RAMA UNIVERSITY

www.ramauniversity.ac.in

FACULTY OF EGINEERING & TECHNOLOGY

MOBILE SECURITY

LECTURE -10

Umesh Kumar Gera
Assistant Professor
Computer Science & Engineering

OUTLINE

- Secure an Android Device
- Background for android framework
- The main Android platform building blocks are
- Android apps extend the core Android operating system.
- MCQ
- References

SECURE AN ANDROID DEVICE

Secure an Android Device

Android incorporates industry-leading security features and works with developers and device implementers to keep the Android platform and ecosystem safe. A robust security model is essential to enable a vigorous ecosystem of apps and devices built on and around the Android platform and supported by cloud services. As a result, through its entire development lifecycle, Android has been subject to a rigorous security program.

As a result, through its entire development lifecycle, Android has been subject to a rigorous security program.

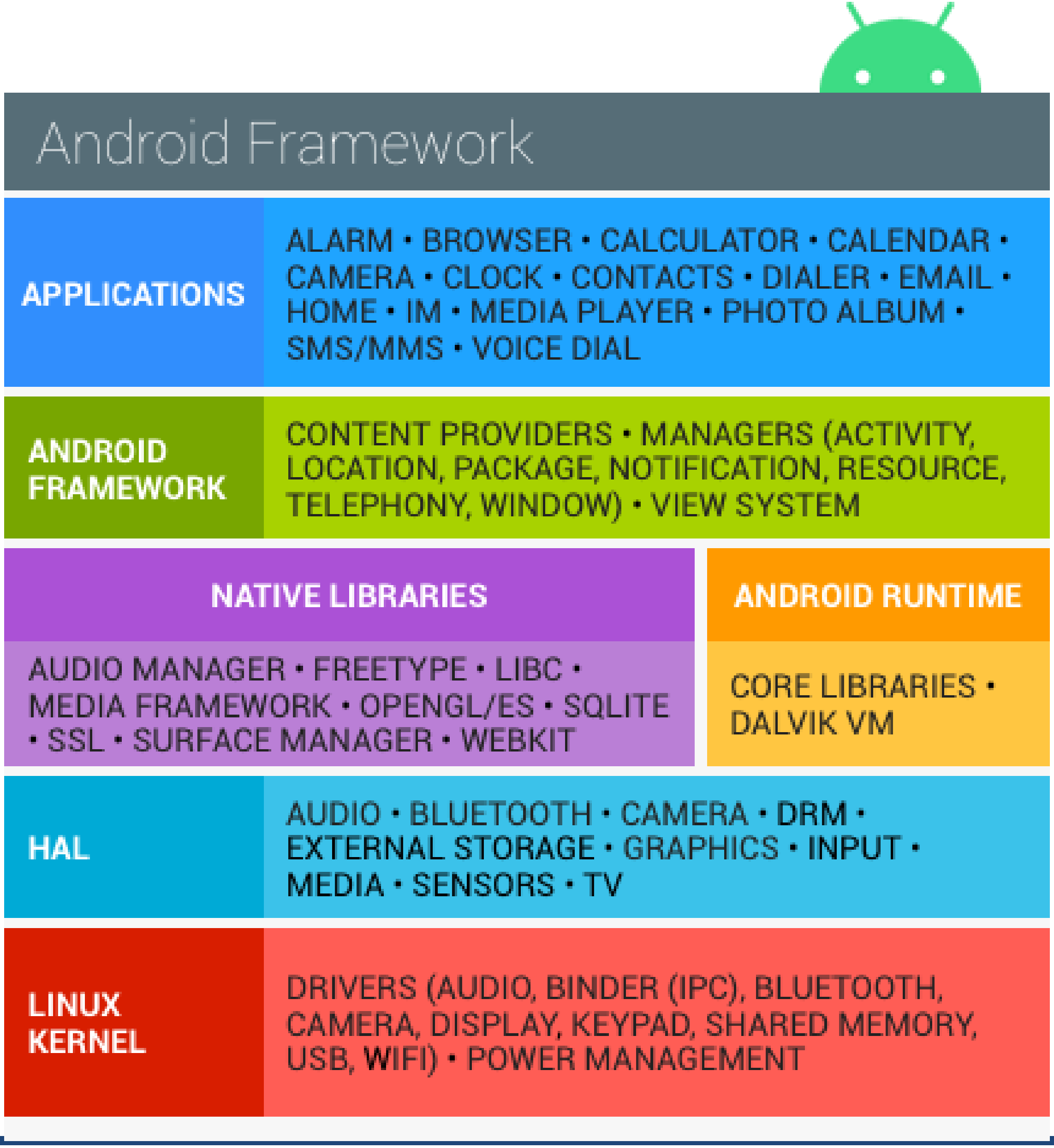
1. **Android is designed to be open.**
2. **Android is designed for developers**
3. **Android is designed for users**

BACKGROUND FOR ANDROID FRAMEWORK

Background for android framework

- ❑Android provides an open source platform and app environment for mobile devices.

Android software stack →



Android Framework

APPLICATIONS
ALARM • BROWSER • CALCULATOR • CALENDAR • CAMERA • CLOCK • CONTACTS • DIALER • EMAIL • HOME • IM • MEDIA PLAYER • PHOTO ALBUM • SMS/MMS • VOICE DIAL

ANDROID FRAMEWORK
CONTENT PROVIDERS • MANAGERS (ACTIVITY, LOCATION, PACKAGE, NOTIFICATION, RESOURCE, TELEPHONY, WINDOW) • VIEW SYSTEM

NATIVE LIBRARIES
AUDIO MANAGER • FREETYPE • LIBC • MEDIA FRAMEWORK • OPENGL/ES • SQLITE • SSL • SURFACE MANAGER • WEBKIT

ANDROID RUNTIME
CORE LIBRARIES • DALVIK VM

HAL
AUDIO • BLUETOOTH • CAMERA • DRM • EXTERNAL STORAGE • GRAPHICS • INPUT • MEDIA • SENSORS • TV

LINUX KERNEL
DRIVERS (AUDIO, BINDER (IPC), BLUETOOTH, CAMERA, DISPLAY, KEYPAD, SHARED MEMORY, USB, WIFI) • POWER MANAGEMENT

BACKGROUND FOR ANDROID FRAMEWORK

The main Android platform building blocks are

Device hardware:

Android runs on a wide range of hardware configurations including mobile phones, tablets, watches, automobiles, smart TVs, OTT gaming boxes, and set-top-boxes. Android is processor-agnostic, but it takes advantage of some hardware-specific security capabilities such as ARM execute-Never**.**

Android operating system:

The core operating system is built on top of the Linux kernel. All device resources, like camera functions, GPS data, Bluetooth functions, telephony functions, and network connections are accessed through the operating system.

Android Application Runtime:

Android apps are most often written in the Java programming language and run in the Android runtime (ART). However, many apps, including core Android services and apps, are native apps or include native libraries. Both ART and native apps run within the same security environment, contained within the Application Sandbox. Apps get a dedicated part of the file system in which they can write private data, including databases and raw files.

BACKGROUND FOR ANDROID FRAMEWORK

Android apps extend the core Android operating system.

There are two primary sources for apps:

Preinstalled apps:

Android includes a set of preinstalled apps including phone, email, calendar, web browser, and contacts. These function as user apps and they provide key device capabilities that can be accessed by other apps. Preinstalled apps may be part of the open source Android platform, or they may be developed by a device manufacturer for a specific device.

User-installed apps:

Android provides an open development environment that supports any third-party app. Google Play offers users hundreds of thousands of apps.

MCQ

6. Which of the following is an example of passive reconnaissance?

a) Telephonic calls to target victim

b) Attacker as a fake person for Help Desk support

c) Talk to the target user in person

d) Search about target records in online people database

7. ________ phase in ethical hacking is known as the pre-attack phase.

a) Reconnaissance

b) Scanning

c) Gaining access

d) Maintaining access

8. While looking for a single entry point where penetration testers can test the vulnerability, they use ______ phase of ethical hacking.

a) Reconnaissance

b) Scanning

c) Gaining access

d) Maintaining access

9. Which of them does not comes under scanning methodologies?

a) Vulnerability scanning

b) Sweeping

c) Port Scanning

d) Google Dorks

10. Which of them is not a scanning tool?

a) NMAP

b) Nexpose

c) Maltego

d) Nessus

REFERENCES

❑https://source.android.com/security