Machine Learning Based Online Malware Scanner

Student Members:

Mevin G Monson
Vijay Sankar S
Vivek Prakash
Paul Thomas Sajith

Project Co-ordinator:

Dr. VINOD P
PROFESSOR
COMPUTER SCIENCE AND ENGINEERING

Globally, the number of smart phone users has risen above a billion, and most of the users use them for their day-to-day activities. Moreover, smart phones have transformed themselves into private devices holding much of personal and private information . From personal contacts information to confidential bank account details, all important data finds a place in today's smart phone. Therefore, the security of the data stored in smart phones turns out to be an issue of great concern. Being one of the most popular mobile platform, Android is prone to various kind of malicious attacks by attackers all around the world. Example attacks include disclosure of users private data (e.g..phone book and calendar entries) to remote parties that do not have direct access to such data or cannot directly establish remote connections. Users are mostly unaware of such kind of attacks. We propose a Machine Learning Based Online Scanner to detect these kind of malicious applications on Android.

Malware Scanners are implemented to classify malware against benign.We aim to collect an App set from 9apps.com and another from a malware set , and perform analysis on various features of the applications like permissions, sensitive APIs, system calls, and network trace etc. Dynamic Analysis tools like Android Monkey, Strace, Tshark can be used to extract details about system calls and network trace whereas static analysis tools like apktool and backsmali can be used to extract permissions and sensitive APIs of the applications. During the analysis a weight is assigned for each feature in the benign set as well as in the malware set depending on their occurrence in both the sets. Based on this data the features are classified using Naive Bayes

Classifier as malware and benign, so that the online scanner can use this data to classify a new application.

By implementing our mechanism to detect malware applications in the Android environment, safety of personal and private information can be achieved.