ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 6, July 2017

Providing Privacy and Security for SMS and Call Data in Android

Vamsi Krishna.Y[1], Kunal S Thali[2], Dayananda P Naik[3]

Associate Professor, Department of Information Engineering, Sri Krishna Institute of Technology, Chikkabanavara, Bangalore, India[1]

U.G Student, Department of Information Engineering, Sri Krishna Institute of Technology, Chikkabanavara, Bangalore, India[2]

U.G Student, Department of Information Engineering, Sri Krishna Institute of Technology, Chikkabanavara, Bangalore, India[3]

ABSTRACT: In the present generation the number of people using the Smartphone has drastically increased, In the survey it says that about 70% of the Smartphone users are using Android operating system cell phones and rest are using IOS, SYMBIAN, BLACKBERRY etc. The applications which are installed in the cell phone will be having access to the user data. Misuse of this sensitive data may lead to data leakage;this can be done with the help of malicious applications. These applications will give access to the user's sensitive data. This type of problem will arise when the user won't have control over the application capabilities which will be asked upon installation. In this paper we will develop an application which will secure the user SMS and CALL data whenever the context is met, i.e Time or location. Whenever the context is met no third party applications can fetch users SMS or CALL data.

KEYWORDS: Context-based access control, Smartphone, Privacy, Data Security, Data Leakage, Mobile Application.

I. INTRODUCTION

Now a days Smartphone's are playing very important role in day to day life. Based on the survey 70-80% of people are using smart phones that are available in the market. Smartphone is a mobile phone which offers advanced technologies with functionality similar to a personal computer. While offering a standardized platform for application developers a smart phone performs as complete operating system software. With the growing speed of technological advancement, Smart phones have become the essential component of our daily performance. The application developers are taking the advantage of these capabilities in order to provide new or enhanced services to their applications. For example Samsung mobile company released a unique S Bike Mode in its J series. The application will need some sensitive data in order to perform the task . i.e we can use the S Bike mode NFC tag and tap a compatible device on it or long press the power button and activate the feature from there[1].In other words we can say that the application will use one or the other data to perform the task. Leakage of this sensitive data may breach to security and privacy risk. So user must secure his personal data. There are many applications which will collect this type of information and sell it to third parties. These applications are called as malicious applications. Malicious applications are the ones which will grant the access to the user's data without the knowledge of the user. Users will not be mobile, they will be roaming all over the city in such situations user may unknowingly expose his personal details to some third party which will be so dangerous. In other words we can say that there is lack of security for the user's data. Protecting the user data has become a very big hurdle for the users. There have been many methods to improve the security of the user data, one among them is context-based access control (CBAC) mechanism systems that allows Smartphone users to set configuration policies over their applications' usage of device resources and services at different contexts. Through the CBAC mechanism, users can, for exampleset privileges for device applications when he is in some confidential meetings, and device applications may re-gain their original privileges when the user is in some free space [2].

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 6, July 2017

Modifying the android operating system is not that easy task it will require years of effort and all other mobile companies should agree for the changes in android operating system which is also a big hurdle to deal with. To misguide the intruder we can provide virtual space and make the intruder to feel like what's the data present over there is real data but actually it is some unwanted data or we can say some dummy data but the intruder will think that the data which he got was the user personal data where as it was some unwanted data [3].The drawback here is to create a virtual space we need extra piece of memory, for example if the user is using 2Gb of memory he will be needed another 2gb for creating virtual space, in other words we can say 2n of the memory will be used where n is the space which the user actually using. To overcome this issue we are implementing an android application which will restrict third party applications by accessing our Call or SMS Data. The application will be having two constraints that is Time and Location. The user must set these constraints if he is having any confidential meeting he can set that time or he can simply enter the location. Our application will verify it with the constraints entered by the user if it is matching the constraints then it will protect the SMS or Call data which will come at that particular time or particular location which is entered by the user

II. BACKGROUND

Here we will cover the overall history of the android operating system, api .

2.1 ANDRIOD

2.2.1 OPERATING SYSTEM AND API

Android Inc. was founded in Palo Alto, California in October 2003 by Andy Rubin, Rich Miner, Nick Sears, and Chris White. Android is a mobile operating system developed by Google, based on the Linux kernel and designed primarily for touch screen mobile devices such as smartphones and tablets. Android's user interface is mainly based on direct manipulation, using touch gestures that loosely correspond to real-world actions, such as swiping, tapping and pinching, to manipulate on-screen objects, along with a virtual keyboard for text input. A virtual keyboard for text input.

Android's source code is released by Google under an open source license, although most Android devices ultimately ship with a combination offree and open source andproprietary software, including proprietary software required for accessing Google services [4].

2.2 LOCATION DETECTION METHOD

Location is the identification or estimation of the real-world geographic location of an object, such as a radar source, mobile phone, or Internet-connected computer terminal. In its simplest form geolocation involves the generation of a set of geographic coordinates and is closely related to the use of positioning systems, but its usefulness is enhanced by the use of these coordinates to determine a meaningful location, such as a street address.

For either geolocating or positioning, the locating engine often uses radio frequency (RF) location methods, for example Time Difference Of Arrival (TDOA) for precision. TDOA systems often utilize mapping displays or other geographic information system. When a GPS signal is unavailable, geolocation applications can use information from cell towers to triangulate the approximate position, a method that is not as accurate as GPS but has greatly improved in recent years [5].

In this paper we will make use of the mobile location only that is with the help of GPS (Global Positioning System) because the accuracy when we use GPS will be higher when compared to other location detection scheme. We can detect the location even through internet but the accuracy of the GPS will be more. For example the GPS might give approximately 3m to 30m accuracy where as an internet based location detection will give an accuracy of 30 to 300m.

III. OVERVIEW OF THE MODEL

Here we will present the overview of our application like how exactly does it work and which all components plays very important role Fig 1 will illustrate the whole architecture which will be explained further.

Our framework consists of user interface, SMS receiver, Telephony Manager, Preference manager, SMS Decoder, Broadcast event manager.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 6, July 2017

2.3 System Architecture

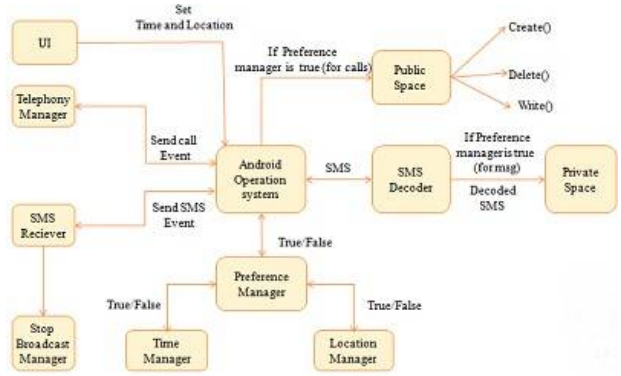

Fig. 1. System Architecture, These are the main components required in order to secure SMS or call data.

User Interface:

In this module the user can set Time or Location. For example if he has a confidential meeting at 2 pm - 4pm , if he sets the Time as 2 pm – 4pm then what ever Calls or Sms he will be getting between that time period will be secured and no other third party applications can access them. In the same way he can also set the Location of the place, if the location is matching the context then the data will be secured.

Telephony Manager:

In this module whenever a call comes to the user cell phone it will be first directed to this , the operating system of android is the one which will forward the call to this module. This manager is useful because once we get the call it will ask the android operating system to check the preference from the preference manager. If the value returned by the preference manger is true then it will be stored in private space so no other third party applications can access these information. If the value returned by the preference manager is false then it will be stored in public space.

Sms Receiver:

This module is same as Telephony manager the only difference here is instead of call data it will look for SMS data.

Preference Manager:

This is the one which is responsible for verifying whether the given context is true or false, It will be connected to the Andriod operating system. When ever new message or call arrives the Andriod operating system will ask this prefernece manager wether the given condition matches the given context or not , if it is matching then the operating system will not give either the message data or the call data for any third party application by storing it in the private space.

Alarm Manager:

In this manager the user context , i.e the time will be recored , when then Prefernece manager is invoked by the Andriod OS to check wether the condition is matching the context , then it will invoke the alarm manager to check wether the time is matching the condition , If it is matching, then the alarm manager will send true to prefernce manager and the same will be returend to the Andriod OS, else false will be returned.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 6, July 2017

Location Manager:
In this manager the user context , i.e the location will be Fetched , when the Prefernece manager is invoked by the Andriod OS to check wether the condition is matching the context , then it will invoke the alarm manager to check wether the Location is matching the condition , If it is matching, then the alarm manager will send true to prefernce manager and the same will be returend to the Andriod OS, else false will be returned.

SMS Decoder:
In this module, when ever an SMS arrives it will be having two fields that is number field and another is text field. These two fields should be sepatared in order to get what the actual data is. The SMS deocoder is the module which will separate the number and data field , the number field will be discarded and the text field will be stored and it will ask the operating system of android to check the preference with prefernece manager, if any of the preference is matichin then we will store the SMS data in private space else wi e will store it in public space.

Private Space:
This is nothing but the privste database where we can store the SMS data. The data which will be stored here will be encrypted using RSA Algorithm. The encryption is done inorder to secure the data. The data will be stored here if and only if the constrains are matching . i.e the os will check the preferences in preference manager ,if it is matching then the SMS data will be stored here.

Public Space:
Public space is nothing but the normal data base where all the sms and call data will be stored. In case of Call data, if the preferences are matching in preference manager that particular call will be dearched and deleted from public space else it will be stored. To search where exactly the call recording is stored we will make use of filetree algorithm.

Broadcast Event Manager:
When the preference manager returns true for SMS data , since no other applications shuld recive the secured data we will tell this manager to not to give this sms data to any third party applications. In other words this managerwill stop the broadcast of the SMS data to other third party applications.

IV. IMPLEMENTATION

In this section, we will discuss the major components of our proposed system, i.e the main modules required in order to secure SMS or Call data.

4.1 APPLICATION MODLE

Here the user is able to set the context of our project i.e. Time or Location. If the user has some Confidential Meeting or if he is sharing any pin which is highly confidential at that time the user may set the timing's or he may just ping the location's longitude and latitude in the interface of our application. These data will be stored in the database of the Time Manager (Alarm manager, in case of time) or Location manager (in case of location) which is present in the Preference manager.

4.2 SMS / CALL Receiver Module

Usually the user will be getting sms / calls to his cellphone, wheneversomeone send sms or someone calls to the user it will be directed to this module i.e. if an Sms arrives it will be directed to the sms receiver module . In the same whenever user gets a call it will be directed to Telephony manager (Call receiver). In case of arrival of the message it will be sent to sms decoder via android operating system. The job of the sms decoder is to decode the data field(message field) and the number field(The person who has sent the message). Once the sms decoder job is done then it will call the next module. As said earlier in case of call wheneversomeone calls the user it will be directed to Telephony manager, here there are no fields like it was in message part (message field and number field) , so it will

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 6, July 2017

directly call the next module.

4.3 PREFERENCE MANAGER:

This module will contain Alarm manager and Location manager the main aim of preference manager is to check whether the context is matching or not, in other words whenever this module is invoked it will check for the values present in Alarm manager or Time manager i.e. it will check whether the user data and the data which is stored in the database of Alarm manager or Location manager is matching or not if it is matching then the data will be stored in private space which indeed tell that the data is secured . Fig 2 will illustrate the verification of the time context, Here the time will be set by service provider or sometimes we can manually set the time these time will be fetched by the Time manager (Alarm manager) and it will compare the same with the data which is stored in database of the Time manager which is given by the user if it is matching then the data will be stored in private space or it will be stored in public space. In the same way Fig 3 will illustrate the verification of the Location context, We can get the location by many means but we are concentrating only on GPS and Cell towers, the location manager will fetch the Location and it will compared with the data which is stored in database of the Location manager which is given by the user, if it is matching then the data will be stored in private space or it will be stored in public space.

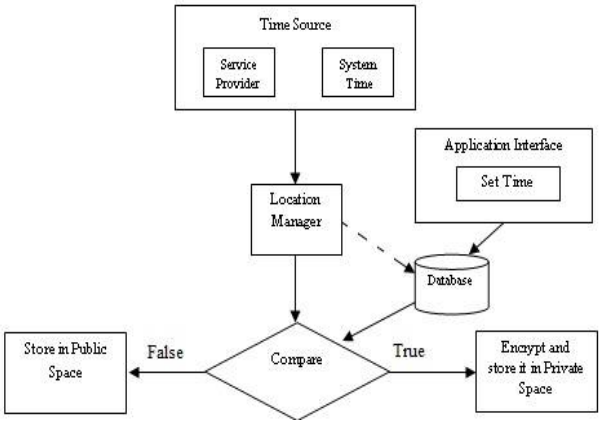

Fig. 2 Verifying the Time, if the location is matching the context then the data will be secured(private space) else it will be stored in public space.

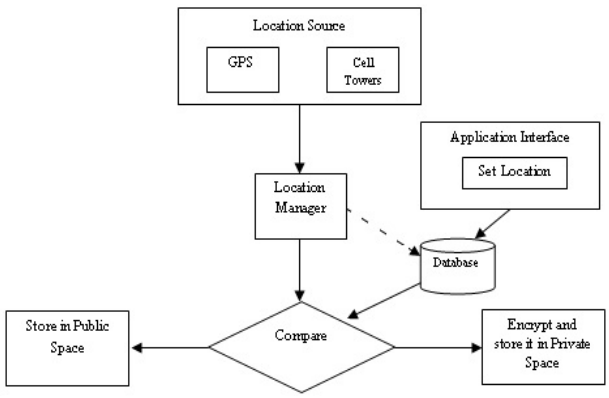

Fig. 3 Verifying the location, if the location is matching the context then the data will be secured(private space) else it will be stored in public space.

4.4 ENCRYPTOR

In the above model, if the preference manager returns true then the sms data which is decoded in the sms decoder will come to this module. The main aim of this module is to encrypt the sms data and store it in private space. In order to encrypt we will be using RSA Algorithm, here we will use 16 bit encryption and then we will store it in private space. Private space is nothing but we will store our data in some other folder which will not be known to third party applications, if they come to know the place where we will store the sms since it will be encrypted the intruder will not understand and hence we will improve the security of the data. In case of call's we are not encrypting anything. If the value in the preference manager is true , then we will find the storage path where exactly the call data will be stored using FILETREE Algorithm, as soon as the user will end his call conversation that particular file will be deleted. So no other third party applications can fetch that data.

4.5 REPOSITORY

Repository is nothing but the storage, In our proposed system we will make use of two kinds of repositories i.e Public Space and Private Space. Public Space is the one where all the SMS and Call data will usually be stored. i.e whenever a message or call comes it will usually be stored in the system defined user storage this storage is called as public storage. Private storage is nothing but the storage which will be located separately in other place in order to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Special Issue 6, July 2017

improve the security of the data. In other words in order to secure the user data we will define a storage which we will call it as private storage , the path of the this storage will not be known to any other applications so it will be hard to fetch the data which is stored in private space, the data will be stored here if only if the value in the preference manager is true. If the value in the preference manager is true then it will send the data to encryptor as discussed earlier and the data will be encrypted and then it will be stored in the private space. If any third party applications by mistakenly comes to know the path of the private storage also since the data will be encrypted the intruder will not understand what is the data which is actually present in the private space.

V. CONCLUSION

In this paper we are developing an application which is used to secure user sms and call data. Here we are mainly concentring on two constraints that is Time and Location. The user is free to set one among this two constraint, we will check the above two constraints with the system. i.e. the time will be cross verified with the system time in the same way the location will be verified with the system location (GPS or Cell tower) if any of this constraints are true then we will store the sms or calls which will come under that constraints into Private space in order to provide security to the user data. If the constraints do not match then we will store the data in public space.

REFERENCES

[1] Wikipedia, (2016). Samsung Bike mode wikipedia. [Online]. Available: https://www.sammobile.com/2016/06/01/how-to-use-s-bike-mode-on-samsungs-galaxy-j-smartphones/
[2] Bilal Shebaro, Oyindamola Oluwatimi, and Elisa Bertino," Context-Based Access Control Systems for Mobile Devices," in Proc vol 12, no 2 ieee transactions on dependable and secure computing , (March/April 2015), pp 150-163.
[3] R. Templeman, Z. Rahman, D. J. Crandall, and A. Kapadia, "Placeraider: Virtual theft in physical spaces with smartphones," in Proc. 20th Annual Netw. Distrib. Syst. Security Symp. (NDSS), Feb. 2013
[4] Wikipedia. Android Wikipedia.[Online]. Avalable: https://en.m.wikipedia.org/wiki/Android_(operating_system)
[5] Wikipedia. Location Detection Methods Wikipedia.[Online]. Avalable:**https://en.wikipedia.org/wiki/Geolocation**