Journal of Engineering Science and Technology
Special Issue on ICCSIT 2018, July (2018) 78 - 90

ANDROID MALWARE DETECTION TECHNIQUE VIA FEATURE ANALYSIS

AI PING NG, KANG LENG CHIEW *, DAYANG HANANI ABANG IBRAHIM, WEI KING TIONG, SAN NAH SZE, NADIANATRA MUSA

Faculty of Computer Science and Information Technology,
University Malaysia Sarawak, 94300 Kota Samarahan, Malaysia
*Corresponding Author: klchiew@unimas.my

Abstract

The rapidly increasing popularity of the Android platform has resulted in a significant increase in the number of malware compared to previous years. Since Android offers an open market model, it is an ideal target to launch malware attacks. Due to this problem, a lot of research work has been proposed to protect users from attacks. However, such protection cannot last long as attackers will usually find ways to defeat protection mechanism. As a result, this paper aims to develop an effective malware detection technique. The proposed method focuses on static analysis approach, which utilizes features from permissions, intents and API calls of an Android application. In order to create a sensitive and representative feature set, the proposed method also uses the correlation-based feature selection method. The final feature set will be fed into the support vector machine to perform the classification. Experimental results have shown that the proposed method achieved reliable detection accuracy at 95% and outperformed the benchmark method.

Keywords: Android, Classification, Feature extraction, Feature selection, Malware, Static analysis.