Secure Transmission of Data Over Short Message Service

Thulasipriya. K[1]
1.UG Scholar Dept of CSE
Adhiyamaan college of engineering.
Hosur, India

Ashwin. M[2]
1.Associate Professor Dept of CSE.
Adhiyamaan college of engineering.
Hosur, India

Abstract:- **Short Message Service (SMS) has been used often in our daily life. When we send an SMS from one mobile to another, the SMS can be sent as plain text. Sometimes, the SMS contains confidential information such as account numbers, passwords and so on. The SMS service providers does not provide any security for the SMS while transmission. Sometimes, the information which is sent will be lost. Secure key distribution is an important concern for security. The most widely used algorithm is Diffie – Hellman Key Exchange. This algorithm is failed to overcome Man-in-the-middle attack. This paper proposes a new algorithm for secure key exchange called Authenticated Key Exchange. The proposed algorithm is simple and flexible and is based on the mathematical logarithms. This algorithm prevents the Man-in-the-middle attack and replay attack.**

Key words- Confidential, Diffie-Hellman Key Exchange, plain text, Man-in-the-middle attack, replay attack.

I INTRODUCTION

Short Message Service is one of the largest growing communication channel to share the information. The SMS concept was first developed by the Friedhelm and Bernard in the France German cooperation GSM, 1984. The first text message "Merry Christmas" was sent by Neil Papworth in 1992 to Richard Jarvis. At first the mobile phones does not have key boards. Papworth typed the SMS in the PC. In 1997, the Nokia i 9000 mobile was introduced with the key board. At first the usage of SMS is very rare. Later in 2000, it has been increased rapidly.

A. Research Problem

Sometimes we send an confidential information such as account numbers, passwords, banking details and so on. But the SMS service provider does not provide any security during transmission. SMS contents are stored in the system network and it can be read or modified by them. During transmission Man-in-the-middle attack and replay attack is possible.

B. Key Contribution

The above contributions can be made possible by Authenticated Key Exchange algorithm. This algorithm prevents SMS from various attacks such as Man-in-the-middle attack and Replay attack. This algorithm uses logarithmic functions so that the sharing of key will be secured. The performance will be increased and the storage space will be reduced.

II BASIC DEFINITION

A. Cryptography

Cryptography is the process of hiding the information from the unauthorized access.

B. Cipher

It is the process of performing encryption and decryption. It converts plain text into cipher text.

C Plain Text

Plain text contains the message which is not in an encrypted format.

D Cipher Text

Cipher text is an encrypted message which can be decrypted based on encryption algorithm.

E Symmetric Key

Sender and Receiver uses the same key for both encryption and decryption.

F Asymmetric Key

Sender and Receiver uses different key for encryption and decryption.

G Confidentiality

Information is protected from the unauthorized access.

H Availability

Information will be available to authorized users without any delay.

I Integrity

Information will not be modified by unauthorized users.

III TRADITIONAL PROBLEM

In our regular messaging system, if an SMS is send from one mobile to another, the SMS will be stored in SMS centre till it receives. At this time the storage space will be wasted. The information can be modified when it is stored. Sometimes, we send the confidential information such as

account numbers, passwords, banking details. To avoid this problem, the information can be encrypted.

IV LITERATURE SURVEY

Previously, various authors have proposed various techniques for SMS security.

In November 1999, [6] the SMS security has been proposed. It uses public key to authenticate the user and stream cipher for encryption and decryption. Stream ciphers are difficult to implement. Stream ciphers do not provide integrity or authentication.

In February 2010, [7] the Secure Extensible Efficient SMS transmission for security. This system allows the two peer to communicate through public key cryptography. The two peers share the same key for both encryption and decryption. It is resistant to brute force attack.

In May 2012, [2] NTRU cryptosystem is implemented in order to overcome to SECSMS. The NTRU cryptosystem has highest speed, fast generation of key, encryption and decryption. This system also shares the same key for both encryption and decryption.

In July 2012, [2] Advanced Encryption Standard algorithm is used for encryption and decryption of SMS. It provides secure, fast and strong encryption of data. There is a confusion of an encryption since the attacker finds difficult to access the data. But the processing speed will be less. It is very complex.

In December 2014, [3] Easy SMS protocol is used to secure the SMS. The symmetric key encryption is used for this protocol. This protocol uses AES algorithm for encryption. This protocol provides lower bandwidth consumption and increases the password strength. This protocol requires more storage space.

In December 2014, [5] it describes about a protocol called SecurdSMS. This protocol uses symmetric key to share the key between two users. SecuredSMS can be activated in the mobile phone using PIN number. It also provides remote locking in case if the phone is stolen or lost. This algorithm is not much secure because same key is used for both encryption and decryption.

V EXISTING WORK

A Diffie-Hellman Key Exchange

The first published public-key algorithm by Diffie and Hellman [8] and is generally referred as Diffie-Hellman Key Exchange. The purpose of this algorithm is to securely exchange a key between two users. This algorithm is based on the discrete logarithms. Discrete logarithm is difficult to calculate. First, we define a primitive root of a prime number ‘p’ as one whose powers modulo ‘p’ generate all integers from 1 to p-1. And if ‘a’ is a primitive root of the prime number ‘p’ then the numbers

a mod p, (a^2) mod p …….(a^p-1) mod p

are distinct and consists of prime numbers from 1 to p-1 in some permutation. For any integer ‘b’ and a primitive root of a prime number ‘p’, we can find a unique exponent I such that

b=a^i(mod p) where 0<=i<=(p-1)

the exponent ‘i’ is referred to as discrete log for ‘b’ for base a mod p

1) Algorithm Description

Suppose two people are communicating, Alice and Bob

Step 1: Alice and Bob shares common public key

A prime number ‘q’
An integer ‘g’ where g<q and is primitive root of ‘q’
Step 2: At Alice: Selects private ‘a’ where a<q then calculates public A = g^a mod q and sends to Bob.
Step 3: At Bob: Selects private ‘b’ where b<q then calculates public B = g^b mod q and sends to Alice.
Step 4: Calculating secret key by Alice: S = B^a mod q
Step 5: Calculating secret key by Alice: S = A^b mod q
Step 6: Alice and Bob now shares the secret key ‘S’ and encrypts the messages using this key. The security of Diffie-Hellman key exchange lies in the fact that, while it is relatively prime it is easy to calculate exponentials modulo a prime, but it is very difficult to calculate discrete logarithms. For larger primes, the task will be considered infeasible.

2) Man-in-the-middle attack

Diffie-Hellman key Exchange is vulnerable to Man-in-the-middle Attack. Suppose Alice and Bob wish to exchange keys, and Darth is the adversary. The attack proceeds as follows:
1. Darth prepares for the attack by generating two random private keys x1 and x2, and then computing the corresponding private keys y1 and y2.
2. Alice transmits ‘A‘ to Bob.
3. Darth intercepts ‘A‘ and transmits ‘y1‘ to Bob. Darth also calculates k2= A^{x2}mod q.
4. Bob receives ‘y1‘ and calculates k1=$y1^b$mod q.
5. Bob transmits ‘B‘ to Alice.
6. Darth intercepts ‘B‘ and transmits ‘y2‘ to Bob. Darth also calculates k1= B^{x1}mod q.
7. Alice receives ‘y2‘ and calculates k2=$y2^a$mod q.

At this point, Bob and Alice think that they share a secret key, but instead Bob and Darth share secret key ‘k1‘ and Alice and Darth share secret key ‘k2‘ in which all future communications are intercepted by Darth, which leads to Man-in-the-middle Attack.

VI ARCHITECTURE

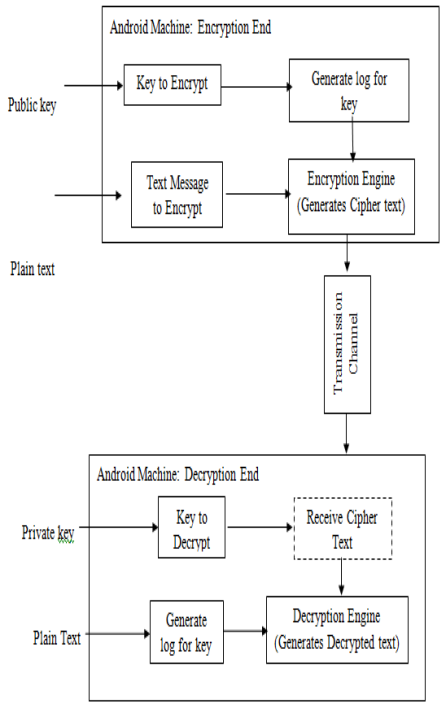

Figure 1. Architecture of Crypto System

A Description

In this paper, we have used two algorithms. One algorithm for sharing the key in a secured manner. Another algorithm for encryption and decryption of messages. Authenticated Key Exchange is used to share the key securely. RSA algorithm is used to encrypt and decrypt the messages. Public key is chosen to encrypt the plain text. The key is chosen and logarithm value is generated for key. The text message is given to the encryption engine to encrypt the plain text. The encrypted text is transmitted via the transmission channel to the receiver end. The receiver receives the cipher text. The receiver uses the private key for decryption. The cipher text is send to the Decryption engine for decryption. The decrypted text is given to the receiver.

VII PROPOSED WORK

Our proposed process describes about the key exchange algorithm. We have considered Man-in-the-middle attack and replay attacks. We have used simple logarithm algorithm for the easier calculation. The design and complexity will be easier.

Suppose Thulasi(T) wants to exchange key with Praveen(P)

Both T and P uses one private key and one public key.

'e' as the public key based on the log.

'x' as the private key

Step 1: T chooses a large prime number G and calculates

$$K1 = \log e (G^x)$$

Step 2: P chooses a large prime number H and calculates

$$K2 = \log e(H^x)$$

Step 3: T sends K1 and Timestamp t1 to P

Step 4: P sends K2 and Timestamp t2 to T

Step 5: T verifies Timestamp 't2' and calculates

$$\text{Key R} = K1 + K2 = \log e(G^x) + \log e(H^x)$$

$$= \log e(G^x H^x)$$

Step 6: P verifies Timestamp 't1' and calculates

$$\text{Key R} = K2 + K1 = \log e(H^x) + \log e(G^x)$$

$$= \log e(H^x G^x)$$

Step 7: By the property of logarithms

$$\log e (AB) = \log e (BA)$$

$$\log e (A^x B^x) = \log e (B^x A^x)$$

$$\log e (AB)^x = x \log e (AB)$$

By using all these properties, we can calculate

$$\log e (G^x H^x) = \log e (GH)^x$$

$$\log e (H^x G^x) = \log e (HG)^x$$

Now

$$\log e (GH)^x = \log e (HG)^x$$

Again we can calculate by the property

$$\log e (GH)^x = x \log e (GH)$$

$$\log e (HG)^x = x \log e (HG)$$

B Elimination of Man-in-the-middle attack

Both T and P uses a secret key 'x' and public key 'e'. If the key is altered in the middle and it is not modified the base will be 'e'. We can calculate $S1 = e^xGH/e^xG$ and $S2 = e^xGH/e^xH$ so that we can easily identify the error.

C Elimination of Replay Attack

Replay attacks are not possible due to the use of timestamps. Both T and P verifies the timestamps before calculating the key in order to eliminate the Replay attacks.

B Algorithm for Encryption and Decryption

To eliminate the Man-in-the-middle attack the RSA algorithm is used. This algorithm uses the public key for encryption and private key for decryption.

Step 1: Select two prime number p and q both p and q should be different.
Step 2: Then calculate n with respect to product of p and q.
Step 3: Calculate the G value by p-1 product of q-1
Step 4: Select a integer e (i.e. gcd(G,e)=1) which is relatively prime to G and it is less than G.
Step 5: Determine d value using ($d\ e^{-1} \bmod Z$)

Step 6: Public key and private keys are generated as e , n and d , n respectively.
Step 7: A plain text is encrypted using the public key by $C= M^e \bmod n$.
Step 8: A cipher text is decrypted using the private key $M= C^d \bmod n$.

The main disadvantage of RSA is it lacks in the performance. The computing time for plain text itself is more. In case of large cipher texts it is not easy to compute. It needs threshold keys to be generated. Generating a threshold key is not a easy task.

VIII CONCLUSION

We have used Authenticated Key Exchange algorithm to share the keys. This algorithm is used for the secure transmission. It overcomes the Man-in-the-middle attack and Replay attack. We have used RSA algorithm to encrypt and decrypt the messages. RSA algorithm is used inorder to increase the performance. Private key used in RSA is protected from unauthorized access. We considered Man-in-the-middle attack and replay attack.

IX REFERENCE

[1]. Oviya.V, Dr.Kirubakaran.S " PEER TO PEER TRANSMISSION OF PASSWORD THROUGH SECURE SMS" in November 2014.
[2]. Rohan Rayarikar Sanket Upadhyay Priyanka Pimpale "SMS ENCRYPTION USING AES ALGORITHM ON ANDROID" in July 2012.
[3]. Narendra S. Chaudhari "EASY SMS : A PROTOCOL FOR END TO END SECURE TRANSMISSION OF SMS" in July 2014.
[4]. Ashok kumar Nanda "SMS SECURITY USING NTRU CRYPTO SYSTEM FOR M-COMMERCE" in June 2009.
[5]. Deepthi Sucheendran, Arun R, Dr. S.Sasidhar Babu, P.Jayakumar "SECUREDSMS A PROTOCOL FOR SMS SECURITY" in December 2014.
[6]. Chi-Chun Lo , Yu-Jen Chen "SECURE COMMUNICATION MECHANISM FOR GSM NETWORK" in November 1999
[7]. Neetesh Saxena , Ashish Payal "ENHANCING SECURITY SYSTEM OF SHORT MESSAGE SERVICE FOR M-COMMERCE IN GSM" in 2012.
[8]. Sakthi Nathiarasan A , Yuvaraj K "SECURE KEY EXCHANGE ALGORITHM - MATHEMATICAL APPROACH" in June 2013.