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

Privacy and Data Security through Middleware for Android Using Context Based Access Control

Vamsi Krishna.Y[1], Manasa.D[2], Sushmitha Pawar.S[3]

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

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

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

ABSTRACT: Over the last decade mobile phones have enormously increased their popularity. People are tending to use Smartphones which has different operating systems Example: Android, IOS, windows etc. Let us consider android operating system which was developed by Google based on Linux kernel .Android's user interface is mainly based on direct manipulation .Other than operating system there is computer software that provides service to the software application which is called as middleware. Anything between the kernel and the user application is considered as middleware. The main focus of this paper is to protect the data from malicious applications which are trying to access our personal data and misuse them and also to provide privacy in the device. For achieving this we use context based access control mechanism which is embedded in the middleware of the device. The contexts considered are Time and Location.

KEYWORDS: malicious applications, context based access control,Middleware.

I. .INTRODUCTION

Nowadays smartphone devices are playing vital role in communication and entertainment. Based on the survey 70-80% of people are using smartphones that are available in the market. And smartphones are more useful in terms of computational capabilities; these varieties have become an advantage for the application developer in order to provide new and enhanced features to their applications. There are different operating systems which are embedded in smartphones; one of the widely used OS is Android. A key feature of modern android mobile device is a centralized service for downloading third party applications. There are some applications which gain access to our sensitive data and resources such apps are called as malicious applications. These data will be misused which may lead to privacy breaches and data leakage. In our paper the focus is to protect user's sensitive data through Middleware software.

Middleware is a interface between kernel and user application. The function such as gesture recognition or speech recognition is usually processed by some middleware, and the results are transmitted to user application. Development in middleware is better than application layer development from the career perspective in terms of money and other opportunities .In this paper, the system proposes an access control mechanism where the working of the context differentiates between closely located subareas within the same location and time. So that context based access control restriction can be specified and enforced. In this concept the privileges will be set in middleware irrespective of the applications.

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

II. BACKGROUND

In this section, we cover information about the previous development based on context based access control in android system.

2.1 ANDROID

2.1.1 Android operating system

Android is an operating system for mobile devices which was developed by Google based on Linux kernel. They are mainly developed for touch screen devices such as smartphones, tablets etc. they are based on direct manipulation, Using touch gestures such as typing, swiping, scrolling, tapping etc. They have keyboard which is used for giving characters as input.Android provides applications which extend the functionality of the device enormously. They are usually written using software development kit and java programming language. Android also has a great selection of third party applications which can be downloaded through APK's or from play store.

2.1.2 Permission system

Android's permission system works when the user install the application to his mobile. Every application has their own permissions which must be agreed by the user while installing the applications. If the permissions are denied, the user cannot install the application. Installation process stops. The permissions which are considered by the applications is to provide the privileges for accessing the data and resources.

2.2 MIDDLEWARE

Middleware provides services to the user applications. It is the interface between the operating system and application. It makes easier for software developers to implement communication by using input and output. This helps in focusing on particular purpose of the application. The access services for databases are characterized by Middleware. Middleware can be divided into two categories. One that provides human-time services and the other that performs in machine time.

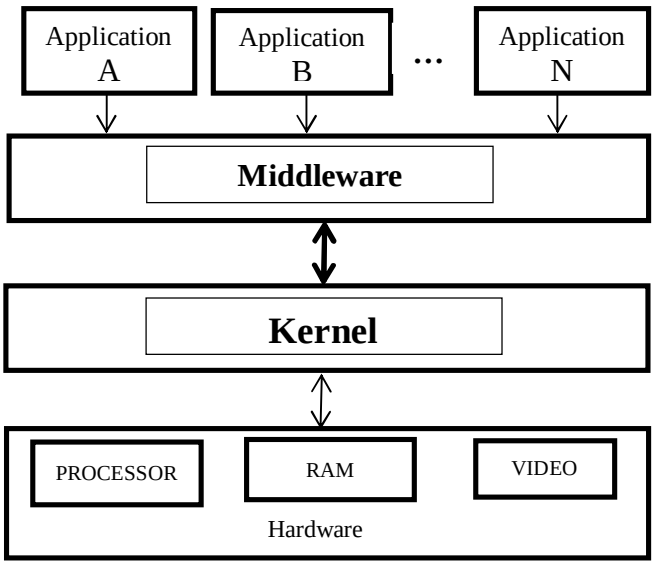

Fig1. Middleware

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

III. ACCESS CONTROL MODEL

In this section, we present an overview of our access control framework through describing its components and the role of its entities.

3.1 SMS RECIEVER: The proposed module is helpful to detect the SMS when any new SMS arrives to the mobile. So that further work may not be that difficult to cope with

3.2 CALL RECIEVER: This module is used to receive the call.

3.3 POLICY MANAGER: The Policy Manager (PM) represents the interface used to create policies, mainly assigning application restrictions to contexts. It mainly gives control to the user to configure which resources and services are accessible by applications at the given context provided

3.4 LOCATION MANAGER: The Context Provider (CP) collects the physical location parameters (GPS, Cell IDs, Wi-Fi parameters) through the device sensors and stores them in its own database, linking each physical location to a user-defined logical location. It also verifies and updates those parameters whenever the device is re-located.

3.5 TIME CONTEXT: This context collects the physical time parameters from the device and stores them in a database. When a data is arrived to the device it checks the user defined time context with the stored context.

IV. MODEL OVERVIEW

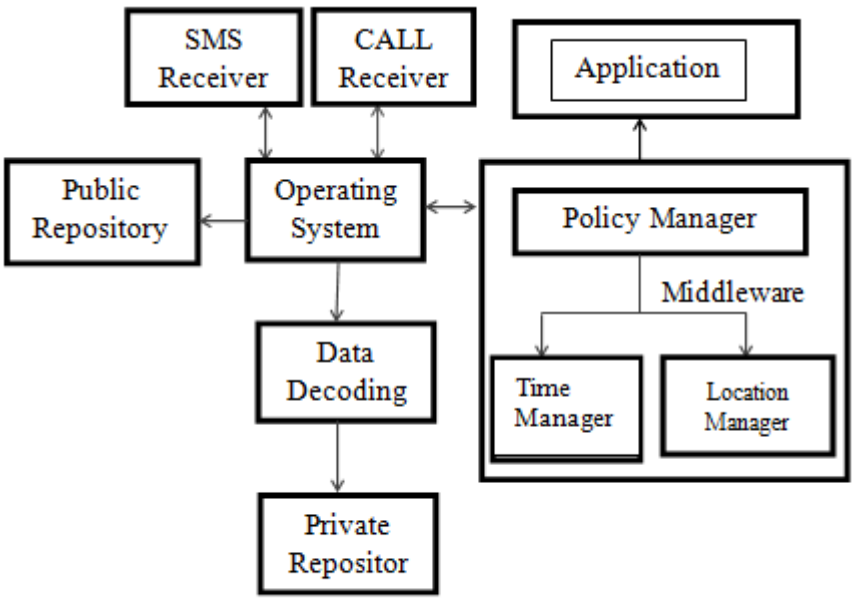

Fig 2: access control framework through middleware

In this section, we present a working of the access control mechanism through middleware with the help of considering the fig 2 (access control framework)

The context such as location and time will be managed by time context and location manager in middleware. This context must be user predefined. Once the SMS or call data is been received by operating system. It is sent to SMS receiver and Call Receiver respectively.

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

Now let's consider two cases. In first case the SMS data must be sent to data decoding where the messages are decoded into text and number fields. Once the messages are decoded they are sent to middleware where the policy will be checked i.e, if the user predefined contexts (Time and Location) is matching with the arrival time and arrival Location of the SMS then the SMS will be encrypted and stored in the private repository where no other malicious applications can fetch the user's personal data. In the second case let's consider call data.in which the call data is sent to middleware where the policies are checked same as that of sms data. If the user predefined and arrival time, location of call is matching then the data is stored in public repository. Once the call is disconnected we find path where the call is stored and delete the file.
This will be the overview of the model with brief explanation.

V. RELATED WORK

This section provides information about the background work which is related to the security of data using context based access control. There are number of approaches which is already been proposed for context based access control. Some of them are discussed in this section.
A Trust and Context Based Access Control Model for Distributed Systems By FujunFeng,Chuang len,Dongshengpeng[1], they focus on overcoming the traditional access control models such as identity based access control.They propose Trust and Context based access control model also called as TCAC.This topic extends the topic called Role Based Access Control. Role assignment in TCAC Based is on the trustworthiness and information about context which is given by users. They also provide a trust evaluation mechanism based on the local and global reputation to compute the trust value of a user in distributed system, which can avoid malicious nodes behave correctly in order to get the highest possible trust value. Finally an implementation framework of the access control system based on TCAC is described. TaintDroid: An Information-**Flow Tracking** System for **Real-time** Privacy Monitoring on Smartphones[2], TaintDroid describes extension to the android mobile-phone platform that tracks the flow of privacy sensitive data through third party application.Taintdroid assumes that downloaded third party application are not trusted,and monitors in real time how these application access and manipulate user's personal data. E.panorama**:** Capturing System-wide information flow for malware detection and analysis.[3],Smartphones are resource constrained.The resource limitation of smartphones precludes the use of heavy weight information tracking system such as panorama. Apache harmo**ny-open source** java platform[4],Android uses the apache harmony implementation of java with the few custom modifications. This implementation includes support for the platform address class, which contains a native address and is used by Direct Buffer objects. The file and network I/O APIs include write and read "direct" variants that consumes the native address from a Direct Buffer.Context Based Access Control System for mobile devices by .Bilal Shebaro, OyindamolaOluwatimi, and Elisa Bertino[5], Modified version of the android operating system supporting context based access control policies.These policies restrict applications from accessing specific data and/or resources based on the user context. The restriction specified in the policy is automatically applied as soon as the user device matches the predefined context associated with the policy.

VI. CONCLUSIONS

In this work, we proposed a middleware version of android operating system supporting context based access control system. The paper explains how we can secure our data and conserve privacy by using context in the middleware. The context which is used will restrict the other malicious applications from accessing user's data. The context which is specified in a policy manager are automatically Applied as soon as the device matches with the user defined context. Our approach requires users to give their own set of policies which is considered as predefined polices.

REFERENCES

[1] FujunFeng,Chuanglen,Dongshengpeng, "A Trustand Context Based Access Control Model for Distributed Systems"
[2] "TaintDroid:An Information-FlowTracking System for Realtime Privacy Monitoring on Smartphones"
[3] "E.panorama:Capturing System-wide information flow for malware detection and analysis".
[4] "Apache harmony-open source java platform "

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

[5] BilalShebaro, OyindamolaOluwatimi, and Elisa Bertino,"Context Based Access Control Sytem for mobile devices"IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 12, NO. 2, MARCH/APRIL 2015
[6] Wikipedia, (May 2013). Samsung galaxy specifications.[Online].Available:http://en.wikipedia.org/wiki/Samsung_ Galaxy_S4
[7] W. Enck, P. Gilbert, B.-G. Chun, L. P. Cox, J. Jung, P. McDaniel, and A. N. Sheth, "Taintdroid: An information-flow tracking system for realtime privacy monitoring on smartphones," in Proc. 9th USENIX Conf. Oper. Syst. Des. Implementation, 2010, pp. 1–6.
[8] 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.
[9] keXu, YingjiuLi,and Robert H.Deng,"ICCDetecter:ICCBsased Malware Detection On Android",In IEEE Transaction on Information Forensic Security volume:11,Issue:6,June 2016pp,1252-1264.