Kann Malware in Android-Apps automatisch gefunden werden? (Verschiedene Analysemethoden für Android-Apps)

Cöllen, Markus
Hochschule Mannheim
Fakultät für Informatik
Paul-Wittsack-Str. 10, 68163 Mannheim

***Zusammenfassung*—An dieser Stelle steht eine kurze Zusammenfassung des Inhaltes des Dokuments.**

Inhaltsverzeichnis

1. Einleitung

2. Grundlagen

2.1. Android und Sicherheitslücken

2.2. Google Play Store

Der Google Play Store oder früher auch Android Market wurde am 28. Ausgust 2008 eröffnet. Dieser bietet den Nutzern einfaches herunterladen und installieren von mobilen Anwendungen, sogenannten Apps. Im Google Play Store sind bereits über 3,7 Millionen Anwendungen bereit zum Herunterladen (Stand vom 18. April 2018) [2] und jeden Monat kommen ca. 30.000 neue Apps hinzu [1]. Durch den rasanten Wachstum steigt auch die Anzahl von schädlicher Software, sogenannter Malware. Der Anteil von bösartigen Apps ist von 2011 bis 2013 um 388% gewachsen [3]. Da nicht alle Anwendungen von Mitarbeitern geprüft werden können hat Google das Programm Bouncer ins Leben gerufen (siehe Kapitel 4).

2.3. Malware

Der Begriff Malware steht für malicous software und bezeichnet Programme, welche unerwünschte oder auch schädliche Funktionen ausführen. Sie stellen eine immer größer werdende Bedrohung dar und durch den rasanten Wachstum ist eine manuelle Auswertung mittlerweile unmöglich geworden. Obwohl es sich bei vielen neuen Arten um verschiedene Varianten bereits bekannter Malware handelt, müssen Analysten erst jedes Sample erneut analysieren um dies feststellen zu können [4]. Bei der Analyse kann Grundsätzlich in zwei Arten unterschieden werden, Statische und Dynamische Analyse (siehe Kapitel 3.1 und 3.2).

2.3.1. Android als Ziel.

2.3.2. Klassifizierung.

3. Analysemethoden

3.1. Statische Analyse

3.1.1. Data Flow.

3.1.2. Control Flow.

3.2. Dynamische Analyse

4. Bouncer

5. FlowDroid

6. Crowdroid

7. Fazit

Eine Abkürzung = Application-to-Application (A2A)

Abkürzungen

A2A Application-to-Application

Literatur

[1] Steffen Bartsch u.a. „Zertifizierte Datensicherheit für Android-Anwendungen auf Basis statischer Programmanalysen.“ In: *Sicherheit*. 2014, S. 283–291.

[2] *Google Play Apps Statistik*. https://de.statista.com/statistik/daten/studie/74368/umfrage/anzahl-der-verfuegbaren-apps-im-google-play-store/. Accessed: 2018-04-22.

[3] *RiskIQ report about Malicious Mobile Apps in Google Play*. https://www.riskiq.com/press-release/riskiq-reports-malicious-mobile-apps-google-play-have-spiked-nearly-400/. Accessed: 2018-04-22.

[4] Philipp Trinius. *Visualisierung von Malware-Verhalten*. Universitätsbibliothek Dortmund, 2010.