Secure and Reliable Data Transfer on Android Mobiles Using AES and ECC Algorithm

Mayur Naik, Avinash Sindkar, Pratik Benali, Chetan Moralwar
Students, D.Y. Patil College of Engineering, Akurdi
University of Pune
{naikmayur2, avi2162, pratikcbenali, chetanmoralwar05}@gmail.com

***Abstract* - Sending data and messages are one of the popular ways of communication. When confidential information is exchanged using messages and data, it is very difficult to protect the information from security threats like man-in-middle attack, DoS attack as well as to ensure that the messages and data is sent by authorized senders. There is always a need to protect the information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. Maintaining privacy in our personal communication is something everyone desires. Encryption is a means to achieve that privacy. As sending data and messages through mobile is now widely used as a business tool; its security has become a major concern for business organization and customers. There is a need for an end to end data encryption in order to provide a secure medium for communication. In this paper we describe the method to encrypt the data and messages transmitted through the mobile devices that allow the user to encrypt the data and messages before it is transmitted over the network. This application describes solution that provides reliable and secure data and message transfer that guarantees provision of confidentiality, authentication, and integrity services.**

Keywords – encryption; security; AES; ECC

I. INTRODUCTION

Mobile phones are part of our daily life. Nowadays, mobile phones provide not only communication services, but also many multimedia and other functions. Mobile phones contain private or personal data. This data is saved in a form of phone contacts, SMS, notices in a calendar, photos etc. Protection of the information depends also on a concrete user and they prevent this information from unauthorized access [4]. The new generations of the mobile devices such as the iPhone and Google Android devices are powerful enough to accomplish most of the tasks that previously required a personal computer. Indeed, this newly acquired computing power gave a rise to plethora of applications that attempt to leverage the new hardware. These include but are not limited to Internet browsing, email, messaging, social networking, and GPS navigation. However, mobile devices have to come a long way in terms of security. Organizations have come to realize that these commercially available smartphones will soon have to serve as an integral part of their operations. This requires a level of security that allows for security of data at-rest and on the move to support secure communications [2]. As sending data and messages through mobile is now widely used as a business tool; its security has become a major concern for business organization and customers [1].

There is a need for an end to end data encryption in order to provide a secure medium for communication. Our system will be developing on Android platform which allows the user to encrypt the data and messages before it is transmitted over the network and it describes solution that provides guarantees provision of confidentiality, authentication, and integrity service. It provides double encryption technique to secure the information sent through mobiles. It has been understood that encryption has long been used by militaries and governments to facilitate secret communication. Encryption is now commonly used in protecting information within many kinds of civilian systems Encryption can be used to protect data "at

rest", such as files on computers and storage devices (e.g. USB flash drives). In recent years there have been numerous reports of confidential data such as customer's personal records being exposed through loss or theft of laptops or backup drives. Encrypting such files at rest helps protect the information from disclosure and misuse. Encryption can be classified into two categories symmetric and asymmetric. Symmetric encryption is the process where a single key is used for both encryption and decryption. Asymmetric encryption uses two related keys, one for encryption and the other for decryption. One of the keys can be announced to the public as the public key and the other kept secret as the private key. We are using both the symmetric encryption as well as asymmetric encryption for protecting the data. Wireless networks have experienced a big growing in the last years. From typical Internet services to multimedia applications, all of them need a big amount of bandwidth. For this reason the IEEE has paid much attention according to the improvement of new versions of standard 802.11 [6].WLAN networks allow a good framework to develop much type of services and applications like multimedia messages applications, to send and receive sounds and video, Multicast diffusion of multimedia contents to a group of users depending on their geographical location, etc [5].

Android is an open source and Linux-based Operating System for mobile devices such as smartphones and tablet computers. Android was developed by the Open Handset Alliance, led by Google, and other companies. Android offers a unified approach to application development for mobile devices which means developers need only develop for Android, and their applications should be able to run on different devices powered by Android. The first beta version of the Android Software Development Kit (SDK) was released by Google in 2007 where as the first commercial version, Android 1.0, was released in September 2008. On June 27, 2012, at the Google I/O conference, Google announced the next Android version, 4.1 Jelly Bean. Jelly Bean is an incremental update, with the primary aim of improving the user interface, both in terms of functionality and performance. The source code for Android is available under free and open source software licenses. Google publishes most of the code under the Apache License version 2.0 and the rest, Linux kernel changes, under the GNU General Public License version 2 [7].

II. EXISTING SYSTEM

The messages through mobile phones travels as plain text and privacy of the messages contents cannot be guaranteed, not only over the air, but also when such messages are stored on the handset. The contents of messages are visible to the network operator's systems and personnel. The demand for active messages based services can only be satisfied when a solution that addresses end-to-end security issues of messages technology is available, where primary security parameters of authentication, confidentiality, integrity and non-repudiation are satisfied. The A5 algorithm is an encryption algorithm used in the GSM system that is used to provide voice and data privacy but the A5 algorithm can easily be compromised [1].

Multiple versions of the A5 algorithm exist which implement various levels of encryption [8].

- A5/0 utilizes no encryption.
- A5/1 is the original A5 algorithm used in Europe. A5/1 is a stream cipher used to provide over-the-air communication privacy in cellular telephone standard. It is one of seven algorithms which were specified for GSM use. It was initially kept secret, but became public knowledge through leaks and reverse engineering. A number of serious weaknesses in the cipher have been identified [9].
- A5/2 is a stream cipher used to provide voice privacy in the GSM cellular telephone protocol. A5/2 is a weaker encryption algorithm created for export and used in the United States.

- A5/3 is a block cipher with 128 bit key and 64 bit input and output. It is not secure enough.

A. Security Threats

Understanding the basics of message security opens the door to preventing some common security threats in message usage: [1]

- **Man-in-middle Attack:** This is the network that authenticates users. The user does not authenticate network so the attacker can use a false BTS with the same mobile network code as the subscriber's legitimate network to impersonate himself and perform a man-in-the-middle attack.
- **Replay Attack:** The attacker can misuse the previously exchanged messages between the subscriber and network in order to perform the replay attacks.
- **Message Disclosure:** Since encryption is not applied to message transmission by default, messages could be intercepted and snooped during transmission. In addition, messages are stored as plain text by the mobile networks before they are successfully delivered to the intended recipient. These messages could be viewed by users in the network who have access to the messaging system.
- **Spamming:** While using message as a legitimate marketing channel, many people have had the inconvenience of receiving message spam. The availability of bulk message broadcasting utilities makes it easy for virtually everyone to send out mass messages.
- **Denial of Service (DoS) Attacks:** DoS attacks are made possible by sending repeated messages to a target mobile phone, making the victim's mobile phone inaccessible.
- **Phone Crashes:** Some vulnerable mobile phones may crash if they receive a particular type of malformed short message. Once a malformed message is received, the infected phone becomes inoperable.
- **Message Viruses:** There have been no reports of viruses being attached to short messages, but as mobile phones are getting more powerful and programmable; the potential of viruses being spread through message is becoming great.
- **Message Phishing:** Message phishing is a combination of message and phishing. Similar to an Internet phishing attack using email, attackers are attempting to fool mobile phone users with bogus text messages.

III. PROPOSED SYSTEM

The proposed system allows the user to send the messages and data from there smartphones in an encrypted format. The user can encrypt the data and messages before it is transmitted over the network. This proposed system describes solution that provides reliable and secure data transfer that guarantees provision of confidentiality, authentication, and integrity of the messages and data that are transferred through the network. The proposed system helps for the security of end to end communication between the users who wants to transmit the data or messages through there smartphones. The messages and data will be transmitted in an encrypted format and not in the plain text as in the existing system. At the receiving end the receiver can decrypt the message and data with the appropriate key. As there is a huge amount of confusion and diffusion of the data during encryption which makes it very difficult for an attacker to interpret the encryption pattern and the plain text form of the encrypted data.

This system provides the need of following services:-

- **Authentication:** Confirm true identities between sender and receiver, and prevent impersonation attack from illegal intruders.

- **Confidentiality:** Ensure that decrypted messages or data are accessible only to those authorized senders and receivers.
- **Integrity:** Ensure that receiver can check out that the data or messages that have been sent are not modified.
- **Non-repudiation:** No party can deny the receiving or transmitting the messages or data communicating between them.
- **Availability:** Ensuring that authorized users have access to information and associated assets when required.

In our system the user can send the message and data in three different modes:-

1. **Insecure:** In the Insecure mode the user can send the message and data in the simple plaintext format.
2. **Secure:** In the Secure mode the user can send the message and data in the encrypted format, in these mode our system uses only one encryption algorithm.
3. **Ultra Secure:** In the Ultra Secure mode the user can send the message and data in the double encrypted format using two different encryption algorithms.

Here in the proposed system we will use two different encryption algorithms to provide additional security to the messages and the data.

A. Encryption Algorithms

In the proposed system we will use both symmetric and asymmetric encryption algorithm. Symmetric encryption is the process where a single key is used for both encryption and decryption. Asymmetric encryption uses two related keys, one for encryption and the other for decryption.

1. Advanced Encryption Standard (AES)

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. Originally called Rijndael, the cipher was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who submitted to the AES selection process. AES has been adopted by the U.S. government and is now used worldwide. It supersedes the Data Encryption Standard (DES), which was published in 1977. The algorithm described by AES is a symmetric-key algorithm, meaning the same key is used for both encrypting and decrypting the data [10]. AES is a block cipher .It has variable key length of 128, 192, or 256 bits; default 256. It encrypts data blocks of 128 bits in 10, 12 and 14 round depending on the key size. AES encryption is fast and flexible; it can be implemented on various platforms especially in small devices. Also, AES has been carefully tested for many security applications [11].

Algorithm:-

Step1: KeyExpansion-round keys are derived from the cipher key using Rijndael's key schedule

Step2: Initial Round

1. AddRoundKey

Step3: Rounds

1. SubBytes-a non-linear substitution step where each byte is replaced with another according to a lookup table.
2. ShiftRows-a transposition step where each row of the state is shifted cyclically a certain steps.
3. MixColumns-a mixing operation which operates on the columns of the state, combining the four bytes in each column.
4. AddRoundKey

Step4: Final Round (no MixColumns)

1. SubBytes
2. ShiftRows

3. AddRoundKey

2. Elliptic curve cryptography (ECC)

Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Elliptic curves are also used in several integer factorization algorithms that have applications in cryptography, such as Lenstra elliptic curve factorization. The use of elliptic curves in cryptography was suggested independently by Neal Koblitz and Victor S. Miller in 1985. Elliptic curve cryptography algorithms entered wide use in 2004 to 2005. The algorithm was approved by NIST in 2006 [12]. Elliptic curve algorithm has ability of providing high security with smaller key size makes it very useful in resource-limited device such as mobile phone. This has put elliptic curve at an advantage over the RSA and Elgamal algorithm [1].

Algorithm:

Stepl: Consider a message 'Pm' sent from A to B.

'A' chooses a random positive integer 'K', a private key 'nA' and generates the public key PA=nA *G and produces the cipher text 'Cm' consisting of pair of points Cm={kG,Pm+kPB} where G is the base point selected on the Elliptic Curve, PB=nB*G is the public key of B with private key 'nB'

Step2: To decrypt the ciphertext, B multiplies 1st point in the pair by B's secret & Subtract the result from the 2nd point Pm + kPB - nB(kG) = Pm + k(nB G) - nB(kG)=Pm [1].

CONCLUSION

In this paper we have worked for the encryption of the messages and data for securing it from the unauthorized person. The proposed technique combines the symmetric encryption and asymmetric encryption algorithm. The proposed technique encrypts the message and data using Advanced Encryption algorithm and Elliptic Curve algorithm. After this step the encrypted message and data is transmitted through there smartphone from the sender to the receiver over the network. The receiver at the receiving end will decrypt the message or the data using the appropriate key. The advantage of this technique is achieving the protection criteria such as confidentiality, authenticity and integrity of the messages and data transmitted between two communication parties. Thus, this technique provides for the secure and reliable end to end transmission of messages and data between the sender and receiver.

REFERENCES

[1] R. Chavan and M. Sabnees, "Secured Mobile Messaging," *IEEE-2012*, pp. 1036-1043, 978-1-4673-0210-4/12.

[2] Z. Wang, R. Murmuria and A. Stavrou, "Implementing and Optimizing an Encryption Filesystem on Android," *IEEE-2012*, pp. 52-62, 978-0-7695-4713-8/12.

[3] M. Agoyi and D. Seral, "SMS security: an asymmetric encryption approach," *IEEE-2010*, pp. 448-452, 978-0-7695-4182-2/10.

[4] D. Lisonek and M. Drahansky, "SMS Encryption for Mobile Communication," *IEEE-2008*, pp. 198-201, 978-0-7695-3486-2/08.

[5] P. Lopez, D. Gracia, S. Almagro, J. J. Alcaraz and F. Cerdam "Development of cooperative application for sending SMS on Wifi mobile phones," *IEEE-2008*, pp. 274-278, 978-0-7695-3367-4/08.

[6] http://www.ieee802.org/15/ Institute of Electrical Engineers. The Working Group for Wireless Personal Area Networks (WPAN).

[7] Android, http://www.tutorialspoint.com/android/androidtutorial.pdf.

[8] A5 Algorithm, http://www.gsm-security.net/faq/gsm-encryption-algorithm-a5-cipher.shtml.

[9] A5 Algorithm, http:// en.wikipedia.org/ wiki/A5/1

[10] Advanced Encryption standard, http://en.wikipedia.org/wiki/Advanced_Encryption_Standard.

[11] Nishika and R. Yadav, "Cryptography on Android Message Applications- A Review," International Journal on Computer Science and Engineering (IJCSE)-2013, pp. 362-367, 0975-3397.

[12] Elliptic Curve Cryptography, http://en.wikipedia.org/wiki/Elliptic_curve_cryptography.