2 0. [8]

1) The sender communicates with the receiver. It is done through any normal means. It is about the confidential discussion to be followed. 2) Then both the sender and receiver are ready with their application. The sender types in the recipients' number. It types the body of the message and clicks Send. 3) The ECC algorithm is implemented at the sender end. And the keys are generated. The senders Public Key is then sent. 4) The receiver acknowledges this by clicking the Read button. Here, the received key is read by the receiver application. And the ECC algorithm is triggered at receivers end. The receiver's Secret Key is generated. And its Public Key is sent to the sender.

5) The sender receives the Public Key from the receiver. Then sender's Secret Key is generated. The message is encrypted using ECC algorithm. The encrypted message is sent to the receiver.

6) The receiver receives the message and decrypts it. Decryption is done using his Secret Key. ECC algorithm is used to get actual message.

## 3.5 Encryption using sensors

This system is based on data encryption. It uses readings from sensors. They can be touch sensor or the accelerometer as the encryption key. Motion gestures also can be used. Or multi touch gestures could be used. Encryption and decryption is done using the same key. It is a symmetric key cryptography. Since same key is shared between the sender and the receiver. The key could be a gesture or could be a sensor reading. The key used to encode the data byte can be of various kind. They can be:

- It can be motion gestures such as shaking the phone. So, the readings from accelerometers can be used.
- Elementary touch gestures can also be used. The gesture is identified. Then the encryption key is a based on the gesture.
- There can be compound touch gesture. Here, a set of X, Y coordinates is used.

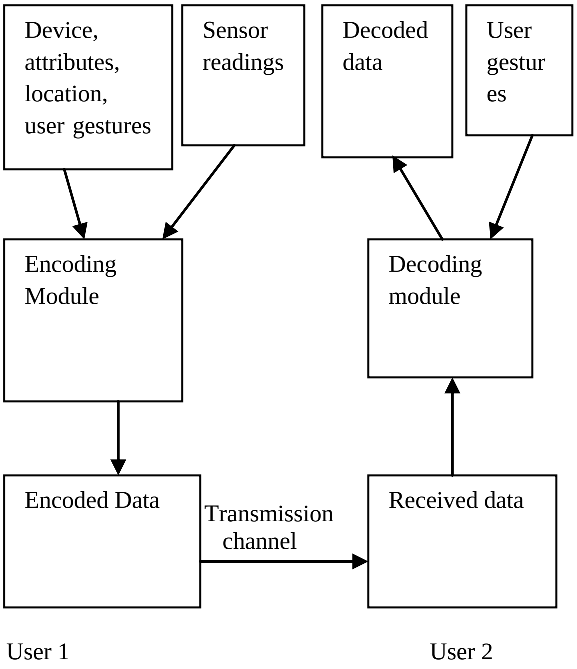

**Fig 1. Encoding**

This set is used to encode the data. The sender sends the message. This consists of raw data, other attributes along with sensor readings. The raw data is the actual message which the sender has to send. The sensor reading is used as a key to encrypt the message to be sent. This can be environment or device attributes or gestures. This data is given through an encoding module. The encoding module does the encryption. It is encrypted and transmitted to the receiver. The receiver receives this data sent by the sender.

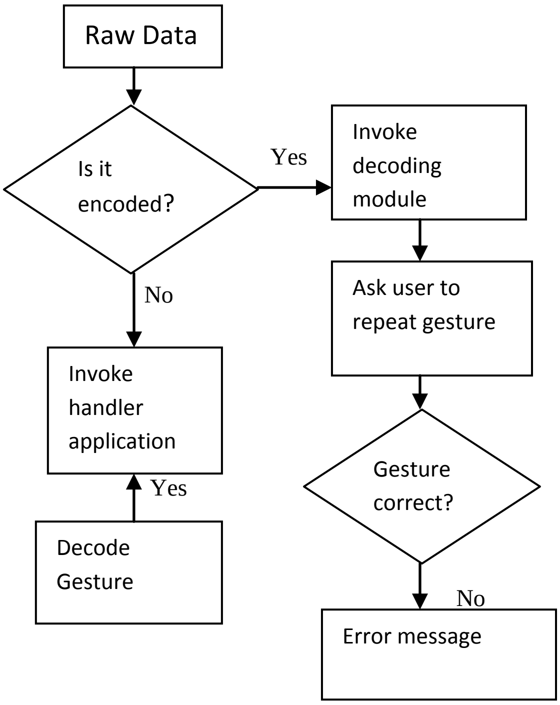

**Fig2. Decoding**

He decodes the data. The encrypted message O is a function of the shared where f is the function for encrypting input. At the receiver end, O is decrypted using the same key K. I=f'(K,O). Bitwise XOR is used. The output of pre-processing

steps is in the form of a one dimensional array of n points. The first step is to perform XOR of the key and input vectors,

O= K XOR I

to get back the original decoded input data I,

I=O XOR K.

key K. And the input data I is shown,

O=f(K,I)

where f is the function for encrypting input. At the receiver end, O is decrypted using the same key K.

I=f'(K,O).

## 4. COMPARATIVE ANALYSIS

**Table 1. Comparing encryption techniques**

| Technique<br>Parameter | Type of Cryptography | Concept | Security |
|---|---|---|---|
| Using one time keypad. | Secret key | Uses SHA-1 hash algorithm to encrypt using TMSI. | Secure |

| | | | |
|---|---|---|---|
| Approach using common public key | Public key cryptography | The sender encrypts the message using a common public key | Less secure than sensor based and one time key pad |
| Application layer mechanism | Secret key cryptography | Signature is calculated Using device IMEI, secret key and payload | Less secure |
| Securing SMS using cryptography | Public key cryptography | The sender and the receiver used ECC | Less secure |
| Encryption using sensors. | Secret key cryptography | The encryption key is either user gestures or some other sensor readings | Secure for transmitting messages across multiple transmission channels |

| Technique<br>Parameter | key feature | Difficulties |
|---|---|---|
| Using one time keypad. | It does not alter the GSM architecture | A new truly random secret key must be issued prior to every communication |
| Approach using common public key. | Uses a common public key instead of personal public key. | All the identifications must be stored at the server or SMS gateways |
| Application layer security mechanism | Message compression can provide better efficiency | More time consuming than others since it requires compression |
| Securing SMS using cryptography. | It is also applicable in devices with very limited memory | The sender and the reciever should be using same application and should be active at the same time |
| Encryption using sensors | Using sensors enables more secure way of encrypting and transmitting data across multiple transmission channels | The noise should be dealt with properly |

Above discussed methods shows differences due to different encryption concepts applied. Each technique uses different keys for encrypting messages. Each technique consists of their own drawbacks. Encryption using one-time keypad is considered to be secure, but it requires a new key to be generated each time a message is sent. Encryption using sensors would be a good solution if the noise that comes along with the raw data is dealt with in a proper manner. It offers a secure way to transmit messages through multiple channels.

## 5. CONCLUSION

This paper reviews the latest security schemes such as Using one-time keypad, approach using common public key, application layer security mechanism, securing SMS using cryptography, encryption using sensors which are used for SMS message security in modern mobile devices. Performance of mobile devices depends on encryption time of a security scheme used for SMS. There is very little performance difference in these categories. Each of these techniques has its own disadvantages. When one-time keypad is used for encryption, it gives an advantage that the GSM architecture is not altered but it faces the issue that, each time a new random key must be issued and distributed prior. In case of encryption using application layer mechanism, it increases efficiency by compression but it consumes more time which becomes a drawback. Therefore it is concluded that any of these discussed techniques can be used according to the extend of security required.

## 6. REFERENCES

[1] Muhammad Waseem Khan, “SMS Security in Mobile Devices: A Survey”,Int. J. Advanced Networking and Applications Volume: 05, Issue: 02, Pages:1873-1882 (2013)

[2] Jongseok Choi and Howon Kim,“A Novel Approach for SMS Security”, International Journal of Security and Its Applications, vol. 6, 2012

[3] N. Gligoric, T. Dimcic, D. Drajic, S. Krco, and N. Chu, “Applicationlayer security mechanism for M2M communication over SMS”, Proc. Telecommunications Forum (TELFOR), 2012, 5- 8.

[4] J. Bose and T. Arif,“Encryption in mobile devices using sensors”, Proc. Sensors Applications Symposium (SAS), IEEE, 2013, 55-60.

[5] Nor Badrul Anuar, Laingan Kuen, Omar Zakaria, Abdullah Gani, Ainuddin Wahid Abdul Wahab, “GSM Mobile SMS/MMS using Public key Infrastructure: m-PKI”,WSEAS TRANSACTIONS on COMPUTERS, Issue 8, Volume 7, August 2008

[6] Chih-Lin Hu and Chien-An Cho, “A Novel Mobile Content Delivery Scenario with Simple Double-Key Secure Access Control”, International Journal of Security and its Applications Vol. 3, No. 1, January, 2009

[7] Mary Agoyi, Devrim Seral, “SMS SECURITY: AN ASYMMETRIC ENCRYPTION APPROACH”, 2010 Sixth International Conference on Wireless and Mobile Communications

[8] Erfaneh Noroozi, Salwani Mohd Daud, Ali Sabouhi, “Secure Digital Signature Schemes Based on Hash Functions”, International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278- 3075, Volume-2, Issue-4, March 2013

[9] Neetesh Saxena, Ashish Payal, “Enhancing Security System of Short Message Service for M-Commerce in GSM”, International Journal of Computer Science Engineering Technology (IJCSET) 2012

[10] Neetesh Saxena,Narendra S. Chaudhari, “A Secure Digital SignatureApproach for SMS Security”, IP Multimedia Communications A SpecialIssue from IJCA, 2009

[11] N. J. Croft and M. S. Olivier, “Using an approximated one-time pad to secure short messaging service (SMS)”, Proc. Southern African Telecommunication Networks and Applications Conference. South Africa, 2008.