Statische Informations- und Datenflussanalyse von Android-Apps

Markus Schmidt
Universität Siegen, Bachelorstudiengang Informatik
markus1.schmidt@student.uni-siegen.de

Im Zeitalter von zunehmender Überwachung durch Kriminelle oder staatlichen Institutionen gewinnt die IT-Sicherheit immer mehr an Bedeutung. Von einer Sicherheitslücke sind oft viele Endgeräte betroffen. Die Folge kann eine große Menge an ausgespähten Daten sein. Dahingehend existieren Werkzeuge zur Analyse von Applikationen wie die Datenflussanalyse, welche die technischen Aspekte, und die Informationsflussanalyse, welche die inhaltlichen Aspekte, wie zum Beispiel Sicherheitslücken im Programmcode, analysiert. In der vorliegenden Arbeit wurden einige Methoden vorgestellt. Außerdem wurde eine Analyse an einer Beispiel-App evaluiert.

Die Analyse mit der Methode Dexpler [BJK13] anhand der Beispiel-App ist eine reine Datenflussanalyse und zeigt die technischen Möglichkeiten und Grenzen der statischen Analyse auf. Für einfache Verschachtelungen im Quelltext werden zuverlässige Ergebnisse produziert, die für die weitere inhaltliche Analyse genutzt werden können. [FAR+13] Mithilfe der Analyse des Dalvik-Bytecodes der kompilierten apk-Datei eines Android-Handys wird der Datenfluss gut lesbar repräsentiert. Mit verschiedenen Repräsentationen als zum Beispiel Kontrollflussdiagramm, Quelltext und Zwischenstufen des Dekompilierens lassen sich einzelne Aspekte fokussieren und beurteilen.

Die Methoden der Informationsflussanalyse stellen als grösstes Problem die Identifikations-IDs (IMEI, IMSI, Phone Number) heraus. Daneben wird besonders der Standort abgefragt. Dies ist meist für Werbenetzwerke interessant, die bezüglich des Standortes personalisierte Werbung anzeigen und den Anwender so gezielt beeinflussen wollen. Die Ergebnisse aller Methoden unterscheiden sich nur unwesentlich. Die statische Daten- und Informationsflussanalyse kann bei der Analyse helfen, allerdings sind die Ergebnisse immer als Tendenz zu verstehen.

Literatur

[BJK13] Alexandre Bartel und Martin Monperrus Jacques Klein, Yves Le Traon. Dexpler: Converting Android Dalvik Bytecode to Jimple for Static Analysis with Soot. 2013.

[FAR+13] Christian Fritz, Steven Arzt, Siegfried Rasthofer, Eric Bodden, Alexandre Bartel, Jacques Klein, Yves le Traon, Damien Octeau und Patrick McDaniel. Highly Precise Taint Analysis for Android Applications. 2013.