Managing Context Based Access Control Systems for Mobile Devices

Mr. Vijai Bharrath DLK
Assisstant Professor Information Technology
Velammal Institute Of Technology,Panchetti-601204
vijaybharathk@gmail.com

Ms. Nisha Rajan[1], Ms. Nalini Preetha R[2]
Final Year Student, Information Technology
Velammal Institute Of Technology,Panchetti-601204
rajannisha@outlook.com[1] ,
preethaaravichandran@gmail.com[2]

Abstract - An android is a name given to a mobile operating system made by Google. An operating system is software that acts as an interface and manages computer hardware and software resources. In any other operating system, there is a problem of malevolent software or malicious contents trying to wreck havoc. A malicious software is any software that is used for or can disrupt computer operation and gather access to private systems [1].Android applications will frequently have access to private and confidential resources and information in the user's device. There is high degree of possible exploitation of these resources. We can take an example of an application using a video camera to document the on-going activities of an organization. Android users do have a certain amount of control over the application capacities and capabilities after installing it based on user's context [2]. In our paper, we propose another way where network managers can control what applications are granted access or revoked.

*****

I. INTRODUCTION

Android became very popular because of its various advantages and capacities. The first point is multitasking, meaning it can run many applications or services at the same time making the time factor feasible. Secondly, the process of notifying the user is made really easy because of high-end user interface. Third, there is easy access to millions and billions of applications in the Google Play Store and most of them are free [3]. This made a vast majority of the population to buy android based mobile phones. Though there are so many advantages, the problem of security is a crucial point to take note of. There are many ways to get information or data of the user from a service on their mobile phone. Most of these services can collect confidential data without the user's knowledge and can cause risks for the user. It is possible for an application to spy and release private data without the approval or even consent of the user.[4] Due to this reason, users carrying their devices in common places risk security problems by releasing personal information without their acceptance because they are unaware of such badware in their devices. The common solution to this is to not take the smartphone when going to certain confidential places, but this is easier said than done. In the case of certain government organizations, they restrict their employees from bringing any device having camera, video and recording facilities- which is most of the phones these days- even though their devices may contain private information which the user may be in need of. So the next step which can be possible is to have a good control over the capacities and capabilities of their devices. This can be done by reducing certain service privileges while being in private and confidential places based on context with more stress on location and time [2]. In the existing system, with context-based policies it can benefit most of the population by making certain applications disabled based on the location restrictions and enable it back when the user is out of such private locations. This is the case for government officials and law enforcement agents who are not supposed to bring the mobile devices during confidential meetings.[5]This requires the user to set their own policies to restrict applications based on the location. However, the difficulty of setting up these configurations requires the same knowledge needed to inspect service and resource permissions listed at the time of installation of the application [2]. In this paper, we give the network manager the role to block badware from using or even accessing the data that if exposed will affect the security of the network. This is important to achieve security in the network of corporate organizations and government bodies.

II. ABOUT ANDROID

The android architecture can be explained in terms of a software stack which has 4 main components i.e., an operating system, a run-time environment, middleware and libraries. This is diagrammatically represented below (fig: 1.1). All the layers are integrated together so to provide the application development in a most feasible way with a good execution environment. The diagram shows the basic architecture of android.

A. Linux Kernel:

This layer proves as an interface between the hardware and the remaining upper layers of the software stack.
Multi tasking, memory and power management are most of the responsibilities. It was originally used for desktops and servers.

B. The virtual machine (Dalvik):

The advantage here is that the applications cannot interfere with the operating system or other executing applications.

 ISSN: 2321-8169
1174 - 1177

Since there is a high degree of abstraction the applications are not dependent on one specific form of hardware. This was developed by Google and relies on the Linux Kernel.

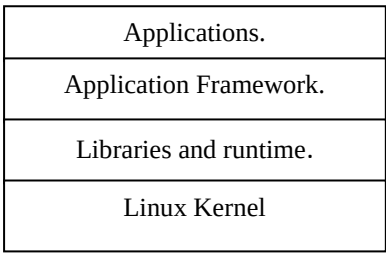

Figure 2.1: Basic android architecture.

for low-level functionality [6]. For execution within this virtual machine, the code must be converted to .dex format which is dalvik executable format; this has lesser memory than a normal Java bytecode.

C .Android Libraries:
The android core libraries are essentially are Java wrappers around a set of c/c++ based libraries. For example, when we want to draw 3D graphics on the display, the library calls OpenGL c++ library.[6] This works with the kernel to draw the required object.

D. Application Framework:
The framework is a set of operations and services that together, form the environment where the applications are run and managed. The concept of reusability is provided here. Meaning, an application can publish its capabilities combined with the data and information so that they can be found and reused.

E. Applications:
This is the top most layer in the diagram. It includes both the applications that are provided with one specific implementation along with third party applications installed after the user buys the device.

F. Inter-process Communication:
Let us consider the service sending data is the caller and the one who receives the data callee. The caller sends the data after serialization into bytes, through the kernel to the callee. The callee performs deserialization process, reads the data and recognizes what it's supposed to do. The result is forwarded to the caller. Android makes the callee decide who has the right to call it. These messages and data are collectively called intents[7].Applications can specify filters for intents which show what intents an application wants to receive.

III. SYSTEM ARCHITECTURE

In this section we will introduce the architecture of the system capable of incorporation. Given below are the list of modules that are present along with the diagrammatic representation of the proposed system:

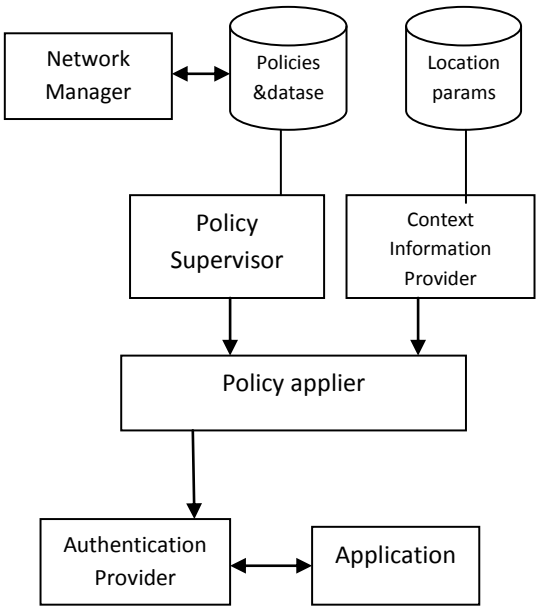

Figure 3.1 The system architecture.

A. Context Information Provider:
The first step is where the context information is discovered, the location parameters are discovered with the help of Global Positioning Satellite and Wireless Fidelity parameters. The second step involves the acquisition [8] where the collected information about physical parameters are stored in a database or repository. Linkage between physical and logical locations is done. If relocation occurs, updation is possible.

B. Authentication Provider:
This module performs authentication and authorization purposes so that there is no misuse or exploitation of the services and data of the device. Android has a good checking mechanism for the grant or revoke signal but the authentication mechanism performs a second layer of security.

C. Policy Supervisor:
The creation of policies is done here i.e which restriction should be present for one specific location. For example, the College conference hall has a restriction of the camer a, so for this location, the resources to use the camera will be revoked permission.

D. Policy Applier:

The Policy Applier performs the process of comparison between the location and the restriction. When a service or resource is requested the policy applier checks for any restriction and based on the restriction will accept or deny the access. The result is sent to the authentication provider. The Policy Applier checks if there is a match between the corresponding location and restriction. The authentication provider then applies the restrictions, if there is no match it is considered as a new location and there will be default restrictions for the new location defined in Policy Supervisor.

E. Network Manager:

The registration of all the mobile numbers on a server is the main duty of a Network Manager. The policy setting mechanism is done by the manager for restricting the application on a mobile device when the user enters a sensitive area. As the service starts, the policy is set for the mobile and the control is passed to the 4 modules.

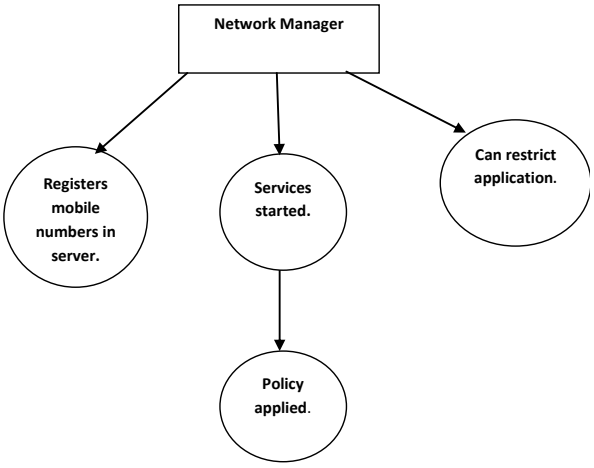

Fig:3.1 The network manager.

IV. FINDING THE SPOT/PLACE.

To get the required location there are two phases to be passed through.

A .Spot/Place capturing phase:

Firstly the scanning mechanism scans and takes a snap of the location data within many smaller areas. This is to perform better accuracy in applying restrictions. The first is the triangulation step [9] where we find out a particular point in location based on the surrounding multi points of location which are already discovered. Once the distance is same, we can calculate the unknown point. The second is proximity which is similar to the previous step except we take a single discovered point. In this way the latitude parameters and longitude parameters are found out. Since using satellite is widely used the accuracy is not as close to wireless fidelity parameters which can provide distinction between two sub areas. Both of the data together will provide the desired location where we can check if any restriction is present. If it is a new location a default policy should be applied which is suitable. The person can enter the co ordinates on her own or through other devices which contain the co ordinates in a saved state.

B. Spot/Place detection phase:

For every Nth second/minute
{
Get current location parameters(GPS latitude, GPS longitude, GPS altitude, Wi-Fi access point, Wi-Fi RSSi)
If current context= Saved context Then
Apply policy restriction of detected location
Else Then
Apply unregistered location –based policy restriction
End If
}

For a definite set of seconds or minutes, the location snap is taken to find out the device's location at that point of time. The required location parameters are taken with the help of global positioning satellite and wireless fidelity. The collection of areas that have a subset of the neighboring points are taken from the repository in the first step. Based on accurate measures by the wireless fidelity parameters we can narrow down the list to only a few making the comparison process easy. The comparison is carried out to check if it is the same location as with the one saved in the database or repository, if there is a match it means the location is known and
that particular restrictions are applied. If it is an unregistered location it means it is a new area and the default policy restriction is applied. The same procedure is performed for some more points along the way and we check the number of evaluating steps or tests passed. Through this procedure we can determine the where abouts of the device.

V. CONCLUSION:

The process of using network manager increases the security and protects the sensitive details. Exploitation of system resources are effectively reduced. The hacking of sensitive information can also be minimized by this procedure once the device enters a secure network guarded by these restrictions. This will allow users to carry devices at ease without the fear of exploitation.

REFERENCES:

[1] "Malware definition". techterms.com. Retrieved 26 August 2013.
[2] Context-based Access Control Systems for Mobile Devices,IEEE Transactions on (Volume: PP , Issue: 99) 29 April 2014.
[3] http://mobilecon.info/advantages-and-disadvantages-android-mobile-

phone.html#sthash.S2gwvaVV.dpbs advantages of android.

[4] J. Leyden, "Your phone may not be spying on you now - but it soon will be," http://www.theregister.co.uk/2013/04/24/kaspersky_mobile_malware_infosec/, April 2013.

[5] http://eci.nic.in/eci_main/faq/faq_mcc.pdf "MODEL CODE OF CONDUCT FOR THE GUIDANCE OF POLITICAL PARTIES AND CANDIDATES".

[6] http://www.techotopia.com/index.php/An_Overview_of_the_Android_Architecture "An Overview Of the Android Architecture".

[7] http://www3.cs.stonybrook.edu/~rob/teaching/cse409-fa11/notes/09-19-alin-tomescu.pdf "Android Security Model".

[8] "Context-aware security and secure context-awareness in ubiquitous computing environments" Konrad Wrona, Laurent Gomez. SAP Research, 805, Avenue du Docteur Maurice Donat, 06250 Mougins, France.

[9] http://www.ijarcsse.com/docs/papers/Volume_3/6_June2013/V3I5-0480.pdf "A Survey of Positioning Algorithms on Mobile Devices in Location Based Services".