APPLYING MACHINE LEARNING TO DETECT ANDROID MALWARE: ANDROPYTOOL AND OMNIDROID

Contents

The possibilities and advantages of applying Machine Learning to solve the most diverse problems are beyond question. It has been proved how this wide set of techniques can help to address varied issues related to computer vision, natural language processing, fraud detection, robotics or bioinformatics, among many others. In this tutorial we aim to present the possibilities of this field when dealing with a complex, current and critical problem: the detection of malware in Android devices. As we will show, Machine Learning techniques such as classification and clustering algorithms, deep learning or evolutionary computation are currently being employed to detect those malware samples whose behavior exhibits malicious patterns. Furthermore, we will explain the different tools designed for performing Android malware analysis and reverse engineering processes. Finally, we will describe in first place our framework **AndroPyTool**, aimed at extracting a wide set of features from Android applications with the goal of deeply charactering their behavior and in second place the **OmniDroid** dataset, a comprehensive dataset of features from Android benign and malicious applications.

Intended audience

Open to all audiences interested in malware detection and machine learning.

Tutorial format

Mainly practical

The 19th International Conference on Intelligent Data Engineering and Automated Learning, IDEAL 2018

21-23 November, Universidad Autónoma de Madrid, Spain

AI+DA

APPLIED INTELLIGENCE AND DATA ANALYSIS RESEARCH GROUP
Escuela Politécnica Superior, Universidad Autónoma de Madrid, 28049
+34 914972288 | aida.research@uam.es | https://aida.ii.uam.es/