

Mechanism and Security Concerns of the Android Operating System

Akansha Gulati¹, Kirti Patel², Supriya Deshmukh³

Students^{1,2}, Assistant Professor³

Department of Computer Science and Engineering,

MRIIRS, Faridabad, Haryana, India

Corresponding Author's Email: akanshagulati86@gmail.com¹

Abstract

Google's Android is a mobile and tablet operating system based on the Linux kernel. The ultimate revolutionary aspect of the Android Operating System is open source, which allows anybody to freely publish their apps on the Android market. This openness introduces a large number of developers that use this platform, but it also presents the risk that a user may download harmful software produced by network hackers and endanger their privacy. This necessitates research into Android's security mechanisms as well as making it simple and user-friendly to alert the user to places where he should be careful. This article discusses the architecture of the Android operating system, security aspects of an android, security challenges encountered by the Android, and remedies for Android security issues.

Keywords: *Android, architecture, security, security solutions*

INTRODUCTION

The Android platform is based on the Linux kernel. Because of its security characteristics, the Linux kernel has grown in popularity over the years. Furthermore, the Linux kernel adds a layer of abstraction between the device and the hardware [4]. This level of abstraction

includes all of the required hardware drivers, such as display, camera, and keypad. The Android operating system architecture is seen in Figure 1.

The parts that follow go over the various components of the Android operating system.

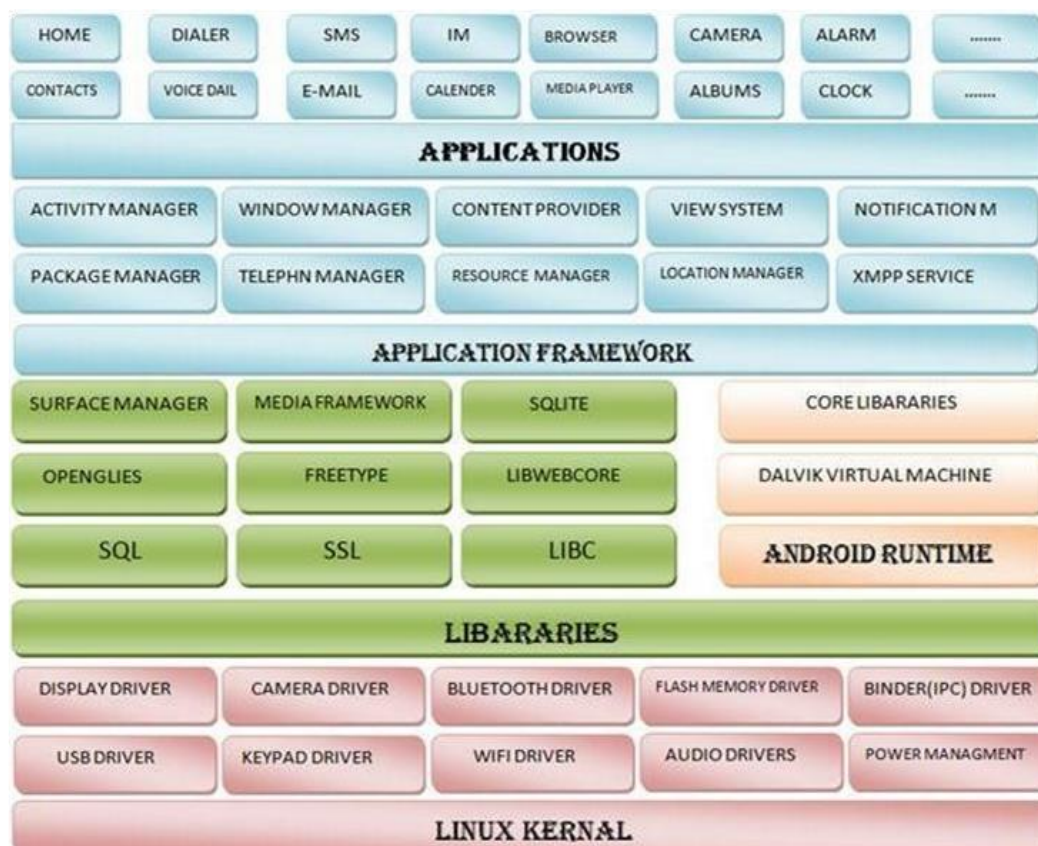


Figure 1: Architecture of the Android Operating System.

Linux Kernel

The Linux kernel is at the heart of the Android architecture. This layer serves as a bridge between the hardware and the user. It handles all activity, memory, and resource sharing. This layer is generally utilised by hardware makers since it ensures that hardware abstraction layers remain unchanged even if the underlying hardware changes.

Memory space on mobile devices is limited. As a result, having a Linux kernel service for memory management is critical.

Libraries

A collection of libraries sits on top of the Linux kernel. Surface Manager, SQLite, WebKit, the well-known library libc, Media Framework, Free Type, SSL, and other libraries are included. These libraries are developed in C or C++ and are accessed through a Java interface [1].

These libraries provide the following functionalities:-

- The Surface manager, which manages device display.
- SQLite database serves as repository storage for Android.

- WebKit is a free and open-source web browser engine.
- Libc includes C libraries.
- The media framework supports the playing and recording of popular audio and video formats. Static image files are also supported [1].
- SSL libraries for Internet security

Android Runtime

The second layer from the bottom is the Android runtime. The Android runtime comprises a collection of fundamental libraries as well as the Dalvik Virtual Machine [4]. The Dalvik Virtual Machine is a kind of Java Virtual Machine designed specifically for Android [4].

The Dalvik Virtual Machine was created specifically for mobile devices [1]. The Dalvik Virtual Machine is similar to the Java Virtual Machine. But for mobile phones, the Java virtual machine allows the computer to execute Java instructions as well as other applications written in various languages and compiled to Java byte code [13]. Another distinction is that the Dalvik virtual machine is register-based, whereas the Java virtual machine is process-based.

The Dalvik Virtual Machine makes use of Linux fundamental features such as memory management, portability, and multi-threading, which are important features of the Java programming language. The Dalvik virtual machine operates in contexts with limited memory and computing capacity. The Android runtime also lets Android developers build apps for Android by giving them access to a set of important Java libraries.

Application Framework

The Application Framework enables numerous higher-level services and mechanisms that android developers may leverage to create unique apps. The Application Framework is a set of fundamental tools that a developer may use to create more complicated tools.

The Android framework includes the following key services –

- **Activity Manager** – It regulates the activity lifecycle. It gives the user a way to engage with the programme.
- **Content Providers** – The Content Provider acts as a go-between for your Android system and [18]. Enables applications to communicate with one another and exchange data.

- **Resource Manager** – It controls numerous resources, such as layout files, strings, and images, that may be used in the development of new apps.
- **Notifications Manager** – It allows programmes to display warnings and notifications to the user on the screen.
- **View System** – It provides rich and extendable views for designing user interfaces for programmes, like buttons, grids, textboxes, and so on.

Applications

In this layer, the user may develop and install programmes. Contacts, camera, calendar, media player, Web Browser, and Alarms are examples of such programmes.

Different Security Features of Android OS

The Android operating system is popular because of the security features. The following are the security features provided by the Android to its users:

1. Security at operating system level
2. Application sandbox for all applications
3. Security in interprocess communication
4. Application signing

5. Application defined and user-granted permissions

Linux Kernel

Because Linux is open source software, it is continually being examined, attacked, and updated by a large number of research researchers. After several changes, Linux has become a safe and reliable kernel.

The Linux kernel provides Android with a number of important security measures, including: A user-based permissions model for each file and directory. In Linux there are 3 user-based permissions: Owner, Group, Other users.

1. **Owner** - The Owner permissions for the owner of the files or directories.
2. **Group** –The group permissions for the group that has been given the files or directories.
3. **Other users** - The other Users permissions apply to all other users on the system. Every file or directory has three basic permission types:
4. **Read**- The read permission refers as the user can read the contents of the file

5. **Write** - write permissions refer as the user can to write or edit the files or directories.
6. **Execute** - The execute permission refers as the user is allowed to execute the files or view the contents of directories.

This permission model makes sure that these security features are maintained while accessing Android files.

- a. Process isolation: It is a distinct process that executes the apps by assigning a unique user identifier (UID) to each Android app.
- b. A safe mechanism for inter-process communication.
- c. A one-of-a-kind capability for removing non-essential and insecure kernel components.

The Application Sandbox

An application sandbox is a security tool that executes untested scripts or programmes from untrustworthy individuals and websites. Sandboxing allows for restricted access to a device's resources [1].

The system's security is improved as a result [1]. This method provides a platform for malware code execution while simultaneously preventing the software from causing harm to the host device [1]. This is accomplished by restricting access to only those resources for which permission has been given [1].

Secure Inter-process Communication

Inter-process communication is the technique through which Android components communicate with one another. Instead of using outdated Linux mechanisms for inter-process communication such as file systems, network sockets, and shared files, the Android operating system includes the newest approaches for IPC such as Services, Intents, Content Providers, and Binder [3].

Application signing

Applications that operate on the Android operating system must be digitally signed in order for the developer to be identified. The application signature function also fosters confidence between apps.

Application-defined and User-granted Permissions

Permissions are one method of securing Android-based applications. Android

applications are safe since no permissions are provided by default. Location data (GPS), SMS/MMS functions, Bluetooth functions, camera functions, telephony functions, and network or data connections are among the protected APIs [1].

Security Issues Faced By Android

1. **Malicious Applications:** Malicious applications are causing major issues. Some of these applications might expose the location, contacts, private information, and other personal information of the smart phone user. These malicious applications will download other malicious applications from the Internet. This disclosure of private information may jeopardise an individual's security.
2. **Unsafe websites:** Malicious applications may be present on some websites. Any user of an Android smart phone who surfs the Internet using the browser may be attacked if he or she hits a malicious webpage, and the attacker may run any malware using any browser.
3. **Data security of mobile devices:** Smart phones vary from desktop computers in that they are portable, putting them at a larger risk of loss.

When a user loses his or her smart phone, the data on the device is difficult to restore.

4. **External storage:** The protection of files produced on external storage, such as Secure Digital Cards, is a critical security concern for mobile phones (SD cards). SD card files are universally readable and writeable, and they may be deleted and edited by any user.

Network data security for mobile devices

The usage of unsecured wifi networks allows attackers or hackers to obtain the user's personal information, which may then be used to gain access to their bank account data and other secure information.

Solutions for Security Issues of Android OS

Not Using External Storage

Files generated on portable storage devices like Secure Digital cards (SD Cards) are universally readable and writable. Because portable storage can be removed by the user or others, as well as modified by any other application, the user should avoid storing sensitive information on it.

Disable Unknown Sources Option in Android

When a user attempts to install an app from a website other than Google Play, the notice "UNKNOWN SOURCES" should appear, with the choice to enable or disable the installation.

To protect security, only download software from trusted sources, such as the Google Play store on the Android platform. It is already deactivated by default for security reasons.

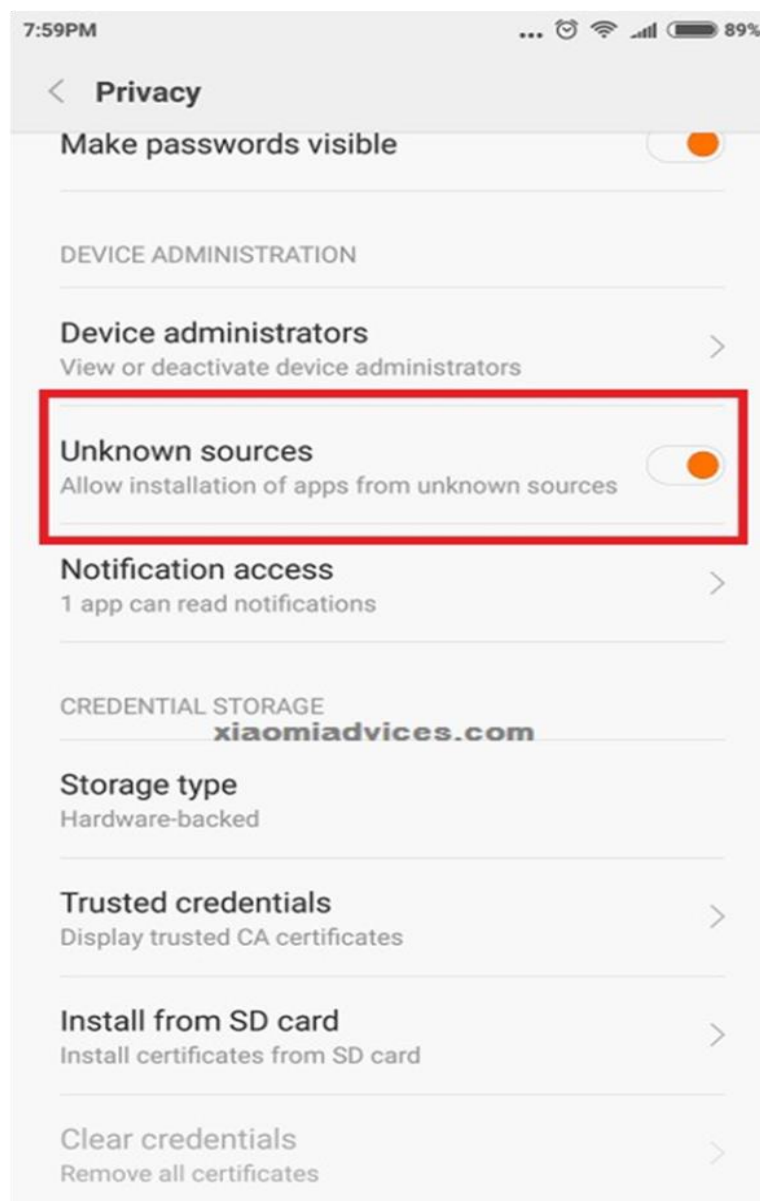


Figure 2: Disable Unknown Sources Option in Android

Grant Permissions Wisely

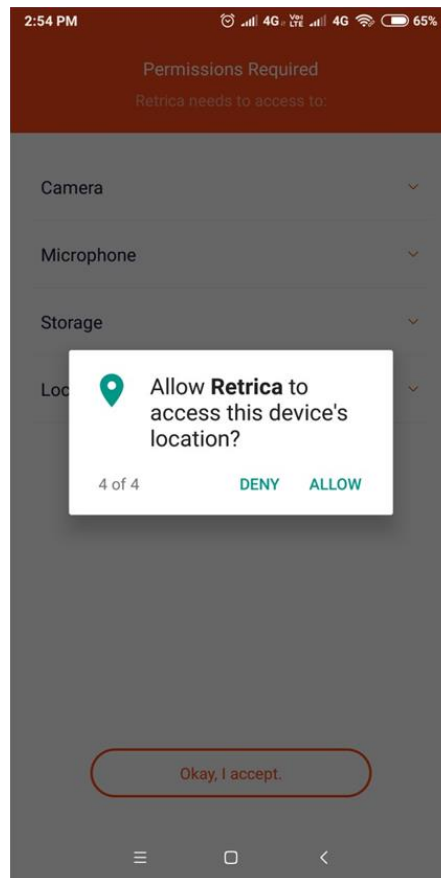


Figure 3: Grant Permissions.

When a user installs an app from Google's Play Store, a pop-up window appears with a list of all the permissions the user requires. This might involve accessing the user's text messages, phone call records, media assets, and so on. Some programmers', for example, some camera applications, demand the user's phone contacts, which is not acceptable. Giving this permission may result in information leakage. So, before installing a programme, carefully study all of the permissions.

Data Encryption

Encrypting or password-protecting your personal data ensures that it cannot be viewed by another user.

Keep your apps up-to-date

Users should upgrade their programmes as soon as a newer version becomes available. Several issues have been resolved in the latest versions of the programmes. When vulnerability in a programme is discovered and fixed by the developers, a fresh version is issued. This also enhances the device's efficiency.

Use an Antivirus App

A user should install an antivirus application to identify and eliminate harmful files. Avast, Norton, Fast Heal, and more antivirus applications for Android are available.

Disable GPS Option in Android

When it is not necessary, users should disable the GPS option in Android. This is

because other applications may access the smart phone's location unnecessarily, consuming more battery power and mobile data. As a result, cybercriminals can track the user's location and use the location information for criminal purposes. As a result, users only utilise GPS when absolutely essential.

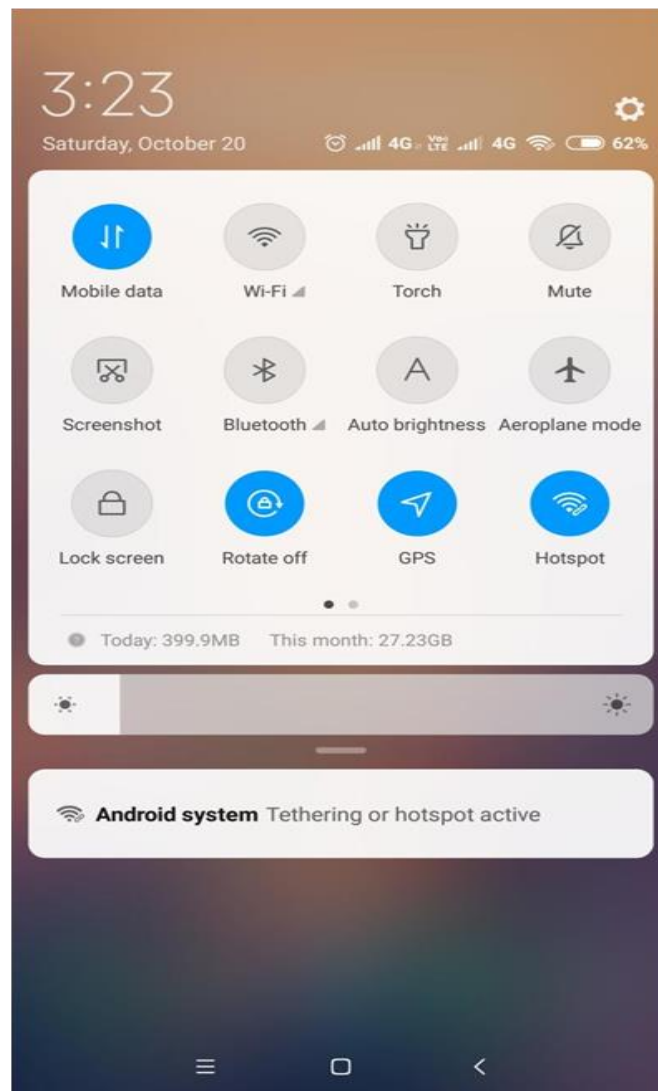


Figure 4: Disable GPS Option in Android

Enable SIM Card Lock

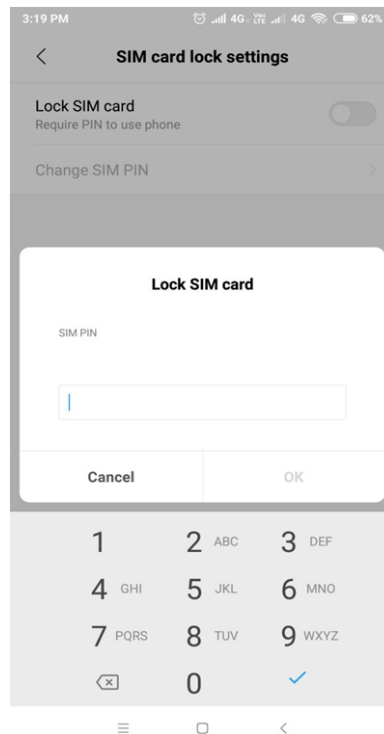


Figure 5: Enable SIM Card Lock

Disabling the SIM card lock option on Android allows a burglar to acquire information about the user's identity because phone numbers are used to create social media accounts, websites, and apps, among other things. Using text message authentication and OTP, cybercriminals can alter the password and get access to accounts and bank accounts (one-time password). For example, a Facebook account may be accessed by selecting the "forgot password" option on the login page, which sends the security code to the phone number provided. So, users should turn on the SIM card lock to protect their identities and accounts.

CONCLUSION

The Android operating system is one of the most popular and will most likely be around for many years to come. As Android-based mobile devices get more powerful, they have more uses and hence more data saved on them. As a result, it is critical that users and developers understand the security dangers and what they can do to safeguard their personal information. Users must be aware of any applications that they install on their device and use caution before granting permission to applications. Developers must make the necessary changes to avoid security breaches or vulnerabilities.

Developers are now striving to improve Android security in the latest version of Android "P." Google aims to improve Android P's "privacy and security."

REFERENCES

1. <https://pdfs.semanticscholar.org/11f4/b8efd1a9af746f17ac5e8d6a789bd3c3a9b7.pdf>
2. <https://www.scribd.com/document/208852386/Cc-4201519521>
3. <https://vdocuments.mx/documents/android-vulnerability-to-impersonate-trusted-applications.html>
4. <https://www.quora.com/What-is-the-Android-application-Architecture>
5. <https://stackoverflow.com/questions/10283725/what-is-difference-between-software-stack-and-os-why-android-is-not-an-os-but>
6. https://www.researchgate.net/profile/Carlos_Carrascosa/publication/221611128_Does_Android_Dream_with_Intelligent_Agents/links/00b495176646066162000000.pdf?disableCoverPage=true
7. <https://www.scribd.com/document/262130241/Android-vulnerability-to-impersonate-trusted-applications>
8. http://www.academia.edu/6499341/CC_4201519521
9. <https://www.safaribooksonline.com/library/view/android-malware-and/9781482252200/chapter-09.html>
10. https://www.reddit.com/r/MotoG/comments/7twx99/any_news_of_the_oreo_update_on_moto_g5_plus/
11. https://www.researchgate.net/profile/Ben_Benjamin/publication/264751361_Penetration_Testing_for_Android_Smartphones/links/53edf0260cf26b9b7dc63766/Penetration-Testing-for-Android-Smartphones.pdf
12. https://en.wikipedia.org/wiki/Java_virtual_machine#C_to_bytecode_compilers
13. <https://tailforwindows.org/download-file/java-programming-with-oracle-sqlj>
14. <https://www.studypool.com/discuss/6251152/os-mechanisms-that-handle-deadlocks-etc>
15. <http://www.ijfeat.org/papers/march20162.pdf?i=1>
16. <https://quizlet.com/215337386/bcis-chapter-7-review-questions-flash-cards/>