



CODEINSPECT

ANALYSEWERKZEUG FÜR ANDROID-APPS

Viele mobile Anwendungen weisen zum Teil gravierende Sicherheitsmängel auf. Um die detaillierte Prüfung der Sicherheitseigenschaften von Android-Apps für Analysten, Entwickler und IT-Consultingunternehmen effizienter zu gestalten, hat Fraunhofer SIT CodeInspect entwickelt. Mit diesem Werkzeug lassen sich schnell und mit höchstem Detailgrad Schwachstellen in der App aufspüren, auch wenn diese nicht im Quelltext vorliegt. Unterschiedliche vollautomatische Analysen in Kombination mit manuellem Live-Debugging ermöglichen es, Apps schnell und vollständig nach Auffälligkeiten wie Programmierfehlern, Sicherheitslücken oder schadhaftem Verhalten zu durchforsten. Zusätzlich bietet CodeInspect als einziges Werkzeug eine integrierte Liveanalyse der App während der Laufzeit.

Immer mehr mobile Endgeräte halten Einzug in den Unternehmensalltag. Sie werden genutzt, um kritische Geschäftsdaten zu verarbeiten, ohne dabei an den festen Arbeitsplatzcomputer gebunden zu sein. Während dies besonders für Bereiche wie den Außendienst massive Vereinfachungen mit sich bringt, stellt es auch erhöhte Anforderungen an die Sicherheit dieser Geräte und der darauf installierten Apps. Oftmals liegen die Apps jedoch nicht im Quellcode vor oder es sollen sehr spezifische Firmenrichtlinien geprüft werden, wodurch viele bestehende Analyseverfahren ausscheiden. Mit CodeInspect lassen sich Apps dennoch präzise und effizient mit bestehendem Personal im eigenen Haus analysieren.

Auch App-Entwickler stehen vor ähnlichen Herausforderungen. Oftmals setzen sie Bibliotheken von Drittanbietern ein, zu denen kein Quelltext vorliegt. Dennoch müssen diese Bibliotheken auf Sicherheitslücken geprüft werden. Bei funktionalen Fehlern ist oft-

mals nicht ersichtlich, warum diese auftreten. Mit CodeInspect lassen sich binäre Bibliotheken schnell und einfach begutachten.

Wie funktioniert CodeInspect?

CodeInspect übersetzt den binären Code der App zunächst in eine für Menschen lesbare Sprache. Basierend auf dieser Sprache kann eine manuelle Analyse der App durchgeführt werden. Mithilfe des integrierten Debuggers lässt sich Schritt für Schritt die Funktionsweise der App analysieren. Zudem bietet CodeInspect auch vollautomatische innovative Analysen, die den Benutzer auf Schwachstellen, schadhaftes Verhalten und Verschleierungen in der App aufmerksam machen. Die gefundenen Probleme werden vollautomatisch validiert, um mögliche falsche Warnungen zu eliminieren. Alle Ergebnisse werden in einem übersichtlichen Bericht automatisch dokumentiert.

Plugin-Infrastruktur

Die Funktionalität von CodeInspect lässt sich über Plugins erweitern und individuell anpassen. Mit dem Plugin zur Datenflussanalyse lässt sich etwa überprüfen, ob und auf welchem Weg sensible Daten des Benutzers an Dritte gesendet werden.

CodeInspect eignet sich für:

- IT-Sicherheitsabteilungen/IT-Sicherheitsverantwortliche
- Softwareentwickler
- Entwickler von Software-Bibliotheken
- Hersteller von Antivirenschutzsoftware
- Hersteller von Sicherheitssoftware
- App-Store-Betreiber

Infos zu Werkzeug und Lizenzierung unter:
www.codeinspect.de - kostenlose Testphase möglich.

*Fraunhofer-Institut für Sichere
Informationstechnologie SIT*

*Kontakt:
Dr. Siegfried Rasthofer
Rheinstraße 75
64295 Darmstadt*

*Telefon 06151 869-177
siegfried.rasthofer@sit.fraunhofer.de
www.codeinspect.de*