Hello Everyone! In this video, you will learn about the Android operating system, it's architecture and it's its security features.

A Mobile Device is a general term used for handheld computing devices which are small in size such as Smartphones, Tablets, E-readers etc. These devices have Small form factor, are portable and have wireless communication capability.

Mobile devices have a series of networks and interconnected systems existing to support mobility. The utility of modern mobile devices is greatly enhanced by software applications and their supporting cloud services. Mobile Operating Systems provide dedicated application stores for end users offering a convenient and customized means of adding functionality. However, Application stores may pose an additional threat vector for attackers to distribute malware or other harmful software to end users. This is especially true of third-party application stores not directly supervised by mobile OS vendors

Contemporary mobile devices contain integrated hardware components to support a variety of I/O mechanisms. While some of the communication mechanisms are wireless (i.e., cellular, Wi-Fi, Bluetooth, GPS, NFC), others require a physical connection (i.e., power and synchronization cable, SIM, external storage). As seen in Figure, each of these different wireless and wired device communication mechanisms exposes the device to a distinct set of threats

and must be secured otherwise the overall security of the device may be compromised.

- Android is the most popular and commonly used mobile operating system.
- It is based on a modified version of the Linux kernel and other open-source software, primarily designed for touchscreen mobile devices such as smartphones and tablets.
- Android is developed by a partnership of developers known as the Open Handset Alliance and commercially sponsored by Google.
- It was disclosed in November 2007, with the first commercial Android device, the HTC Dream, launched in September 2008.

Let's understand the architecture of Android OS.

The foundation of the Android platform is the Linux kernel. Using a Linux kernel allows Android to take advantage of key security features and allows device manufacturers to develop hardware drivers for a well-known kernel. The hardware abstraction layer (HAL) consists of multiple library modules, each of which implements an interface for a specific type of hardware component, such as the camera or Bluetooth module. For devices running Android version 5.0 (API level 21) or higher, each app runs in its own process and with its own instance of the Android Runtime (ART). ART is written to run multiple virtual machines on low-memory devices by executing DEX files. A DEX file is a bytecode format designed specifically for Android and optimized for a minimal memory footprint.

Many core Android system components and services, such as ART and HAL, are built from native code that requires native libraries written in C and C++. The Android platform provides Java framework APIs to expose the functionality of some of these native libraries to apps. If you are developing an app that requires C or C++ code, you can use the Android NDK to access some of these native platform libraries directly from your native code. The entire feature set of the Android OS is available to you through APIs written in the Java language. These APIs form the building blocks you need to create Android apps by simplifying the reuse of core, modular system components, and services, which include the following. Android comes with a set of core apps for email, SMS messaging, calendars, internet browsing, contacts, and more. Apps included with the platform have no special status among the apps the user chooses to install. So a third-party app can become the user's default web browser, SMS messenger, or even the default keyboard (some exceptions apply, such as the system's Settings app).

No to apps in Android devices are allowed to talk to each other directly. Communication between them happens via well-defined interfaces exposed by the OS security checks, once you allow it. Here, IN this figure two Apps A and B are sandboxed i.e. isolated and cannot talk to each other without user’s permission.

Thank You