Jordan James
1001879608

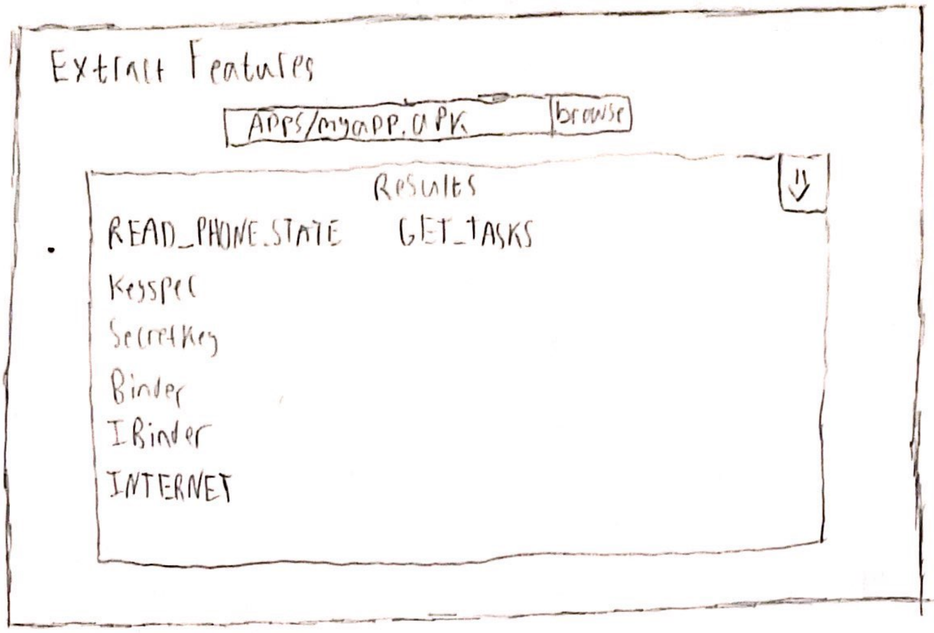
Project Proposal

The need for mobile security has been rising ever since smart phones became popular. Android is one of the most popular mobile operating systems in the world and is open source. Since the framework is open source it is much easier for hackers to create malicious apps and software that targets phones running on Android. Due to this, the need for mobile antivirus apps is at an all-time high. To help satisfy this need, I propose an Android malware detector app that can classify an Android app as either malicious or benign. The app will also give the user probability scores for the certainty of an app being malicious and benign so they can make the final decision on whether to block the app or not.

The malware detector app will have the feature to classify an Android app as malicious or benign. It will also have a feature to display probability scores for malicious and benign and allow the user to override the classification as a trusted source. Finally the Android detector app will have a feature to scan all directories for Android apps and classify each of these as malicious or benign. These features will allow the app to be competitive with other similar mobile antivirus such as Avira Antivirus Security for Android, McAfee Mobile Security Free, and BullGuard Mobile Security & Antivirus Free.

The Android malware detector app proposed will have the ability to take a single Android app as input and parse the function and system calls used in the program. Using the parsed operations of the program, the malware detector app will use Baye's theorem to determine if an app is malicious or not based on prior knowledge of malicious and benign apps. The prior knowledge for the app will come from the Kaggle dataset, Android Malware Dataset for Machine Learning, found at https://www.kaggle.com/shashwatwork/android-malware-dataset-for-machine-learning?select=drebin-215-dataset-5560malware-9476-benign.csv. This dataset contains 215 attributes of function and system calls parsed from 15,036 applications of which 5,560 are malicious applications from the Drebin project and 9,476 are benign apps.

,



Extract Features

Apps/myapp.apk browse

Results

READ_PHONE_STATE GET_TASKS

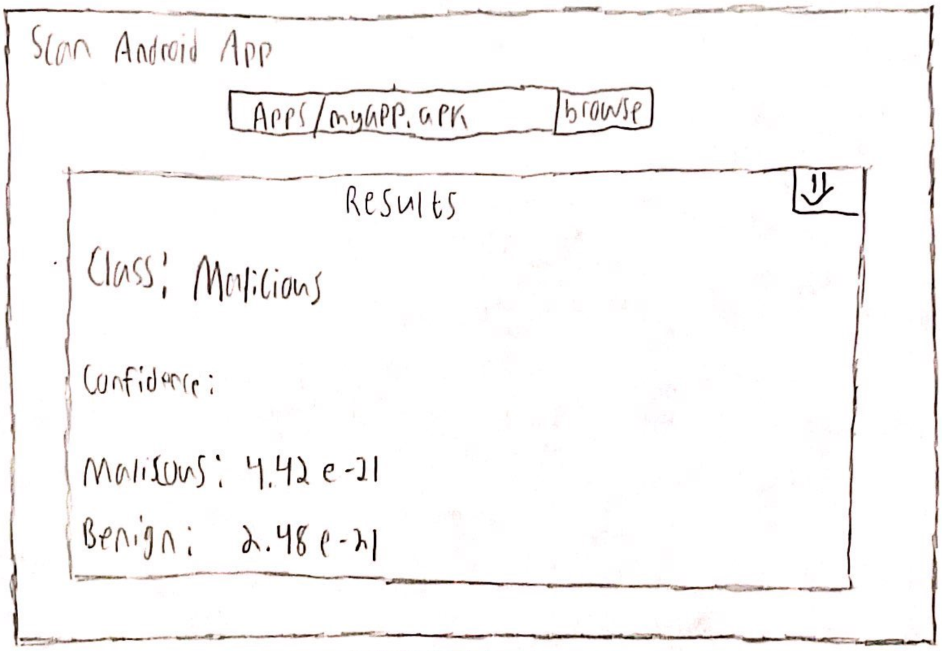
KeySpec

SecretKey

Binder

IBinder

INTERNET



Scan Android App

Apps/myapp.apk browse

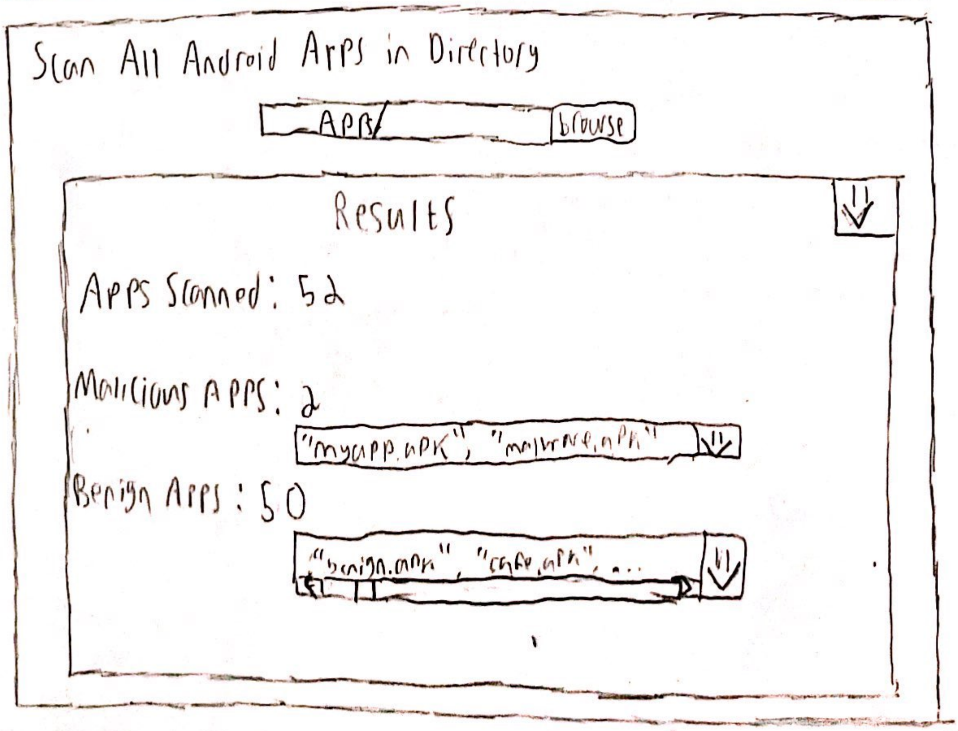
Results

Class: Malicious

Confidence:

Malisous: 4.42 e-21

Benign: 2.48 e-21



Scan All Android Apps in Directory

APPS/ browse

Results

Apps Scanned: 52

Malicious Apps: 2

"myapp.apk", "malware.apk"

Benign Apps: 50

"benign.apk", "cafe.apk", ...

Scanned with CamScanner