Titel: AnSWER – Android Software Risk Evaluator

Einleitung:

Mobile Applikationen („Apps“) haben immer häufiger Zugriff auf sensible Daten wie z. B. Passwörter, Dokumente und persönliche Bilder. In Anbetracht dieser Tatsache gewinnt das Thema Sicherheit bei der Entwicklung von mobilen Applikationen einen immer größeren Stellenwert. Insbesondere Googles Android Plattform in ihrer Rolle als Marktführer ist ein beliebtes Ziel für Angreifer, welche Schwachstellen in mobilen Applikationen ausnutzen, um an sensible Daten zu gelangen. Studien[2] zeigen, dass bis zu 24% aller mobilen Apps Sicherheitslücken aufweisen. Die Einhaltung von Best Practice Guidelines wie z. B. das „OWASP – Mobile Security Project“[3] sollte deshalb ein fixer Bestandteil des Software-Entwicklungsprozesses sein, um so Entwicklern zu helfen, sichere Anwendungen zu erstellen. Obwohl es eine Vielzahl von Werkzeugen gibt, welche Sicherheitsexperten unterstützen, das Verhalten von bereits veröffentlichten Applikationen zu bestimmen (mittels Byte-Code Analyse), gibt es kaum Tools zur Überprüfung des Programmcodes während des Entwicklungsprozesses. Durch die kurzen Entwicklungszyklen in mobilen Anwendungen und die ständigen Updates der mobilen Plattformen entsteht so für Entwickler eine weitere Anforderung, welche oft nicht berücksichtigt wird. Wie können also bekannte Sicherheitsrisiken bereits während der Entwicklung erkannt und behoben werden? AnSWER stellt einen neuen Ansatz vor, der anhand von statischer Code Analyse den Quellcode von mobilen Applikationen hinsichtlich potentieller Sicherheitslücken überprüft.

Methodik:

Die Grundlage dieses Konzepts sind spezielle Security Richtlinien[1] (Linter Regeln) basierend auf den fünf wichtigsten Sicherheitsrisiken (M1-M5) der „Top 10 OWASP Mobile Risks“ für mobile Anwendungen. Die Implementierung basiert auf dem bereits bestehenden „Android Lint Tool“, welches sowohl in die Entwicklungsumgebung „Android Studio“ integriert ist, als auch als Teil der „Continuous Integration“ (CI) Pipeline verwendet werden kann. Insbesondere die Integration in den Build-Prozess erlaubt die kontinuierliche Überprüfung der App während des gesamten Software-Entwicklungsprozesses.

Evaluierung:

Zum Testen des entwickelten Linter Regel-Sets und zur Überprüfung der Praxistauglichkeit wurden zehn weit verbreitete Open Source Android Apps sowohl mit AnSWER als auch mit einem kommerziellen Security Checker (Mobile X-Ray App Scanner[1]) untersucht. Dieser

[1] https://www.htbridge.com/mobile

untersucht im Gegensatz zu AnSWER das Android Package (APK), welches im Google Play Store veröffentlicht wird.

Applikation	Kategorie	# Downloads
Signal	Communications	10.000.000
Lightning Web Browser	Communications	500.000
FreeOTP Authenticator	Tools	100.000
Nextcloud	Tools	100.000
Open Camera	Photography	10.000.000

Tabelle 1: Auszug der evaluierten Open-Source Apps und ihre Download Zahlen aus dem Google Play Store

Die gefundenen potentiellen Sicherheitslücken wurden anschließend auch durch manuelle Code Reviews genauer analysiert, um „falsch-positiv“ Ergebnisse zu filtern.

Ergebnisse:

Die Anzahl der gefundenen Risiken zeigt, dass der Ansatz von AnSWER in den meisten Fällen mehr potentielle Fehler findet als die kommerzielle Lösung. Wie in Abbildung 1 ersichtlich ist, wurden im Durchschnitt 5,4 mehr Risiken erkannt. Dies entspricht einer Steigerung von 27% gegenüber der kommerziellen Lösung.

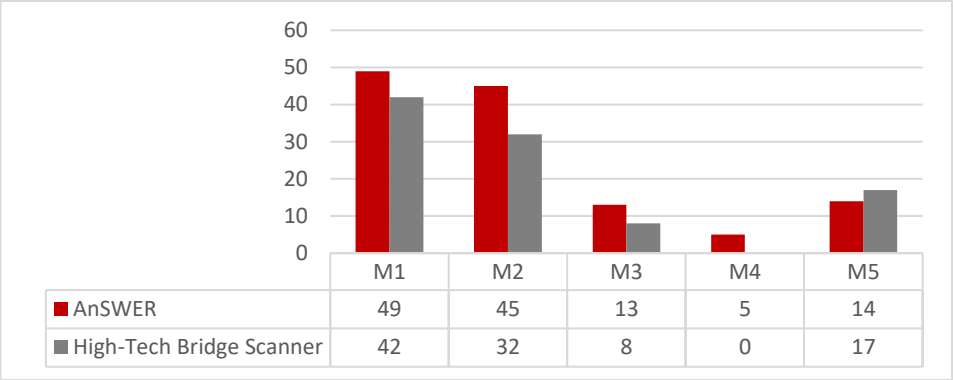

Abbildung 1: Vergleich der gefundenen Sicherheitslücken

Conclusio:

Die getesteten Applikationen zeigten teilweise gravierende Mängel, welche durch die Verwendung von AnSWER bereits während der Entwicklung erkannt und behoben hätten werden können. Darüber hinaus konnten durch die direkte Verknüpfung mit dem Quellcode nicht nur mehr potentielle Mängel gefunden werden, sondern auch deren genaue Stelle im Code lokalisiert werden.

[1] Lind V. 2018. Improvement of App Security with Security Checks Integrated into Build Process. Diplomarbeit FH JOANNEUM.

[2] NowSecure, Inc. 2016. NowSecure Mobile Security Report; https://www.nowsecure.com/ebooks/2016-nowsecure-mobile-security-report/ (abgerufen am 10.12.2018)

[3] OWASP Mobile Security Project. Mobile Security Project Top 10 Mobile Risks. https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10 (abgerufen am 10.12.2018)