Fraunhofer
SIT

FRAUNHOFER-INSTITUT FÜR
SICHERE INFORMATIONSTECHNOLOGIE

Fraunhofer-Institut für Sichere Informationstechnologie SIT

Kontakt:
Ph. D. Lotfi ben Othmane
Rheinstraße 75
64295 Darmstadt

Telefon 06151 869-510
Fax 06151 869-224
lotfi.ben.othmane@sit.fraunhofer.de
www.codeinspect.de

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 gemeinsam mit der Technischen Universität Darmstadt CodeInspect entwickelt. Mit diesem Werkzeug lassen sich schnell Schwachstellen und Malware im Programmcode aufspüren. Ein interaktiver Debugger hilft, den Code von Apps schnell zu untersuchen und nach Auffälligkeiten wie Sicherheitslücken, Fehlern oder schadhaftem Verhalten zu durchforsten. CodeInspect ist das einzige Werkzeug, das eine Live-Analyse im Bytecode auf effiziente und benutzerfreundliche Weise ermöglicht.

Täglich kommt eine Vielzahl mobiler Apps für Smartphones und Tablets auf den Markt. Antiviren-Hersteller und Sicherheitsanalysten müssen deshalb täglich Tausende Apps untersuchen. Besonders sensible Apps, etwa für Online-Banking, oder Code-Stücke, die verdächtig aussehen, müssen manuell und besonders sorgfältig überprüft werden. Genauso müssen Softwareentwickler Bibliotheken von Drittanbietern prüfen, wenn sie Zweifel an der Qualität und Sicherheit haben. Analysten und App-Store-Betreiber stehen dabei vor dem Problem, dass die Analyse von Android-Anwendungen schwierig und zeitaufwendig ist. Denn diese liegen oft nur im Binärcode als APK-Datei vor, oder der Code wurde absichtlich verschleiert und unleserlich gemacht. CodeInspect erleichtert diese Arbeit.

Wie funktioniert CodeInspect?
CodeInspect ist ein Framework, das zunächst den binären Code der App in eine für Menschen lesbare Zwischensprache übersetzt. Herzstück von CodeInspect ist ein interaktiver Debugger mit eingebautem Single-Stepping: Damit geht der Analyst den Code der App Schritt für Schritt durch, um nach Unregelmäßigkeiten zu suchen. So können Analysten und Entwickler mithilfe von CodeInspect das Verhalten von Apps genauer unter die Lupe nehmen als dies mit herkömmlichen Werkzeugen möglich ist. Damit kann der Analyst den Code nicht nur lesen, sondern gleichzeitig live sehen, was gerade im Bytecode passiert. CodeInspects Live-Analyse zeigt Laufzeitwerte nicht nur an, sondern erlaubt auch direkte Eingriffe des Analysten in den Programmablauf. Sogar das Einbinden von externem Javacode ist möglich.

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

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