International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Android Security, An Overview

Raj Singh Gaur

Abstract: ***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 applications and devices built on and around the Android platform and supported by cloud services.***

Keywords: Android, security

1. Introduction

Android is a mobile operating system developed by Google, based on the Linux kernel and designed primarily for touch screen mobile devices such as smartphones and tablets. An Android app is a software application running on the Android platform. Because the Android platform is built for mobile devices, a typical Android app is designed for a smartphone or a tablet PC running on the Android OS.

Security threats on Android are reportedly growing exponentially, however, Google engineers have argued that the malware and virus threat on Android is being exaggerated by security companies for commercial reasons, and have accused the security industry of playing on fears to sell virus protection software to users. Google maintains that dangerous malware is actually extremely rare, and a survey conducted by F-Secure showed that only 0.5% of Android malware reported had come from the Google Play store. Google says, Android has been subject to a rigorous security program.

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 applications 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.

2. Objectives

Android seeks to be the most secure and usable operating system for mobile platforms by re-purposing traditional operating system security controls to:

- Protect application and user data
- Protect system resources (including the network)
- Provide application isolation from the system, other applications, and from the user

3. Features

To achieve above objectives, Android provides these key security features:

- Robust security at the OS level through the Linux kernel
- Mandatory application sandbox for all applications
- Secure inter-process communication
- Application signing
- Application-defined and user-granted permissions

4. Applications

Android applications extend the core Android operating system. There are two primary sources for applications:

Pre-installed applications: Android includes a set of pre-installed applications including phone, email, calendar, web browser, and contacts. These function both as user applications and to provide key device capabilities that can be accessed by other applications. Pre-installed applications may be part of the open source Android platform, or they may be developed by a device manufacturer for a specific device.

User-installed applications: Android provides an open development environment that supports any third-party application. Google Play offers users hundreds of thousands of applications.

5. Plateforms

Android provides an open source platform and application environment for mobile devices. *Figure 1* summarizes the security components and considerations of the various levels of the Android software stack. Each component assumes that the components below are properly secured. With the exception of a small amount of Android OS code running as root, all code above the Linux Kernel is restricted by the Application Sandbox.

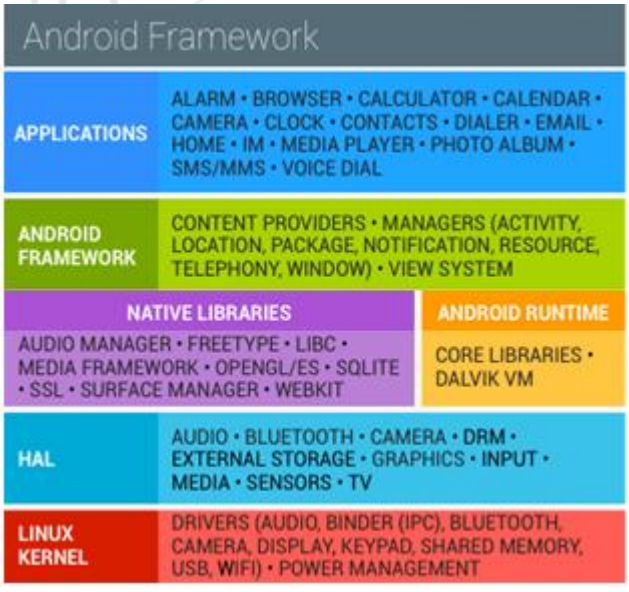

Figure 1: Android software stack

Licensed Under Creative Commons Attribution CC BY

The main Android platform building blocks are:

- **Device hardware**: Android runs on a wide range of hardware configurations including smart phones, tablets, watches, automobiles, smart TVs, OTT gaming boxes, and set-top-boxes. Android is processor-agnostic, but it does take 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, network connections, etc. are accessed through the operating system.
- **Android Application Runtime**: Android applications are most often written in the Java programming language and run in the Android runtime (ART). However, many applications, including core Android services and applications, are native applications or include native libraries. Both ART and native applications run within the same security environment, contained within the Application Sandbox. Applications get a dedicated part of the filesystem in which they can write private data, including databases and raw files.

6. Security Services

Google provides a set of cloud-based services that are available to compatible Android devices with Google Mobile Services. While these services are not part of the Android Open Source Project, they are included on many Android devices. The primary Google security services are:

1) **Google Play**: Google Play is a collection of services that allow users to discover, install, and purchase applications from their Android device or the web. Google Play makes it easy for developers to reach Android users and potential customers. Google Play also provides community review, application license verification, application security scanning, and other security services.
2) **Android updates**: The Android update service delivers new capabilities and security updates to selected Android devices, including updates through the web or over the air (OTA).
3) **Application services**: Frameworks that allow Android applications to use cloud capabilities such as (backing up) application data and settings and cloud-to-device messaging (C2DM) for push messaging.
4) **Verify Apps**: Warn or automatically block the installation of harmful applications, and continually scan applications on the device, warning about or removing harmful apps.
5) **SafetyNet**: A privacy preserving intrusion detection system to assist Google tracking and mitigating known security threats in addition to identifying new security threats.
6) **SafetyNet Attestation**: Third-party API to determine whether the device is CTS compatible. Attestation can also assist identify the Android app communicating with the app server.
7) **Android Device Manager**: A web app and Android app to locate lost or stolen device.

7. Security Programme

The key components of the Android Security Program include:

1) **Design review**: The Android security process begins early in the development lifecycle with the creation of a rich and configurable security model and design. Each major feature of the platform is reviewed by engineering and security resources, with appropriate security controls integrated into the architecture of the system.
2) **Penetration testing and code review**: During the development of the platform, Android-created and open source components are subject to vigorous security reviews. These reviews are performed by the Android Security Team, Google's Information Security Engineering team, and independent security consultants. The goal of these reviews is to identify weaknesses and possible vulnerabilities well before major releases, and to simulate the types of analysis that will be performed by external security experts upon release.
3) **Open source and community review**: The Android Open Source Project enables broad security review by any interested party. Android also uses open source technologies that have undergone significant external security review, such as the Linux kernel. Google Play provides a forum for users and companies to provide information about specific applications directly to users.
4) **Incident Response**: Even with all of these precautions, security issues may occur after shipping, which is why the Android project has created a comprehensive security response process. Full-time Android security team members monitor Android-specific and the general security community for discussion of potential vulnerabilities and review security bugs filed on the Android bug database. 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. These cloud-supported responses can include updating the Android platform (over-the-air updates), removing applications from Google Play, and removing applications from devices in the field.
5) **Monthly security updates**: The Android security team provides monthly updates to Google Nexus devices and all of our device manufacturing partners.

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 applications and devices built on and around the Android platform and supported by cloud services.

Reference

[1] www.android.com

Author Profile

Raj Singh Gaur is Faculty, Staff Training Centre, Union Bank of India, Bhopal. He did PG in Pub. Personnel Management, CAIIB, Certificates in Trade Finance and in KYC-AML by IIBF. He can be contacted at raj.gaur [@] rediffmail.com

Licensed Under Creative Commons Attribution CC BY