Mobile Security Architecture

Anatomy of a Mobile Attack

C|EH Certified Ethical Hacker

Point 01 – THE DEVICE

BROWSER

- Phishing
- Framing
- Clickjacking
- Man-in-the-Mobile
- Buffer Overflow
- Data Caching

PHONE/SMS

- Baseband Attacks
- SMiShing

APPS

- Sensitive Data Storage
- No Encryption/Weak Encryption
- Improper SSL Validation
- Config Manipulation
- Dynamic Runtime Injection
- Unintended Permissions
- Escalated Privileges
- Access to device and User Info

MALWARE

Point 02 – THE NETWORK

THE NETWORK

- Wi-Fi (no encryption/weak encryption
- Rogue Access Point
- Packet Sniffing
- Man-in-the-Middle (MITM)
- Session Hijacking
- DNS Poisoning
- SSLStrip
- Fake SSL Certificate

Point 03 – THE DATA CENTER

INTERNET

WEB SERVER

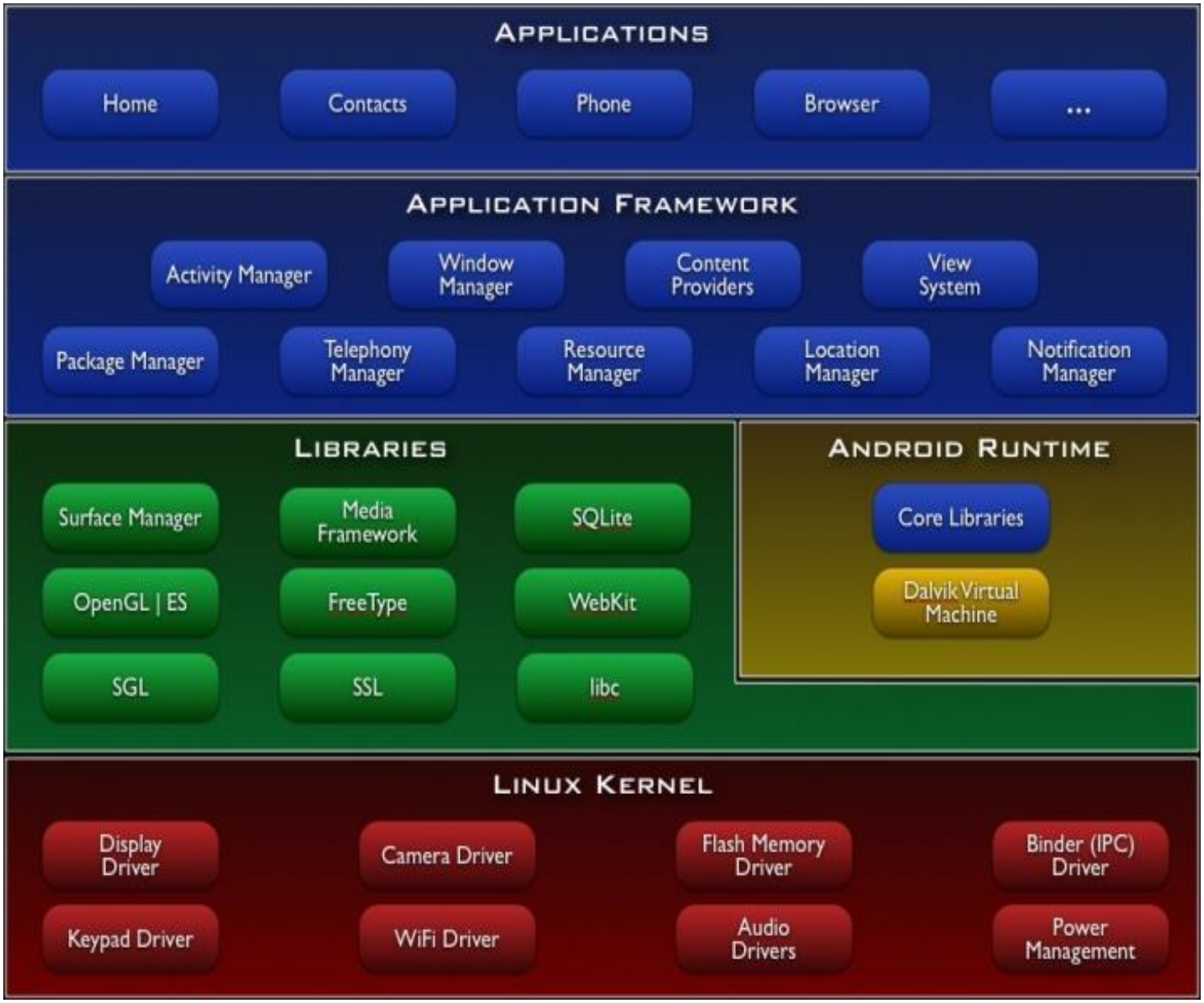
- Platform Vulnerabilities
- Server Misconfiguration
- Cross-site Scripting (XSS)
- Cross-site Request Forgery (XSRF)
- Weak Input Validation
- Brute Force Attacks

DATABASE

- SQL Injection
- Privilege Escalation
- Data Dumping
- OS Command Execution

https://viaforensics.com

Mobile Attack Vectors

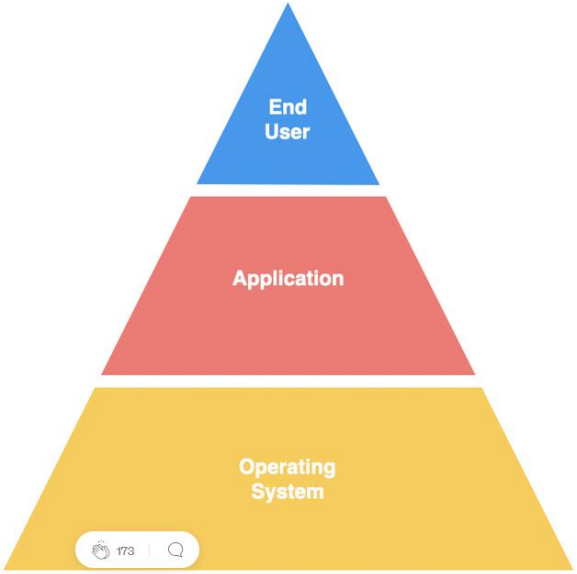


http://developer.android.com/images/system-architecture.jpg

Android Security Model

The security model is based on the consent of the following parties:

- **Operating System**
- **Application**
- **End-User**



For an action to be successfully executed, all three parties must agree on it.

Operating System

The security of the Android operating system is based around the following key security features of the Linux kernel:

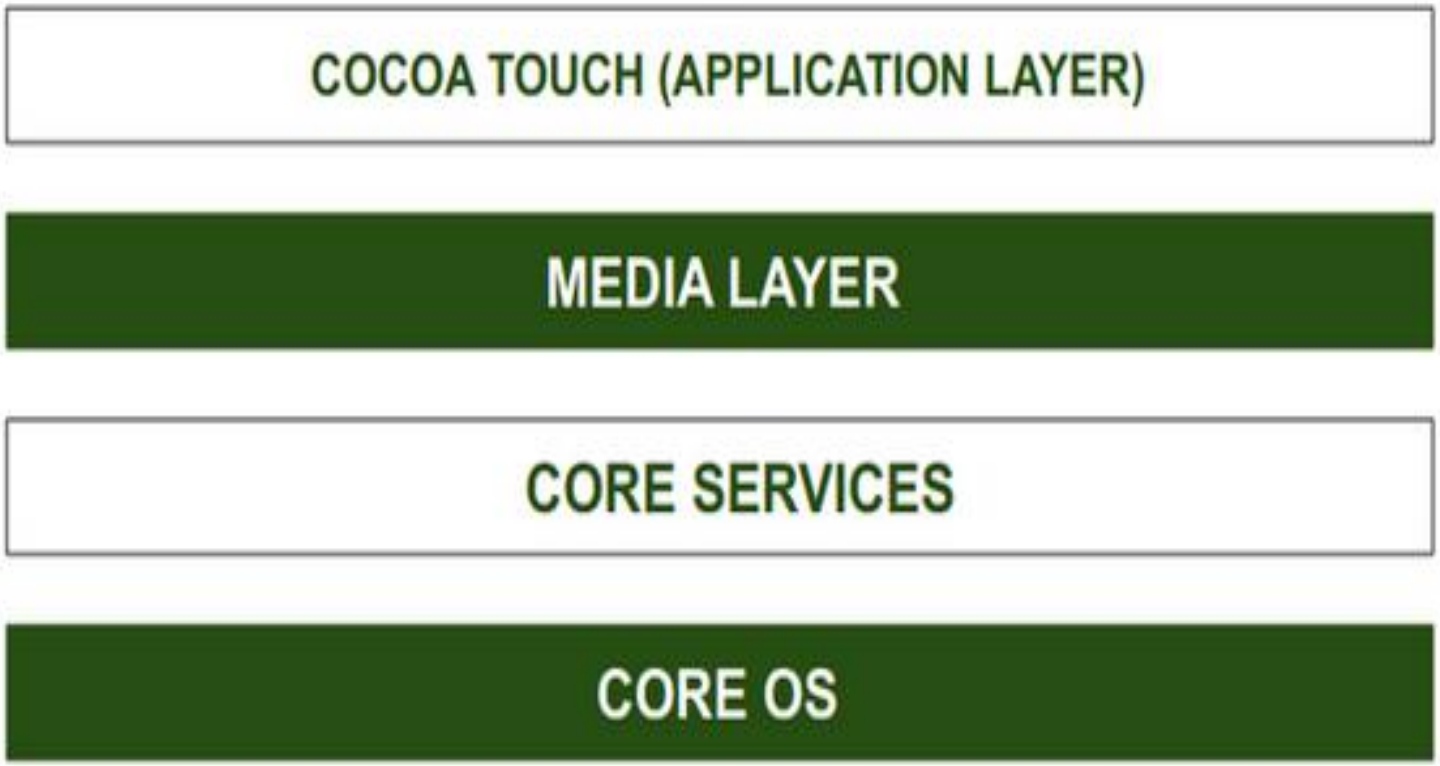
- **Process Isolation**
- **User-Based Permission Model**
- **Inter-Process Communication (IPC)**

IOS SECURITY ARCHITECTURE

iOS architecture

There are basically four layers in the iOS architecture: **Core OS, Core Services, Media, and Cocoa Touch**. The first refers to interactions with the kernel and hardware, essential services along with their associated frameworks, graphic handling, and the user interface along with the app interaction in charge of audio and video.

iOS architecture



Features of iOS operating system

- It is Highly Securer than other operating systems.
- iOS provides the facility of multitasking like while working in one application we can switch to another application easily.
- The user interface of iOS's includes multiple gestures like swipe, tap, pinch, Reverse pinch.
- iBooks, iStore, iTunes, Game Center, and Email are user-friendly.
- It provides Safari as a default Web Browser.
- It has powerful API and Camera.
- It has deep hardware and software integration.

Core Services Layer in iOS

- **Address Book Framework:** The Address Book Framework provides access to the contact details of the user.
- **Cloud Kit Framework:** This framework provides a medium to transfer data between your app and iCloud.
- **Core Data Framework:** It is the technology used to handle the data model of a Model View Controller app.
- **Core Foundation Framework:** This framework offers data management and service features for iOS applications.
- **Core Location Framework:** This framework helps in delivering location and heading information to the application.