Abstract

The electronic devices such as a mobile have become popular day by day, which is the major target of malicious applications (malapps). The detection and removal of malicious apps from android is the major issue in now days. So keep the malapps out of the app markets is an ongoing challenge. One major design points of Android security mechanism is control the permission that restricts the access of users having responsibility to the app developers with regard to accurately specifying the requested permissions and to the users with regarding to fully understanding the risk of granting certain combinations of permission. In this report, we have studied different techniques to determine themalapps in android. In permission induced
risk first, analyse the risk of an individual permission and the risk of a group of corresponding permissions. Then used different feature ranking methods. Then use different methods to identify risky permission subsets. Secondly, then analyze the usefulness of risky permissions for malapps detection with subset selection. Thirdly, in depth analyze the detection results and determine the feasibility as well as the limitations of malapps detection based on permission requests.

References

- Wei Wang, Xing Wang, Dawei Feng, Jiqiang Liu, Zhen Han, and Xiangliang Zhang "Exploring Permission-Induced Risk in Android," in IEEE transactions on information forensics and security, no. 11, november 2014.

Index Terms

Computer Science

Security
Keywords
Android  Malapps Detection  Permission Control  Induced Risk.