

How to Tame Your Android Malware

Ivan Burke and Heloise Pieterse

Abstract:

The Android mobile market has expanded greatly in recent years, but with its increased market share Android became a popular target for malware developers. The latest Anti-Virus reports suggest that Android account for the majority of malware detected on mobile devices. This is largely due to the open nature of Android development and the level of system utilities Android software developers are given access to. This paper reviews the currently available open source solutions available, for analysing mobile malware. In this paper the authors, provide an overview of the anatomy of an Android applications. Several malware analysis tools and reverse engineering tools have been developed to analyse and deconstruct APK files. The paper presents a method by which common open source tools can be used to dissect the APK file to uncover its intent. To conclude the authors identify the current shortcomings, with regards to currently available open source software, when it comes to the classification of malicious Android applications.

Keywords: android, malware, reverse engineering, analysis, open source