1. Project title, abstract, Participant names

**Title**

Android Application Permission Manager (AAPM): Educate, Inform and Protect Android Users from Malicious Apps

**Abstract**

Android applications (apps) request access to device resources and data, such as storage, GPS location, camera, microphone, SMS, phone identity, network information etc. When app permissions are required, the user will be prompted to grant them. Often, an app will not have full functionality if the user refuses to allow it to access these resources. Legitimate mobile apps, advertisements (ads) and malware all require access to mobile resources and data in order to properly function. Therefore, it is difficult for the user to make informed decisions balancing security and functionality. We have implemented the Android Application Permission Manager (AAPM) that will educate and inform users, and help prevent them from installing malicious apps. Our framework classifies apps into three risk categories using the following 5 features: (1) dangerous combinations of permissions, (2) ad networks associated with the app, (3) the number of possible privacy threats, (4) the range of permissions in the app’s category, and (5) over-privileged app permissions. The features are extracted by analyzing 1625 top free/paid apps from Google Play, the official Android market. We tested several classifier models such as k-NN, Classification Tree, Random Forest, Naive Bayes and SVM. The accuracy of these classifiers is considerably high using our dataset of 1823 apps, including 198 top malicious apps. We decided to implement SVM for our framework based on the performance, which exceeded 93.5% classification accuracy, and its suitability for our data.

**Participants**

Katherine Schwartz (undergraduate student) and Eralda Caushaj (graduate student)

Advisor: Dr. Huirong Fu

2. Papers, status of papers, products

**Paper**: Android Application Permission Manager (AAPM): Educate, Inform and Empower Android Users from Malicious Apps

**Status**: To be submitted for publication after some minor revisions

**Products**: Android Application Permission Manager (AAPM) app, which is near completion

3. Findings

* Malicious applications (apps) and invasive advertisement (ad) networks pose a threat to the security and privacy of users of the Android mobile operating system.
* Average Android users are not provided with adequate tools to determine whether the apps on their devices misuse their personal information.
* Certain features of an app, including number of permissions vs. the category average and number of ad networks among others, can be used to determine how dangerous the app is to a user’s security and privacy.

4. Contributions:

a.. within Discipline

We have developed a security framework (AAPM) that utilizes a Support Vector Machine (SVM) machine learning algorithm to classify how much risk is posed by Android applications. We use a set of five features as input to the SVM. These five features were selected by examining the properties of a large dataset of over 1200 popular apps and 99 mobile malwares. The SVM was trained with a labelled set that we assembled consisting of 1625 safe and benign apps and 198 malicious apps. It achieved a classification accuracy of over 93.5% when tested using 10-fold cross validation.

b.. to Other Disciplines

The features we have identified as dangerous could serve as a guide to software developers. Those developing for the Android platform could take factors such as the invasiveness of ad networks they are considering and the types of permissions they request into consideration when developing an app, in order to best protect the privacy and security of their users.

c. to Human Resource Development

The app we have developed allows the average user to become more informed about the risks posed by mobile malware. Informed users are more likely to make responsible decisions regarding their personal data privacy and the data privacy of their organization.

d.. Beyond Science and Engineering

The app that we have developed is designed with the average Android user in mind. Many people use the Android operating system, and very few of these users have the necessary background to correctly asses the risks posed by apps. Our app will allow users without a background in computing to make informed decisions regarding their security and privacy.

5. Training and Development for the students

The project I worked on focused on Android security. I learned how the Android system is structured and how applications and malware operate. I dove deep into the subject of Android security, learning the advantages and disadvantages of current approaches. I then participated in the creation of a novel solution. When we decided to implement machine learning, I researched and tested many different machine learning models. I studied the mathematics behind them and their strengths and weaknesses. I then contributed to the decision to use an SVM. Though I did not have any prior experience with Android security or machine learning, I am now confident in my expertise in both fields.