Fraunhofer
SIT

FRAUNHOFER INSTITUTE FOR
SECURE INFORMATION TECHNOLOGY

Fraunhofer Institute for Secure Information Technology SIT

Contact:
Dr. Siegfried Rasthofer
Rheinstrasse 75
64295 Darmstadt
Germany

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

CODEINSPECT

ANALYSIS TOOL FOR ANDROID-APPS

Many mobile apps suffer from security vulnerabilities, some of which have severe consequences for users and providers. Analysts, developers, and IT consultants therefore often need to analyze Android apps in detail before they are allowed into productive use. To make this task easier and more efficient, Fraunhofer SIT has developed the CodeInspect tool. With this tool, the user can discover not only even complex vulnerabilities efficiently and precisely, but also potential malicious behavior, and obfuscations. CodeInspect features various fully automated analyses as well as a live debugger for manual investigation. Unlike any other tool, CodeInspect provides the user with a live analysis while the app is running. Since CodeInspect works directly on the compiled app, no source code is necessary.

Company employees perform more and more of their daily tasks with mobile devices. Consequently, these devices process an increasing amount of sensitive business data. Especially in areas such as external customer care, the mobile movement has greatly improved productivity. On the other hand, it has also posed new challenges on the security of the devices and the apps installed on them. Oftentimes, classic code scanning techniques are not applicable, because no source code is available for the apps. With CodeInspect, you can nevertheless analyze these binary-only apps for security vulnerabilities efficiently and precisely. Normal IT or development experience is sufficient to conduct the analysis in-house without costly external consultants or providers.

App developers often face very similar challenges. Many developers use third party libraries for which they do not have the source code. Still, they must analyze these libraries for security vulnerabilities or identify the root cause of app malfunction. With CodeInspect, you can investigate the behavior of such closed-source libraries quickly and easily.

How does CodeInspect work?

CodeInspect first translates the app's binary code into a human-readable language. Based on this language, the user can then manually investigate the app. With the integrated debugger, they can step through the app on a per-instruction basis and observe its behavior. Additionally, CodeInspect provides a variety of fully automated and innovative analyses that indicate vulnerabilities, potential malicious behavior, and obfuscations inside the app to the user. The tool automatically validates the discovered problems in order to avoid false alarms. It then assembles all results into a well-arranged report.

Plugin infrastructure

Other developers and analysts can extend and customize CodeInpect's functionality through individual plug-ins. With our data flow plug-in, for example, an analyst can easily check whether and how the app transfers sensitive data.

CodeInspect is the ideal tool for:

- IT Security Departments or Advisors
- General Software Developers
- Developers of Software Libraries
- Antivirus and Protection Tool Providers
- Security Software Providers
- App Store Operators

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