**Generating Summary Risk Scores for Mobile Applications**

**ABSTRACT:**

One of Android’s main defense mechanisms against malicious apps is a risk communication mechanism which, before a user installs an app, warns the user about the permissions the app requires, trusting that the user will make the right decision. This approach has been shown to be ineffective as it presents the risk information of each app in a “stand-alone” fashion and in a way that requires too much technical knowledge and time to distill useful information. We discuss the desired properties of risk signals and relative risk scores for Android apps in order to generate another metric that users can utilize when choosing apps. We present a wide range of techniques to generate both risk signals and risk scores that are based on heuristics as well as principled machine learning techniques. Experimental results conducted using real-world data sets show that these methods can effectively identify malware as very risky, are simple to understand, and easy to use.

**EXISTING SYSTEM:**

Android’s main defense mechanisms against malicious apps is a risk communication mechanism which warns the user about the permissions an app requires before the app is installed by the user, trusting that the user will make the right decision. The specific approach used in Android has been shown to be ineffective at informing users about potential risks. The majority of Android apps request multiple permissions. When a user sees what appears to be the same warning message for almost every app.

**DISADVANTAGES OF EXISTING SYSTEM:**

* Risk warnings quickly lose any effectiveness as the users are conditioned to ignore such warnings.
* Used static analysis to determine whether an Android application is over privileged
* The permission system is complex

**PROPOSED SYSTEM:**

In this paper, we investigate permission-based risk signals that use the rarity of critical permissions and pairs of critical permissions. In this approach, initially reported in permissions that have significant security or privacy impact are identified as critical, and if an app requests a critical permission (or a pair of critical permissions) that is rarely requested by apps in the same category as the app, the app is labelled as risky. Using a binary risk signal, i.e., labelling each app as either risky or not risky.

**ADVANTAGES OF PROPOSED SYSTEM:**

* The idea of risk score functions to improve risk communication for Android apps, and identify three desiderata for an effective risk scoring function.
* We introduce a framework that includes both therarity based risk signals and probabilistic models, and explore other ways to instantiate the framework.

**SYSTEM REQUIREMENTS:**

**HARDWARE REQUIREMENTS:**

* System : Pentium IV 2.4 GHz.
* Hard Disk : 40 GB.
* Floppy Drive : 1.44 Mb.
* Monitor : 15 VGA Colour.
* Mouse : Logitech.
* Ram : 512 Mb.
* MOBILE : ANDROID

**SOFTWARE REQUIREMENTS:**

* Operating system : Windows XP/7.
* Coding Language : Java 1.7
* Tool Kit : Android 2.3 ABOVE
* IDE : Eclipse

**REFERENCE:**

Christopher S. Gates, Ninghui Li, Senior Member, IEEE, Hao Peng, Bhaskar Sarma, Yuan Qi, Rahul Potharaju, Cristina Nita-Rotaru, Member, IEEE Computer Society, and Ian Molloy“Generating Summary Risk Scores for Mobile Applications” **IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING,VOL. 11,NO. 3, MAY-JUNE 2014.**