Design of Image Based Authentication System for Android Smartphone Users

Indira C K #1, Kavitha D #2

#1 M.Tech, Computer Science Engineering, G.Pulla Reddy Engineering College (Autonomous) Kurnool, Andhra Pradesh, India

#2 Professor, Department of CSE, G.Pullareddy Engineering College, Kurnool, Andhra Pradesh, India

Abstract—The devices most often used for IT services are changing from PCs and laptops to smartphones and tablets. There are some advanced features in android Smartphone, with which user can easily share applications via online market store i.e. Google market store. The rapid growth of the smartphone market and the use of these devices for email, online banking, and accessing other forms of sensitive content has lead to the emergence of a new and ever-changing threat landscape. Security systems are rapidly being developed, as well as solutions such as remote control systems. However, even with these solutions, major problems could still result after a mobile device is lost. This paper describes the security measures to improve Android Operating System so that users can safely use the android smart phones.

Keywords- Android, smartphone, Lock Screen, authentication

I. INTRODUCTION

Developed by the Open Handset Alliance (visibly led by Google), Android is a widely anticipated open source operating system for mobile devices that provides a base operating system, an application middleware layer, a Java software development kit (SDK), and a collection of system applications. Android mobile application development is based on Java language codes, as it allows developers to write codes in the Java language. Mobile Development India has worked extensively on projects ranging from gaming software, organizers, media players, picture editors to go-cart devices and more.[1]

II ANDROID SYSTEM ARCHITECTURE

In android operating system, there are four layers. Android has its own libraries; it is helpful for developing and designing any application of android platform. These libraries are written in C/C++. Linux kernel is the 1st layer which is written in C. Linux also helps to wrap the application.

- Application layer: It is the most upper layer in android architecture. All the applications like camera, Google maps, browser, sms, calendars, contacts are native applications. These applications works with end user with the help of application framework to operate.
- Application framework: Android applications which are developing, this layer contain needed classes and services. Developers can reuse and extend the components already present in API. In this layer, there are managers which enable the application for accessing data. These are as follows:
  - Activity manager: It manages the lifecycle of applications. It enables proper management of all the activities. All the activities are controlled by activity manager.
  - Resource manager: It provides access to non-code resources such as graphics etc.
  - Notification manager: It enables all applications to display custom alerts in status bar.
  - Location manager: It fires alerts when user enters or leaves a specified geographical location.
- Package manager: It is use to retrieve the data about installed packages on device.
- Window manager: It is use to create views and layouts.
- Telephony manager: It is use to handle settings of network connection and all information about services on device.
- Android runtime: In this section, all the android applications are executed. Android has its own virtual machine i.e. DVM (Dalvik Virtual Machine), which is used to execute the android application. With this DVK, users are able to execute multiple applications at same time.
- Libraries: Android has its own libraries, which is written in C/C++. These libraries cannot be accessed directly. With the help of application framework, we can access these libraries. There are many libraries like web libraries to access web browsers, libraries for android and video formats etc.
- Linux kernel: This layer is core of android architecture. It provides service like power management, memory management, security etc. It helps in software or hardware binding for better communication.

III ANDROID SECURITY FRAMEWORK

The Google Android mobile phone platform is one of the most anticipated smartphone operating systems. Smart phones can be used in place of Computers/Laptops. As mobile devices attain increasing capabilities, there are many more opportunities for novel applications development. Recent development of mobile application development has reached a high demand on today’s cellular market. Android defines a new component-based framework for developing mobile applications, where each application is comprised of different numbers and types of components. Activity components are the basis of the user interface; each screen presented to the user is a different Activity [1]. Service components provide background processing that continues even after its application loses focus. Content Provider components share information in relational database form. SQLite is embedded into android which supports relational database. For instance, the system includes an application with a Content Provider devoted to sharing the user’s address book upon which other applications can query. Finally, Broadcast Receiver components act as an asynchronous mailbox for messages from the system and other applications. As a whole, this application framework supports a flexible degree of collaboration between applications, where dependencies can be as simple or complex as a situation requires.

IV IMPROVED AUTHENTICATION SYSTEM FOR ANDROID SMARTPHONES

A. Basic principle of motion

To provide flexibility to the users, the interfaces have been developed that are accessible through a browser. The GUI's at the top level have been categorized as

1. Administrative user interface
2. The operational or generic user interface

The ‘administrative user interface’ concentrates on the consistent information that is practically, part of the organizational activities and which needs proper authentication for the data collection. These interfaces help the administrators with all the transactional states like Data insertion, Data deletion and Date updation along with the extensive data search capabilities.

The ‘operational or generic user interface’ helps the end users of the system in transactions through the existing data and required services. The operational user interface also helps the ordinary users in managing their own information in a customized manner as per the included flexibilities

B. System Architecture

The system adapts three-layer architecture. Below architecture diagram represents mainly flow of requests from users to database through servers. In this scenario overall system is designed in three tires separately using three layers called presentation layer, business logic layer and data link layer.

![System Architecture Diagram]
The upgraded authenticated system consists of 3 modules

- **Set Image Password Module:** In this module we are able to set the password for our application. This is necessary to provide extra security for our application. It also provide authentication to the user.

- **Change Login Id Module:** If we want to change our existing password, then we must enter into this module and change the login details.

- **Access Activity Module:** In this module first we need to verify the password before going to access the application. Authentication through the images only. If the password is correct then it allows us to access the screen and go to next page otherwise it displays invalid password.

**C. Working of improved authentication system for Android smartphones**

**Step 1.** The Lock Screen consists of activities, so it is included in the Home Launcher application package. The Screen receives the “On/Off Broadcast Receiver” so it is processed with Intent from Screen-On, activating the Lock Screen Activity.

**Step 2.** The Lock Screen Activity consists of Password settings and, to unlock the screen, a password of user’s choice must first be entered. After setting the password, the user is asked to enter the password to go to the application. Each image is displayed as a button and every button contains some number. If it matches it allows to access the application.

**Step 3.** In the Home Launcher application, there are five slides and declared icons with widgets. The user can make widgets, icons, folders, and setting slides through various kinds of touches (touch, long-click, drag, home button, and menu button).

**VI CONCLUSION**

With the vigorous development through Android, mobile applications have been widely used on the various mobile devices. The maturity of the hardware and software platforms of mobile devices and the promotion of the Mobile Internet have brought a great opportunity to the migration of the web applications to mobile platforms. When we need to store large amount of important personal information on the mobile devices good security is required[6]. The use of the improved authentication system ensures protection of personal information.

**VII. FUTURE WORK**

Android is being installed in tablets and many other IT devices that require good security systems. The future Enhancements are:

1. Strong protection with password and encryption of records and images will be provided.
2. The dedicated Integrated Development Environment (IDE) will be improved to accelerate the applications development.

**REFERENCES**


