ANALISIS IMPLEMENTASI METODE KLASIFIKASI BAYES UNTUK DETEKSI MALWARE ANDROID

ANANG FAHMI RIDLO
(Pembimbing : Aisyatul Karima, S.Kom, MCS)
Teknik Informatika - S1, FIK, Universitas Dian Nuswantoro
www.dinus.ac.id
Email : 111201207092@mhs.dinus.ac.id

ABSTRAK

Dewasa ini, penggunaan perangkat mobile smartphone semakin meningkat. Salah satu mobile platform yang paling populer saat ini yaitu Android. Platform Android meningkat kepopulerannya melebihi para pesaingnya seperti iOS, Blackberry, Symbian, dan Windows mobile. Tetapi akibat kepopulerannya tersebut Android juga menjadi target yang paling diincar oleh serangan malware. Sudah banyak sekali metode yang diusulkan untuk mengatasi masalah serangan malware pada platform Android. Dari berbagai macam metode tersebut memiliki kelebihan dan kekurangannya masing-masing. Meskipun begitu malware juga berkembang seiring berjalannya waktu. Beberapa jenis malware menjadi lebih sulit untuk dideteksi. Oleh karena itu pada penelitian ini diajukan metode yang ditujukan untuk menjadi solusi bagi pendeteksian malware pada aplikasi Android secara dini. Proses klasifikasi aplikasi dilakukan dengan cara menganalisis source code dari aplikasi tersebut, oleh karena itu dibutuhkan proses reverse engineering untuk mendapatkan source code dari dataset yang berupa file APK. Penelitian dilakukan menggunakan model parameter berupa permission dan properti-properti berbasis code. Hasil penelitian menunjukkan akurasi classifier sebesar 54.0% pada model permission, 89.5% pada model properti berbasis code, dan 88.0% pada gabungan kedua model tersebut. Dari hasil tersebut dapat ditarik kesimpulan, permission kurang cocok untuk digunakan sebagai parameter klasifikasi aplikasi malware/ aman, parameter terbaik adalah properti berbasis code.

Kata Kunci : Android, Malware, Reverse Engineering, Machine Learning, Naive Bayes.

ANALYSIS OF BAYES CLASSIFICATION METHOD IMPLEMENTATION FOR ANDROID MALWARE DETECTION

ANANG FAHMI RIDLO
(Lecturer : Aisyatul Karima, S.Kom, MCS)
Bachelor of Informatics Engineering - S1, Faculty of Computer Science, DINUS University
www.dinus.ac.id
Email : 111201207092@mhs.dinus.ac.id

ABSTRACT

Today, the use of mobile devices is increasing significantly. One of the most popular mobile platforms today is the Android. The Android platform increased its popularity exceeded competitors such as iOS, Blackberry, Symbian, and Windows Mobile. But due to the popularity of Android, it has also become the most targeted mobile platform by malware attacks. Many methods have been proposed to overcome the problem of malware attacks on Android platform. Each one of them has advantages and disadvantages. Even so, the malware also evolves over time. Some types of malware are becoming more difficult to detect. Due to that reason, the author would like to propose a method that is expected to help and be a solution for early detection of malware in Android applications. Application classification process is done by analyzing the source code of the application, so it needs to do reverse engineering process to get the source code of the dataset from the form of APK file. The study was conducted using the model parameters such as permissions and code-based properties. the result of the research showed that the classifier's accuracy is 54.0% on the model permissions, 89.5% on model-based property code, and 88.0% on the combination of the two models. From these results it can be concluded, the permissions are less suitable for use as a parameter classification of malware/ secure application, the best parameter is code-based properties.

Keyword : Android, Malware, Reverse Engineering, Machine Learning, Naive Bayes.