ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 4, April 2014

SMS Security for Android Mobile Using Combine Cryptographic Algorithms

Poonam Mandavkar[1], Gauri Patil[2], Chetna Shetty[3], Vishal Parkar[4]

Student, Computer, Rajendra Mane College of Engineering &Technology, Ambav, India[1,2,3]

Assistant Professor, Computer, Rajendra Mane College of Engineering &Technology, Ambav, India[4]

Abstract: This work relates to an alternative solution that provides a peer-to-peer SMS security that guarantees provision of confidentiality, authentication, integrity and non-repudiation security services. Short message service (SMS) is a very popular and one of the easy to use communication technology for mobile phone devices. Originally, this service was not designed to transmit secured data, so the security was not an important issue during its design. Yet today, it is sometimes used to exchange sensitive information between communicating parties. A combined cryptographic scheme has been used which is combination of the Diffie Hellman Key Exchange, PBE, SHA and AES algorithms to achieve more robust functionality. For implementation, Android SDK has been developed in Android to introduce a required security services for SMS. The developed application is tested on real equipment such as a device supported to Android 2.2 version. It is able to achieve all the required cryptographic operations completely on the users' mobile phone in less than one second for each operation, and thus the mobile phone performance still remains effective.

Keywords: SMS Security, Combine Cryptographic Algorithms, Android, confidentiality, authentication, integrity and non repudiation.

I. INTRODUCTION

Various types of tools have been created to make human communications simpler and faster. The most significant communication tool is the modern telephone which was first invented by Sir Alexander Graham Bell in the 19th century. Since then, communication devices have evolved into very advanced and sophisticated tools. Mobile technology is mostly preferred by 6 Billion mobile subscribers equating to more than 87% of world population. There are various functions provided by Mobile phones such as make and receive call, SMS, MMS, video calling, Internet, mp3, camera, games etc. These wireless devices were initially started as devices to store personal information. Short message service (SMS) will play an important role in the future business areas, which are popularly known as m-commerce, mobile banking, governmental use, and daily life communication. Furthermore, SMS has become a popular wireless service throughout the world as it facilitates a user to be in touch with any mobile phone subscriber anywhere in the world, instantaneously and without any hassle. The majority of SMS are sending and receiving not only casual greetings, but also important data such as social security numbers, bank account details, passwords, and so on and so forth. In some cases, this data may also include very private information reserved for the personal viewing of the legal recipient. So our aim is to provide a peer-to-peer SMS security that guarantees provision of confidentiality, authentication, integrity and non-repudiation security services. And as Android mobiles are widely in use we choose this device for implementation.

A. What is SMS?

Short message service (SMS) is a very popular and easy to use communications technology for mobile phone devices. Short Message Service (SMS) has become an extension of our lives and plays an important role in daily life. SMS is a popular medium for delivering Value Added Services and are suitable for mobile banking, payment reminders, 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. Sending an SMS is cheap, fast and simple. The service allows for short text messages to be sent from one cell phone to another cell phone or from the Web to another cell phone. When a person sends an SMS he or she usually uses her telephone keypad or physical or on-screen keyboard to type out a message. The user selects the recipient's phone number (or other address information) and clicks "send." From there, the message is sent to a short message service center (SMSC), which stores it and tries to send it on to the recipient. If the receiver is on another network, the message may travel through a gateway mobile switching center (MSC), which allows the different systems to communicate. The SMSC usually stores the message if it cannot be sent immediately and retries later; in some cases, however, the message will be dropped if it is not delivered successfully on the first attempt. Messages can be sent without the voice function of a cell phone being activated because it uses the control channel. This pathway is always active whenever the phone is turned on, and regularly sends and receives signals from the nearest cellular tower.

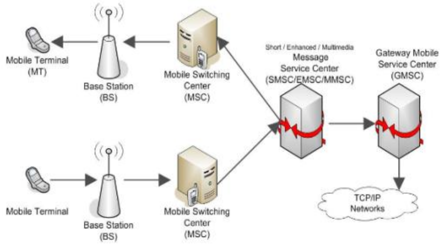
Mobile Terminal (MT)
Base Station (BS)
Mobile Switching Center (MSC)
Short / Enhanced / Multimedia Message Service Center (SMSC/EMSC/MMSC)
Gateway Mobile Service Center (GMSC)
Mobile Terminal
Base Station (BS)
Mobile Switching Center (MSC)
TCP/IP Networks

Fig. 1. Basic SMS service

B. Why there is need of SMS Security?

Unprotected communication channels pose serious security vulnerabilities. Thus, it is pertinent that both the mobile applications and the mobile operators must apply some reliable protective techniques to avoid these assailable vulnerabilities. This used to protect the mobile subscribers from the undesirable communication attacks during the SMS transmission. To overcome different types threats like spamming, Flooding / Denial of Service (DoS) Attacks, SMS Viruses etc. on SMS there is need of security to SMS. Mostly the SMS encryption is used for avoiding the attacks. So in this paper we are going to discuss on how to provide SMS security using four algorithms PBE, Diffie Hellman Key Exchange algorithm, AES, and SHA together for Android mobiles.

C. Combine Cryptographic Algorithms:

For providing high SMS security we are using combination of following cryptographic algorithms.

i. *PBE (Password Based Encryption):*

In many application of cryptography, security mainly depends on key which is generated by sender and receiver. But problem with this key is that there is need to store this key in small space and whenever it is required it is to be retrieved from that place. There may be possibility of search attack on it. For defending from the attack we use password based encryption (PKCS#5). Two common techniques are used in password-based encryption to try to reduce these problems:

- A deliberately slow method is used to derive the encryption key from the password, reducing the number of guesses that an attacker can make in a given time frame.
- Some random bytes, called a salt, are appended to the password before it is used to calculate the key.

ii. *Diffie Hellman Key Exchange Algorithm*:

Diffie Hellman is an algorithm used to establish a shared secret between two parties. It is primarily used as a method of exchanging cryptography keys for use in symmetric encryption algorithms like AES. The algorithm in itself is very simple. Let's assume that Alice wants to establish a shared secret with Bob.

For our example, let's assume that p=23 and g=5.

1. Alice chooses a secret integer ‘a’ whose value is 6 and computes A = g^a mod p. In this example, A has the value of 8.
2. Bob chooses a secret integer b whose value is 15 and computes B = g^b mod p. In this example, B has the value of 19.
3. Alice sends A to Bob and Bob sends B to Alice.
4. To obtain the shared secret, Alice computes s = B^a mod p. In this example, Alice obtains the value of s=2
5. To obtain the shared secret, Bob computes s = A^b mod p. In this example, Bob obtains the value of s=2.
6. The algorithm is secure because the values of a and b, which are required to derive are not transmitted across the wire at all.

iii. *AES (Advanced Encryption Standard):*

The Advanced Encryption Standard (AES) is a symmetric-key block cipher algorithm. The AES has three fixed 128-bit block ciphers with cryptographic key sizes of 128, 192 and 256 bits. Key size is unlimited, whereas the block size maximum is 256 bits. The AES design is based on a substitution-permutation network (SPN).

Working of AES:
Initial Round:

a) AddRoundKey—each byte of the state is combined with a block of the round key using bitwise XOR.

Rounds:

a) SubBytes—a non-linear substitution step where each byte is replaced with another according to a lookup table.
b) ShiftRows—a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
c) MixColumns—a mixing operation which operates on the columns of the state, combining the four bytes in each column.
d) AddRoundKey Final Round (no MixColumns):
e) SubBytes
f) ShiftRows
g) AddRoundKey.

In the AddRoundKey step, each byte of the state is combined with a byte of the round subkey using the XOR operation ($\bigoplus$).In the AddRoundKey step, the subkey is combined with the state. For each round, a subkey is derived from the main key using Rijndael's key schedule; each subkey is the same size as the state. The subkey is added by combining each byte of the state with the corresponding byte of the subkey using bitwise XOR.

iv. *SHA (Secure Hash Algorithm):*

General description:

SHA-256 (secure hash algorithm, FIPS 182-2) is a cryptographic hash function with digest length of 256 bits. It is a keyless hash function; that is, an MDC (Manipulation Detection Code). A message is processed by blocks of 512 = 16 × 32 bits, each block requiring 64 rounds.

Basic operations:

- Boolean operations AND, XOR and OR, denoted by $\wedge$, and $\vee$, respectively.
- Bitwise complement, denoted by $\overline{\ }$.
- Integer addition modulo 232, denoted by A + B.
- Each of them operates on 32-bit words. For the last operation, binary words are interpreted as integers written in base 2.
- RotR(A, n) denotes the circular right shift of n bits of the binary word A.
- ShR(A, n) denotes the right shift of n bits of binary word A.
- AkB denotes the concatenation of the binary words A and B.

Padding:

To ensure that the message1 has length multiple of 512 bits:

- first, a bit 1 is appended,
- next, k bits 0 are appended ,with k being the smallest positive integer such that l + 1 + k ≡448 mod 512, where l is the length in bits of the initial message,

- finally, the length $l < 2^{64}$ of the initial message is represented with exactly 64 bits, and these bitsare added at the end of the message.

The message shall always be padded, even if the initial length is already a multiple of 512.

Block decomposition:
For each block $M \in \{0, 1\}$
512, 64 words of 32 bits each are constructed as follows:

- The first 16 are obtained by splitting M in 32-bit blocks

$$M = W_1 \| W_2 \| \ldots. W_{15} \| W_{16}$$

- the remaining 48 are obtained with the formula:

$$Wi = \sigma 1\ (Wi-2) + Wi-7 + \sigma 0\ (Wi-15) + Wi-16,\ 17 \leq i \leq 64.$$

D. What is Android?

Operating Systems have developed a lot in last 15 years. Starting from black and white phones to recent smart phones or mini computers, mobile OS has come far away. Especially for smart phones, Mobile OS has greatly evolved from Palm OS in 1996 to Windows pocket PC in 2000 then to Blackberry OS and Android. One of the most widely used mobile OS these days is Android. Android does a software bunch comprise not only operating system but also middleware and key applications. Android Inc. was founded in Palo Alto of California, U.S. by Andy Rubin, Rich miner, Nick sears and Chris White in 2003. Later Android Inc. was acquired by Google in 2005. After original release there have been number of updates in the original version of Android.

II. EXISTING SYSTEM

In traditional approach SMS is a mechanism of delivery of short messages over the mobile networks. It is a store and forward way of transmitting messages to and from mobiles. The message (text only) from the sending mobile is stored in a central short message center (SMS) which then forwards it to the destination mobile. This means that in the case that the recipient is not available; the short message is stored and can be sent later. Each short message can be no longer than 160 characters. These characters can be text (alphanumeric) or binary Non-Text Short messages. An interesting feature of SMS is return receipts. This means that the sender, if wishes, can get a small message notifying if the short message was delivered to the intended recipient. Since SMS used signalling channel as opposed to dedicated channels, these messages can be sent/received simultaneously with the voice/data/fax service over a GSM network. SMS supports national and international roaming. This means that you can send short messages to any other GSM mobile user around the world. With the PCS networks based on all the three technologies, GSM, CDMA and TDMA supporting SMS. SMS is more or less a universal mobile data service.

III. PROBLEM DEFINATION

Problem Statement:

"In this project by using combine cryptographic algorithms such as PBE to generate private key, Diffie Hellman key Exchange Algorithm for exchanging key, AES for encryption/decryption and SHA-256 for generating hash value, we provide a peer-to-peer SMS security that guarantees provision of confidentiality, authentication, integrity and non-repudiation security services."

IV. SCOPE OF RPOJECT

Now a days, SMS is fast growing service in Mobile communication technology. SMS service is found to be advantageous as compared to any other service. But without some security mechanism, it is difficult to send data in secure manner. Scope of our project is to provide security mechanism to send data in secure manner. For the efficiency of user and considering current market trend we are using android technology for implementing our approach. In our thesis most of the attacks can be avoided. It can be used by people at organisational level, military people who have to share lot of secure information among each other. The main aim of our project is to provide four important characteristics explained below.

A. Confidentiality:

Confidentiality is the security service which ensures that receiver will be able to verify that signature with public key which they have already received during a key exchange session. Thus users will be able to make certain of the identity of the sender within their mobiles phone, without the need to access to the third party severs to check the sender's authenticity.

B. Authentication:

Authentication is the assurance that the communicating entity is the one that it claims to be. This service provides a system with the capability to verify that a user is the actual one he or she claims to be based on what the user knows or have. Non-repudiation is the security service that prevents the sender and the receiver from denying their participating in message transmission. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.

C. Integrity:

Integrity is the security service which ensures that data is not changed during its transmission from the sender to the receiver. Usually the integrity can be achieved by hashing the encrypted message and encrypting the message hashing then send it with the message to the receiver. Once the receiver receives the message, he will decrypt the encrypted message hashing and compare it with his own hashing on the received message. If the receiver's message hashing equals to the sender's message hashing, then the message has sound integrity, otherwise the message has been modified.

D. Non-repudiation

Non-repudiation is the security service that prevents the sender and the receiver from denying their participating in message transmission. Thus, when a message is sent, the receiver can prove that the alleged sender in fact sent the message. Similarly, when a message is received, the sender can prove that the alleged receiver in fact received the message.

V. PROPOSED SYSTEM

There are two cases in which our proposed system is work.

Case1: When both sender and receiver at active state.

Sender type some secret message inside the messaging panel and enter the receiver's mobile number. When he press 'send' button some internal process perform which is as follows:

a) At sender side, with the help of PBE algorithm one random number is generated.
b) This random number is integrated with some 'salt' value and from that private key is generated.
c) Using Diffie Hellman Key Exchange algorithm public key is generated by using private key.
d) This public key is send to the receiver. At same time one flag value is send to receiver which is used for differentiating key exchange process from actual message transmission.
e) At receiver side, receiver receives sender's public key.
f) With the help of PBE algorithm receiver generates its own private key.
g) Receiver also creates public key by following same procedure which is followed by sender.
h) With the help of public key of sender, receiver creates 'Decryption key' by Diffie Hellman key exchange algorithm and update flag value.
i) Receiver also sends its own public key to sender as well as it send updated flag value.
j) Sender receives receiver's public key. And sender creates 'Encryption key' by Diffie Hellman key exchange algorithm.
k) Now sender encrypt message using 'Encryption key' and create hash value of that original message using SHA algorithm. Both encrypted message and hash value with updated Flag value is send to receiver.
l) At receiver side, receiver receives the encrypted message and it is decrypted using 'Decryption key' which is same as 'Encryption key' of sender.
m) Receiver also creates hash value of decrypted message and check the integrity of that message. If hash value is not matching with sender's hash value then message will be discarded.
n) If Hash value is matched then it indicates original message is received by receiver.

Receiver opens the received message and read that message in normal way.

Case2: When sender is active and receiver is inactive.

Sender type some secrete message inside the messaging panel and enter the receiver's mobile number. When he press 'send' button some internal process perform which is as follows:

a) At sender side, with the help of PBE algorithm one random number is generated.
b) This random number is integrated with some 'salt' value and from that private key is generated.
c) Using Diffie Hellman Key Exchange algorithm public key is generated by using private key.
d) This public key is send to the receiver. At same time one flag value is send to receiver which is used for differentiating key exchange process from actual message transmission.
e) At receiver side, if receiver is inactive then sender wait for acknowledgment of key exchange process.
f) If the sender does not get any acknowledgment from receiver then the message is discarded. And at sender side, notification is given to sender that message is not send to the receiver.

Sender's message is not received by the receiver until receiver is not switch to the active state.

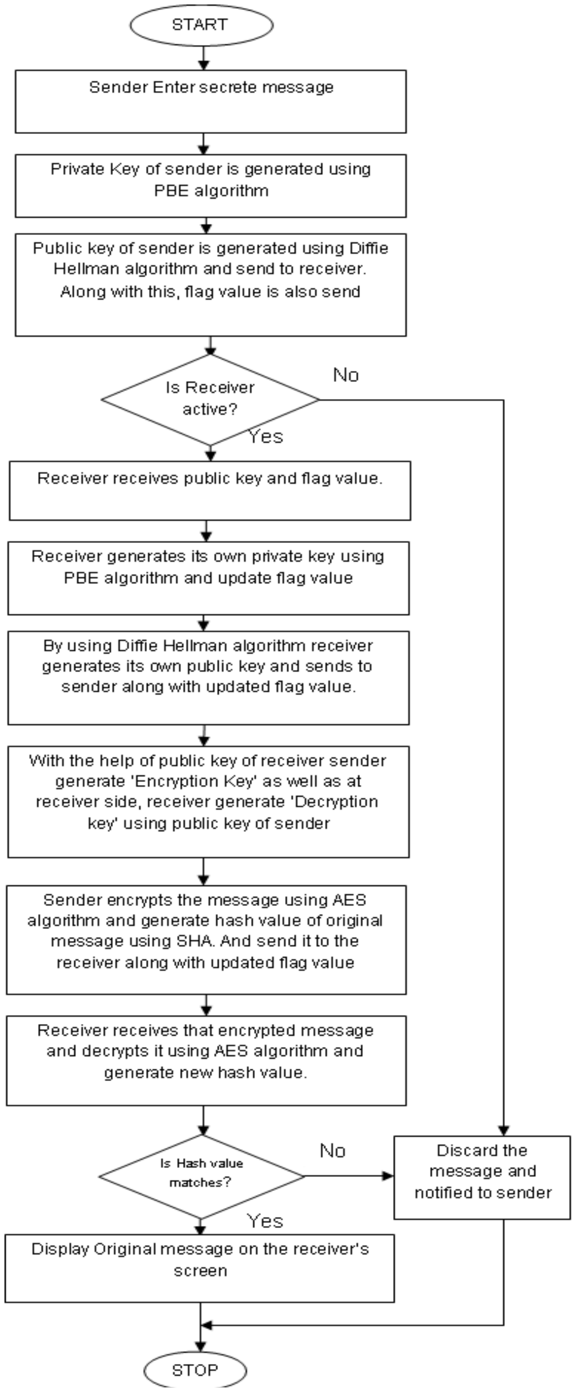
START
Sender Enter secrete message
Private Key of sender is generated using PBE algorithm
Public key of sender is generated using Diffie Hellman algorithm and send to receiver. Along with this, flag value is also send
Is Receiver active?
No
Yes
Receiver receives public key and flag value.
Receiver generates its own private key using PBE algorithm and update flag value
By using Diffie Hellman algorithm receiver generates its own public key and sends to sender along with updated flag value.
With the help of public key of receiver sender generate 'Encryption Key' as well as at receiver side, receiver generate 'Decryption key' using public key of sender
Sender encrypts the message using AES algorithm and generate hash value of original message using SHA. And send it to the receiver along with updated flag value
Receiver receives that encrypted message and decrypts it using AES algorithm and generate new hash value.
Is Hash value matches?
No
Yes
Discard the message and notified to sender
Display Original message on the receiver's screen
STOP

Fig. 2. Flow Diagram of Our Project.

VI. CONCLUSION

Security for SMS is must for preventing our message from different attacks. It's necessary to avoid our message to be interrupted by third person other than sender and receiver. Hence using combine cryptographic algorithms such as PBE, Diffie Hellman Key Exchange algorithm, AES, SHA we provide SMS security solution in Mobile security system. It provides security services such as confidentiality, authentication, integrity and non-repudiation. Using android technology we are following current market trend.

Our project can be used by high level Organizations, military people for sharing their confidential data. We will be providing a robust communication service to the users. Subscribers can easily use this application for the purpose of communication with a high security.

FUTURE WORK

We can improve GUI of an application as well as provide storage of messages in secure form.

REFERENCES

[1] Research Paper on 'A novel peer-to-peer SMS security solution using a hybrid technique of NTRU and AES-Rijndael' by Sameer Hasan Al-bakri and M. L. Mat Kiah, 18 November, 2010.

[2] Research paper on "2011 Review of Mobile Short Message Service Security Issues and Techniques towards the Solution".

[3] Book on "Cryptography and Network Security" By Atul Kahate.

[4] Paper on "Advance Encryption Standard" by Douglas Selent.

[5] Paper on "Public-Key Cryptography Standards: PKCS" by Yongge Wang, Ph.D., University of North Carolina at Charlotte.

[6] http://security.stackexchange.com/questions/5457/which-type-of-encryption-algorithms-android-supports-and-which-would-be-better.

[7] http://techforum4u.com/content.php/356-DIFFIE-HELLMAN-KEY-EXCHANGE-ALGORITHM.

[8] Research Paper on Password-Based Encryption Analyzed by Martin Abadi and Bogdan Warinschi.

[9] http://www.engineersgarage.com.