Abstract

Security and privacy of Smartphone data are critical requirements in case of both personal as well as corporate environment. Hence, there is a need to come up with an effective solution in order to address data leakage issues in smartphones. Generally, taint analysis techniques are used for information flow tracking and data leakage detection purpose. Static Taint analysis techniques can detect the leakages that may not be exposed in runtime. Static analysis derives the information about program’s behaviour by inspecting the program’s code and discovering multiple paths of a program execution. In this work a static taint analysis tool Comnoid is proposed along with companion app ApkGrabber. Comnoid is based on open source tool FlowDroid and is capable of analyzing the inter app communication. Existing version of FlowDroid tool can provide precise static taint analysis but it lacks capability to analyze inter app communication between Android applications. Thus the aim of proposed scheme is to develop a tool to perform Static Taint analysis with inter app analysis which will take Android application APK files as an input and produce a data leakage report.
References

7. Edward J. Schwartz, Thanassis Avgerinos, David Brumley, "All You Ever Wanted to Know About Dynamic Taint Analysis and Forward Symbolic Execution (but might have been afraid to ask)" SP '10 Proceedings of the 2010 IEEE Symposium on Security and Privacy, pp.317-331
9. Peter Hornyack, Seungyeop Han, Jaeyeon Jung, Stuart Schechter, and David Wetherall, "These Aren't the Droids You're Looking For", Retrofitting Android to Protect Data from Imperious Applications In Proc. of ACM CCS, October 2011
Android-based Devices”, SECRYPT, 10th International Conference on Security and Cryptography 2013

Index Terms

Computer Science  Databases

Keywords

Android Operating System; static and dynamic taint analysis; data flow analysis; Mobile Security