ANDROID SECURITY

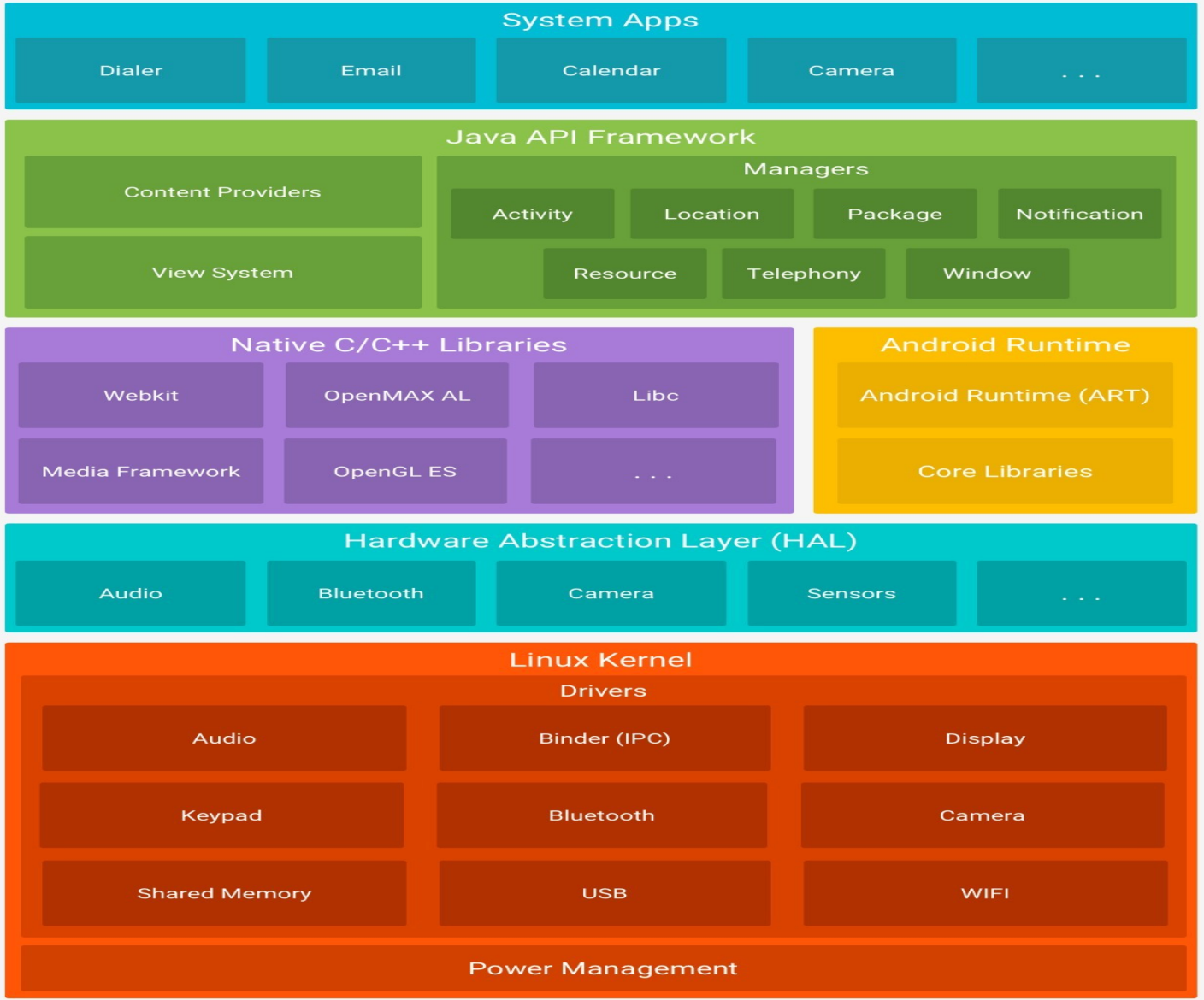
- Android OS is a Linux-based mobile operating system that primarily runs on smartphones and tablets.
- Developed by a partnership of developers known as the Open Handset Alliance and commercially sponsored by Google.
- Previous prototypes of an Android phone closely resembled a BlackBerry, with a physical keyboard and no touchscreen.
- HTC Dream was the first commercially available smartphone to run Android OS
- Google released the public beta version of Android 1.0 for developers, in November 2007.The first commercial version, Android 1.0, was released on September 23, 2008.
- Android 13, released on August 2022 is the latest version.

Designing an Android Device

- Android incorporates industry-leading security features and works with developers and device implementers to keep the Android platform and ecosystem safe.
- **Android is designed to be open**: Android was designed with multilayered security that's flexible enough to support an open platform while still protecting all users of the platform.
- **Android is designed for developers**: Android security released a tool for testing that helps developers find potential security issues on whichever platform they are developing.
- **Android is designed for users**: Users are provided visibility into the permissions requested by each app and control over those permissions.They provide patches for any Android device ie., continue giving security updates.

Android Architecture

- Android Platform
- Linux Kernel- provide basic system functionalities
- HAL- gives application direct access to hardware resources
- Native Libraries- for running application
- Dalvik VM- Execute application
- Application Framework- Provide services to application
- Application- Responsible for direct interaction with users


System Apps
Dialer
Email
Calendar
Camera
. . .
Java API Framework
Content Providers
View System
Managers
Activity
Location
Package
Notification
Resource
Telephony
Window
Native C/C++ Libraries
Webkit
OpenMAX AL
Libc
Media Framework
OpenGL ES
. . .
Android Runtime
Android Runtime (ART)
Core Libraries
Hardware Abstraction Layer (HAL)
Audio
Bluetooth
Camera
Sensors
. . .
Linux Kernel
Drivers
Audio
Binder (IPC)
Display
Keypad
Bluetooth
Camera
Shared Memory
USB
WIFI
Power Management

Google security services

- Google provides a set of services that are available to compatible Android devices with Google Mobile Services. The primary Google security services are

- **Google Play**: Google Play is a collection of services that allow users to discover, install, and purchase apps from their Android device or the web.

- **Android updates**: The Android update service delivers new capabilities and security updates.

- **Verify Apps**: Warn or automatically block the installation of harmful apps, and continually scan apps on the device, warning about or removing harmful apps

Security program overview

- **Design review**: The Android security process begins early in the development lifecycle.
- **Penetration testing and code review**: During the development of the platform, Android-created and open source components are subject to vigorous security reviews.
- **Open source and community review**: AOSP enables broad security review by any interested party.
- **Incident response**: Upon the discovery of legitimate issues, the Android team has a response process that enables the rapid mitigation of vulnerabilities to ensure that potential risk to all Android users is minimized.
- **Monthly security updates**: The Android security team provides monthly updates to Google Android devices and all our device manufacturing partners.

What is an APK File ?

- APK stands for Android Packages
- It’s the .exe equivalent of Android OS
- It’s a ZIP file
- Contains source code and other important files that helps to run an app
- **Key components of an APK file are:**
- AndroidManifest.xml
- Classes.dex
- Resources.arsc
- Res
- META-INF

AndroidMabnifest.XML

- Declares the Android API that the application is going to use
- Permission that an application needs
- List all the Activities,Services,Broadcast Receivers and Content Providers etc.

Classes.dex

- It contains Java bytecode in DEX (Dalvik Exchange) format

res

- Contains device configuration,Bitmaps and Layouts

Resources.arsc

- Contains compiles resources in a binary format
- May also include images,strings or other data used by an app

META-INF

- This folder contains the manifest information and other metadata about the java package carried by the jar file.

MANIFEST.MF : It contains various information used by the java run-time environment when leading the jar file, duch as which is the main class to be run from the jar file, version of the package, build number, creator of the package, security policies/permissions of java applets and the list of file names in the jar along with their SHA1 digests, etc.

CERT.SF : This contains the list of all files along with their SHA-1 digest.

CERT.RSA : This contains signed contents of the CERT.SF file along with the certificate chain of the public key used for signing the contents.

Static Analysis Tools Used

- APKTool
- JD-GUI
- MOBSF

Android's Security Features

App sandbox

- The Android platform takes advantage of the Linux user-based protection to identify and isolate app resources. To do this, Android assigns a unique user ID (UID) to each Android app and runs it in its own process.

App signing

- App signing allows developers to identify the author of the app and to update their app without creating complicated interfaces and permissions. Every app that runs on the Android platform must be signed by the developer.

Authentication

- Android 9 and higher includes Protected confirmation, which gives users a way to formally confirm critical transactions, such as payments.

Biometrics

- Android 9 and higher includes a BiometricPrompt API that app developers can use to integrate biometric authentication into their apps in a device

Encryption

- Encryption ensures that even if an unauthorized party tries to access the data, they won’t be able to read it.

Filesystem Encryption

- Android 5.0 and later supports full-disk encryption. Android 7.0 and later supports file-based encryption.

Password Protection

- Android can be configured to verify a user-supplied password prior to providing access to a device.
- Also, this password protects the cryptographic key for full filesystem encryption.

Android security checkup: 13 steps to a safer phone

- Step 1: Look over all the apps and services connected to your account
- Step 2: Revisit your Android app permissions
- Step 3: Verify that you're using Android's app-scanning system
- Step 4: Peek in on your saved Smart Lock passwords
- Step 5: Assess your password management system
- Step 6: Evaluate your two-factor authentication situation
- Step 7: Optimize your lock screen security
- Step 8: Clean up your list of connected devices
- Step 9: Clean up your devices in the Play Store
- Step 10: Make sure your device is prepared for the worst
- Step 11: Think about whether you should be using a VPN
- Step 12: Make sure you've done your virtual estate planning
- Step 13: Think carefully about third-party security suites