Fraunhofer
SIT

FRAUNHOFER INSTITUTE FOR
SECURE INFORMATION TECHNOLOGY

Fraunhofer Institute for Secure Information Technology SIT

Contact:
Siegfried Rasthofer
Rheinstrasse 75
64295 Darmstadt
Germany

Phone +49 6151 869-177
Fax +49 6151 869-224
siegfried.rasthofer@sit.fraunhofer.de
www.codeinspect.de

CODEINSPECT

ANALYSIS TOOL FOR ANDROID-APPS

Many mobile applications contain some serious security flaws. Together with the Technical University Darmstadt, Fraunhofer SIT has developed CodeInspect to support analysts, developers and IT consulting companies in making the detailed examination of Android app security features more efficient. CodeInspect is able to detect vulnerabilities and malware quickly in program code. An interactive debugger helps to examine the code of apps quickly and to scour for abnormalities such as security vulnerabilities, defects or a defective behavior. CodeInspect is the only tool that enables live analysis in the bytecode in an efficient and user-friendly manner.

Every day a great number of mobile apps for smartphones and tablet computers are introduced into the market. Antivirus producers and other security analysts need to check several thousand apps per day. While they use tools that are able to test an immense number of apps automatically, security-sensitive apps such as banking apps or suspicious looking code fragments have to be checked manually and quite carefully. Software developers have to examine the libraries of third-party providers just the same, when they are in doubt about the quality and security. Both analysts and app store operators have the problem that the analysis of Android apps is difficult and time-consuming. This is because the apps are often only available as an APK file in binary code, or because the code was obfuscated on purpose. CodeInspect makes such analyses easier.

How does CodeInspect work?

CodeInspect is a framework that first translates any Android app's binary code into an intermediate language that is easily understood by human analysts. The heart of CodeInspect is an interactive debugger with built-in single stepping: Using this feature, the analyst can execute the app's code step by step, while at the same time looking for irregularities during the execution. With the help of CodeInspect, analysts and developers can scrutinize apps more quickly and precisely than with conventional tools. The analyst can not only read the code, but also at the same time see what happens during runtime. CodeInspect's live analysis not only displays runtime values but also permits the analyst to directly intervene in the program's sequence.

Plugin infrastructure

The functionality of CodeInspect can be expanded by plugins and adjusting it to individual requirements. E. g. a plugin for the data-flow analysis enables the analyst to check if and how sensitive user data is sent to a third party.

CodeInspect can be used by:

- creators of antivirus protection software
- creators of security software
- IT security departments/IT security professionals
- software developers
- software library developers
- owners of app stores

CodeInspect licences are available on www.codeinspect.de. Fraunhofer SIT and TU Darmstadt offer a time-limited, free of charge test version of CodeInspect.