Security in Android

Seminararbeit

Hochschule für angewandte Wissenschaften
Würzburg-Schweinfurt

Kristoffer Schneider

20. Mai 2015

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Das Android Betriebssystem

Das Unternehmen Android wurde 2003 von Andy Rubin gegründet und wurde 2005 von Google aufgekauft. Seitdem kümmert sich Google und das Android Open Source Project (AOSP) um die Weiterentwicklung des Systems. Aktuell ist Android, mit 55.6% Marktanteil[1], das vorherrschende Betriebssystem für mobile Endgeräte in den USA.

Basis für das Betriebssystem ist ein modifizierter Linux-Kernel und eine Java Virtual Machine (JVM). Bis einschliesslich Version 4.4 wurde hierfür die Dalivk Runtime und für alle neueren Versionen die Android Runtime (ART) verwendet. Jede App läuft in einer eigenen Instanz der entsprechenden Runtime und damit in einer Sandbox.
Oberhalb der JVM sind die meisten Komponenten in Java implementiert.

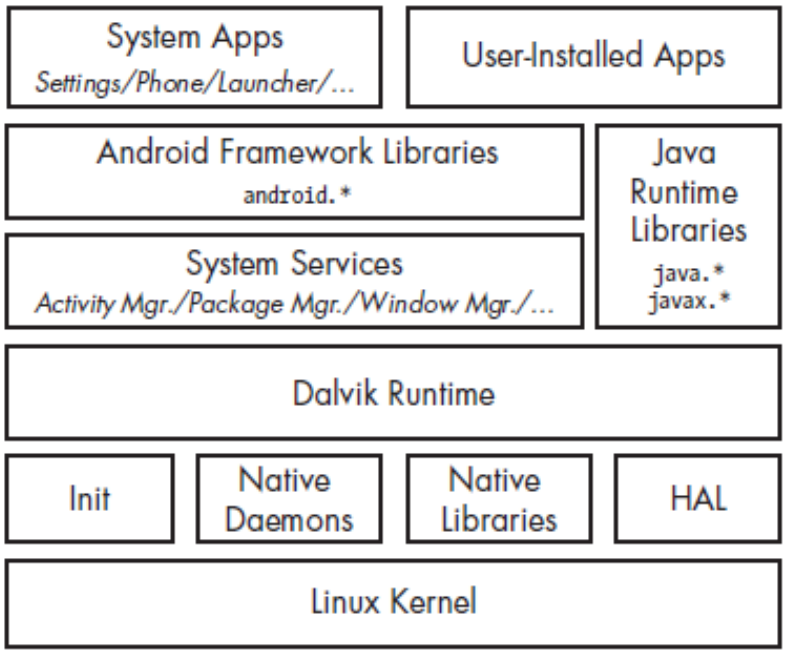

Abbildung 1: Die Architektur von Android ASI-P-2

[1] Kantar Worldpanel: Smartphone OS sales market share, http://www.kantarworldpanel.com/global/smartphone-os-market-share/, 17.5.2015

2 Grundlegender Aufbau einer Android App

> Android apps are written in the Java programming language. The Android SDK tools compile your code - along with any data and resource files - into an APK: an *Android package*, which is an archive file with an .apk suffix. One APK file contains all the contents of an Android app and is the file that Android-powered devices use to install the app.

Eine App besteht im Kern aus zwei Teilen. Den eigentlichen Programmkomponenten und einer Manifest Datei.
Als Programmkomponenten können unter anderem vorkommen:

- Activities - stellen die Benutzeroberfläche dar
- Services - kann im Hintergrund laufen, auch wenn die App minimiert ist
- Content Provider - stellt Daten aus bspw. Datenbanken für die eigene und evtl für andere Apps zur Verfügung
- Broadcast Receiver - um Systemweite Benachrichtigungen zu empfangen (z.B dass ein Download beendet wurde)

In der Manifest-Datei werden Eigenschaften der App definiert. Darunter zählen beispielsweiße:

- Name der App
- Ziel SDK-Versionen
- Versionsnummer
- optional eine UserId (siehe 3.1)
- Permissions (siehe 3.2)

Desweiteren muss jede App signiert werden. Das hierfür benötigte Zertifikat kann sich jeder selbst generieren und muss nicht durch einen Certification Authority (CA) beglaubigt werden. Dabei wird angeraten, dass ein Entwickler für all seine Apps dasselbe Zertifikat nutzt.

3 Sicherheitsaspekte der Android-Architektur

Bereits durch die Architektur des Betriebssystems, insbesondere durch die restriktive Rechtevergabe und das Sandboxing, wird versucht ein möglichst sicheres System bereitzustellen.

3.1 Basis Rechtesystem

Von Linux wurde auch das Basis-Rechtesystem übernommen. Hierbei bekommt jede App eine eindeutige User-ID (UID) zugewiesen, welche im Normalfall zur Installationszeit zugeteilt wird. Jeder Nutzer, und somit auch jede App, arbeitet grundsätzlich erst einmal nur innerhalb der ihm zugewiesenen virtuellen Maschine und dem damit verbundenen Dateisystem.

Da es dennoch in vielen Fällen nötig ist Daten zwischen verschiedenen Apps auszutauschen, gibt es mehrer Möglichkeiten dies zu tun. Die üblichen Wege wären Intends oder SharedPreferences. Zusätzlich gibt es noch die Möglichkeit mehreren Apps dieselbe UID zuweisen zu lassen. Dies ist allerdings nur möglich wenn die entsprechenden Applikationen mit dem selben Zertifikat signiert wurden und in deren Manifest Datei eine gemeinsame UID festgelegt wurde. Durch dieses Rechtesystem wird versucht sicherzustellen, dass kein Nutzerprogramm als *root* ausgeführt wird.

3.2 Sandboxing und Permissions