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

Anders als bei IOS, bei welchem die Nutzer an den Apple Store gebunden sind, können die Android Benutzer selbst entscheiden welchen Store sie verwenden. Der Google Play Store ist mit 82 Milliarden Downloads [1] mit Abstand die größte Plattform. Er wurde am 28. August 2008 unter dem Namen Android Market veröffentlicht. 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 [3] und jeden Monat kommen ca. 30.000 neue Apps hinzu [2]. 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 [5]. 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 [8]. Bei der Analyse kann Grundsätzlich in zwei Arten unterschieden werden, Statische und Dynamische Analyse (siehe Kapitel 3.1 und 3.2).

2.4. Android als Ziel

Ein Hauptgrund, warum Smartphones mit dem Android Betriebssystem so beliebt für Angreifer sind, ist der hohe Verbreitungsgrad dieser Geräte. Dieser liegt im Jahr 2018 bei ca. 86 Prozent und ist somit Sechs mal so hoch wie der Konkurrent IOS mit knapp 16 Prozent Marktanteil [4]. Weil Android unter der Apache Open-Source Lizenz freigegeben ist und das Betriebssystem auf dem Linux-Kernel basiert, können Hersteller dieses beliebig verwenden und für ihre Produkte anpassen. Zudem dient der Linux-Kernel als eine Abstraktion zwischen Software und Hardware und somit kann Android auf verschiedenen Geräten eingesetzt werden. Aufgrund der Tatsache, dass Linux über ein etabliertes Sicherheitskonzept verfügt [7], greift Android auf viele Schutzmechanismen des Linux Kernels zurück oder benutzt diese als ihre Basis [6].

2.4.1. 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] *Anzahl der Apps, die im Google Play Store heruntergeladen wurden*. https://de.statista.com/statistik/daten/studie/243412/umfrage/anzahl-von-downloads-im-google-play-store/. Accessed: 2018-04-25.

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

[3] *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.

[4] *Marktanteil von Android*. https://www.netzwelt.de/news/164146-android-vs-ios-plattform-treue-android-91-prozent-deutlich-hoeher.html. Accessed: 2018-04-25.

[5] *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.

[6] Julian Scheid. „Kapitel 1 Sicherheit mobiler Geräte-Schutzmaßnahmen, Angriffsarten & Angriffserkennung auf Android“. In: *Ausgewählte Themen der IT-Sicherheit* (2012), S. 7.

[7] *Sicherheitskonzepte von Linux*. https://wiki.ubuntuusers.de/Archiv/Sicherheitskonzepte/. Accessed: 2018-04-25.

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