Permission-based Security Evaluation System for Android Applications

Parin Shah
Project Advisor: Dr. Leonid Reznik
Rochester Institute of Technology

Introduction

- Security of the phone majority depends on what applications the user downloads. A malicious application can cause a threat to a single device or the whole network.
- An application may try to obtain personal information from the users without their consent and one of the way of attacking the user is by android permissions.
- This project aims at analyzing malicious applications from the good ones and thus improvising the security.

Background

- Previous work was concentrated on static analysis on criteria like user-experience reviews, battery usage, number of bugs, crashes, usability, credit leakage [1].
- First dataset was obtained from an open-source dataset of malicious applications from a research carried out in Indiana university [2] and other was from the website that hosts the APK files of the applications from the store [3].

Database Preprocessing

![Preprocessing the two datasets](image)

- Permissions required are stored in the AndroidManifest.xml file. Each application has its own APK file that contains the metadata and permissions.
- Both the datasets were created from APK files of around 75-80 android applications. There are in total approximately 120 permissions that are confined by Android.

DATASET 1

- Java code was used to parse through each AndroidManifest.xml of the application and the permissions that were requested by the developer were extracted.
- Binary value was provided if the application used that particular permission or not.
- .csv files are then parsed into WEKA, which is a tool to perform classification, and the results are obtained.

DATASET 2

- Name of the application, the permissions mentioned and the threat index that is calculated and an eventual total score of each application comprised in this dataset.

Application Score = \[ a(0.2)+b(0.4)+c(0.6)+d(0.8)+e(1)+f(100) \]

- The first database showed around 81 percent correctly classified instances.
- The second database showed much better results with around 90 percent correctly classified instances.

Results

![Analysis of Dangerous Permissions](image)

- The threat score for each of the permissions used by the application is analyzed and an average of number permissions in that particular range is formulated and final percentage is obtained.

![Analysis of Non-Dangerous Permissions](image)

![Permissions with their threat index](image)

Conclusion

- Classification techniques like Naïve Bayes, J48 and Random Forest were applied on both the databases and the results from the Database 2 were better than Database 1 since it took many criteria into account.
- The figure shows the percentage evaluated from Database 2. The threshold value is 45.5%.
- The application score above the threshold value can likely be assumed as a malicious application.
- This project provides analysis of android applications based on permissions that can strengthen the security and safeguard users private data.

Acknowledgement & Contact Details

- I would like to express my gratitude to my project advisor and instructor Prof. Leon Reznik and my classmates for their feedback.
- My contact details are as follows:
  - Name: Parin Shah
  - Email ID: pss3096@rit.edu
  - Phone: (585)-770-0499

References