ISSN:0975-9646

A Proposed Security Framework for Enhancing User Privacy on Android Platform

Ritu Talreja[1], Dilip Motwani[2]

Information Technology Department, Computer Engineering Department
Vidyalankar Institute of Technology(Mumbai), India

***Abstract*— Communication through mobile phones, Tablets and PDAs (Personal Digital Assistant) is the new trend in the era of globalization. In day-to-day activities, sensitive information through mobile phones is exchanged among the users. This sensitive information can be in the form of text messages, images, location, etc. Massachusetts Institute of Technology (MIT), Harvard and Carnegie- Mellon did research on Mobile Applications and found that applications leak huge amount of information to the third party servers. 73 per cent of 55 applications were found to leak private information of the users [7]. Transmission of files securely on Android is a big issue. Therefore it is essential to enhance the privacy of user data on Android Platform. The main objective of this project is to enhance the privacy on Android Platform by allowing transmission of data (text messages, location, images and .txt files) in encrypted format. By doing so, the integrity and confidentiality of data is maintained.**

***Keywords*— Android, Privacy, Encryption, Transmission, AES, Blowfish, Triple DES, RSA.**

I. INTRODUCTION

Technology trends in both hardware and software have driven the hardware industry towards smaller, faster and more capable mobile hand-held devices that can support a wider-range of functionality and open source operating systems. Mobile hand-held devices are popularly called smart gadgets (e.g. smart phones, tablets, e-book readers). These new generations of the smart gadget devices such as the iPhone and Google Android devices are powerful enough to accomplish most of the tasks that previously required a personal computer. However, smart gadgets have to come a long way in terms of security and privacy [10].

Android is a popular open source smart-phone and tablet operating system developed by Android, Inc, which was later bought by Google [8]. According to IDC 2014 Report, 1.3 billion Android based mobile phones were shipped during the third quarter of 2014, and as a result, it captured over 84% of smart-phone market[5]. Android was originally based on Linux kernel 2.6 [9]. But to bring innovation and value to customers, Android applications are modified or extended extensively to use sophisticated hardware and software through the platform. The majority of users not only share casual greetings but also shares important data such as banking details, passwords, personal pictures, files and videos etc. In some cases, this data may also include very private information reserved for personal viewing of an authenticated recipient. Therefore, encrypted transmission of data plays an important role in data security. Here we propose an approach to transmit the data in encrypted format using different encryption algorithms.

II. BACKGROUND INFORMATION

A. *Android Architecture*

Android Operating System is a stack of software components which is roughly divided into five sections and four main layers as shown below in the architecture diagram:

Linux Kernel

This layer provides a layer of abstraction between device hardware and it contains all the necessary hardware drivers. Kernel also handles the networking.

Libraries

There are multiple libraries which provide support for storage and sharing of application data, playing and recording audios and videos, and libraries which provide support for Internet security.

Android Runtime

Android Runtime (ART) is the part of second layer from the bottom. The key component of this section is Dalvik VM which is specialized for Android only. ART also contains set of core libraries which helps developers to code variety of Android applications using standard Java programming language.

Application Framework

This layer provides high-level services to the layer above it. Application developers use these services for developing applications. Activity Manager, Content Providers, Resource Manager, Notifications Manager and View System are the key services provided by the Application Framework.

Application

It is the top most layer of the architecture. All types of applications like contacts, music, calendar, etc. are installed at this layer only [6].

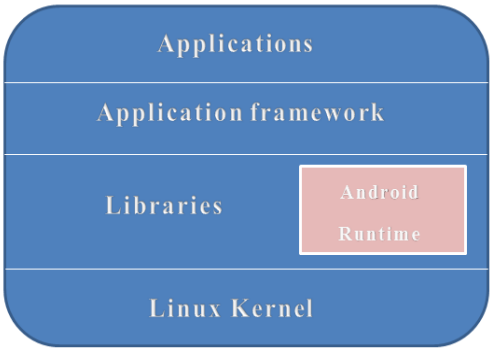

Figure 1: Android Architecture [5]

B. *Encryption*

Encryption is the process of converting normal data or plaintext to cipher text by applying mathematical transformations or formulae. These mathematical transformations or formulae used for encryption processes are called algorithms [1]. Cryptography is the technique of hiding information by encrypting the message. The art of protecting information (encryption) into an unreadable format (encrypted text), is called cipher text.

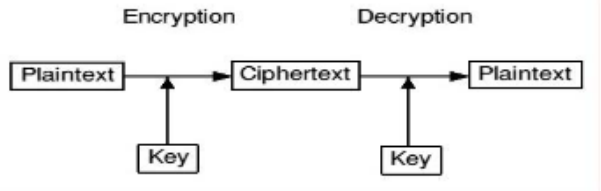

Figure 2: encryption Process [1]

For the proposed system, we have used four encryption algorithms: i) AES (Advanced Encryption Standard) ii) Triple DES (Data Encryption Standard) iii) RSA (Rivest, shamir,Adleman) Algorithm iv) Blowfish Algorithm.

III. RELATED WORK

A. *Secure Storage*

Encryption Filesystem on Android (EncFS) provides the encryption for the file system on Android Platform. I proposed methodology, the data at rest including physical partition on the device and removable storage card is encrypted using user provided password. The encrypted file system is mounted only after successful password verification with user at system boot up.To implement EncFS, three components are used Kernal FUSE library support, user space *libfuse*, EncFS binaries. To make an encryption file-system work on Android, a modified bootstrapping process and password login was integrated into the operating system framework. It supports AES and Blowfish block cipher algorithms for encryption.

File system encryption can only protect the data kept on any external or internal storage but not data in the memory or over the network. Encryption file system is also vulnerable to cryptographic attacks such as known-plaintext attack or side channel attacks against its cryptographic module. Using EncFS incurred a 20 times overhead on performing file operations. [3]

B. *Secure Storage and Transmission*

In **[2]**, Ma Licui, et al. proposes a method of data protection by using the encryption mechanism. Sensitive data here are stored in Android Phone in encrypted format. SDKEY is mainly composed of SD controller, CPU and Secure encryption module. SDKEY-based security encryption module supports basic encryption and decryption such as symmetric, asymmetric and hash, while also provides sensitive data storage area and large capacity storage area. In which sensitive data storage area is used for storing keys and sensitive data, large-capacity storage area is used to store file data, encrypted data and the user's PIN cypher. SDKEY is connected with the Android mobile phone via Micro-SD interfaces.

For secure transmission purpose, Zero-key exchange algorithm is used. Zero key exchange mechanism is designed for data encryption transmission without negotiation of encryption key. In between the two parties when data is exchanged, the data goes through three communications and four encryption and decryption.

This mechanism consumes more bandwidth on the communication channel. This algorithm has trade of between the speed and channel resource. It may not be applicable to all scenarios. Also, another problem with this approach is that there is a need of another hardware device called SDKEY device which is not convenient for user to carry every time.

IV. PROPOSED SYSTEM

The proposed framework (SecTrans) focuses on maintaining the data integrity and confidentiality by encrypting the data before transmission takes place. The proposed system makes use of Google Cloud Messaging Service (GCM) for data transfer between an android device and server and android device to another android device. There are two phases of the project. In the first phase, the user is asked for the registration through the Android application. Upon successful registration, GCM Server issues registration id to android device. This GCM id is valid only for that particular Android device through which it is registered **[4].**In the second phase, the actual data transmission takes place. Here the user has multiple options to transmit data i.e. the user is provided with list of algorithms to choose from; user can transmit the text messages, images, and location as well as .txt files. User can send messages to individuals and groups in encrypted format. The proposed system also allow user to broadcast the message to all users in the contacts. Four different algorithms are used for encryption and decryption: i) AES ii) Triple DES iii) RSA iv) Blowfish. Currently only two algorithms i.e. AES and Blowfish support the Image and .txt file encryption and decryption. The following diagram represents working of proposed system:

STAGE 1: USER REGISTRATION

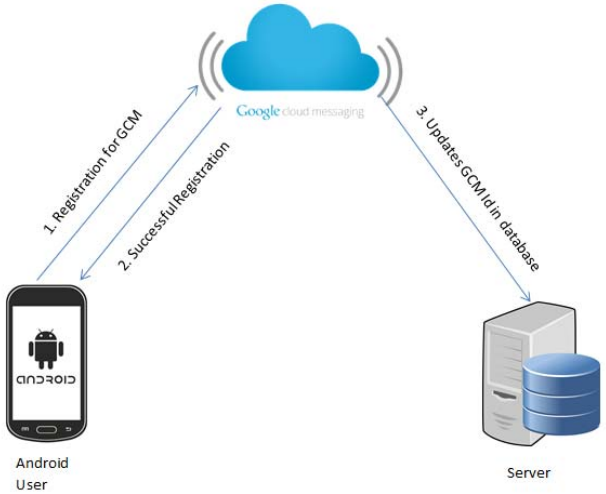

Figure 3: user registration

Steps:

1. First, User enters user name, password, email address and phone number through SecTrans Application.
2. These details go to the GCM server for registration.
3. Upon successful registration, GCM server issues registration id to android device.
4. User name and this Id is stored in the server databsase.

STAGE II: DATA TRANSMISSION:

It is mandatory that user first has to be registered with the SecTrans for transmitting the data in an encrypted format.

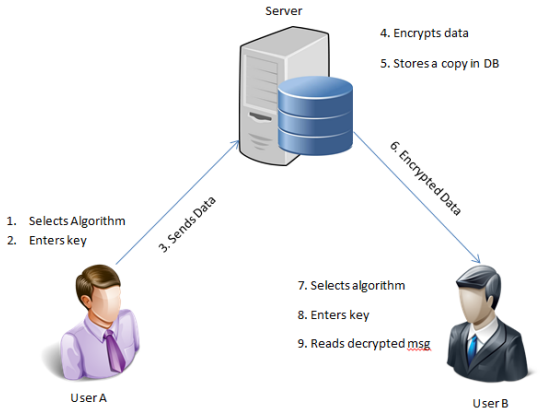

Figure 4: Data Transmission through SecTrans

Steps:

1. For transferring data, User A has to select the algorithm from the list for data encryption
2. User enters the encryption key.
3. User sends the data; data can be in form of text, images, location and .txt files etc.
4. At server side, the data is encrypted
5. Encrypted copy of data is stored in the database of the server.
6. User B receives the data but this data is in unreadable format.
7. User B enters the algorithm same as User A.
8. User B enters the encryption key and message is decrypted.
9. Now the data is in readable format.

The proposed framework not only provides privacy during the transmission but also files (images and .txt files) transmitted through this application are kept in encrypted format in the mobile phone.

V. RESULTS AND ANALYSIS

For the experiment purpose, we selected a small text message as "hello how are you" and we encrypted this message using all the four algorithms. The amount of time required for encrypting the message and space required by the message after encryption is shown below in table.

TABLE I
TIME REQUIRED FOR ENCRYPTION

Algorithm	Time (milliseconds)	Space (bytes)
AES	0	64
Triple DES	40	32
RSA	7622	64
Blowfish	10	32

Here, RSA among all takes much time to encrypt the message whereas AES takes the least time to encrypt the text messages. Space required after encryption is 32 bytes for Triple DES and Blowfish whereas AES and RSA algorithms consume more space of 64 bytes.

VI CONCLUSION

In this paper, we studied about the android framework and tried to understand the threat to its privacy. To deal with the data privacy issue on Android platform, we proposed a security framework which uses four different encryption algorithms to transmit user data in an unreadable format and all the files (images and .txt files) sent using this framework are stored in encrypted format. This framework helps in enhancing user privacy on Android platform and maintains data integrity and confidentiality. The limitation for this framework is that it can encrypt only files which are transmitted using this framework and not the entire phone storage. In future, we will try to provide privacy for complete storage on Android mobile phones.

REFERENCES

[1] Rajdeep Bhanot and Rahul Hans, "A review and comparative analysis of various encryption algorithms", International Journal of Security and Its Applications, Vol. 9, No. 4 (2015), pp. 289-306.

[2] Ma Licui, Li Meihong, Li Lun, Du Ye and Zhang Dawei, "A SDKEY-based Secure Storage and Transmission Approach for Android Phone", 2014 IEEE International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery(2014), pp. 1-6.

[3] Zhaohui Wang, Rahul Murmuria, Angelos Stavrou," Implementing and Optimizing an Encryption Filesystem on Android", 2012 IEEE 13th International Conference on Mobile Data Management (2012), pp. 52 – 62.

[4] Working of GCM, http://www.webgeometrics.com/know-how-gcm-push-notifications-works-on-android-devices/, accessed on May, 2016

[5] Smartphone os market share, q3 2014: http://www.idc.com/prodserv/smartphone-osmarket-share.jsp, accessed on April 2016.

[6] Android Architecture, http://www.tutorialspoint.com/android/android_architecture.htm, accessed April 2016.

[7] Information leaks on Android: http://news.thewindowsclub.com/ios-android-apps-found-leaking-sensitive-user-information-80843/, accessed March, 2016.

[8] Google buys android for its mobile arsenal: http://www.bloomberg.com/bw/stories/2005-08- 16/google-buys-android-for-its-mobile-arsenal, and accessed march 2016.

[9] Maker, f., chan, y., a survey on android vs. Linux, university of California, 2009, pp. 1- 10

[10] Kirti P. lokhande and Avinash Wadhe, "Security in Android File system" , Volume 3 of International Journal of Advanced Research in Computer Science and Software Engineering, 2013.