SEARCH RANK FRAUD AND MALWARE DETECTION IN GOOGLE PLAY

Abstract

The commercial success of Android app markets such as Google Play and the incentive model they offer to popular apps, make them appealing targets for false and malicious behaviors. Some fraudulent developers deceptively boost the search rank and popularity of their apps (e.g., through fake reviews and bogus installation counts), while malicious developers use app markets as a launch pad for their malware.

Existing system:

The efforts of Android markets to identify and remove malware are not always successful. For instance, Google Play uses the Bouncer system to remove malware. Previous mobile malware detection work has focused on dynamic analysis of app executables as well as static analysis of code and permissions. However, recent Android malware analysis revealed that malware evolves quickly to bypass anti-virus tools.

Disadvantages:

- Can't detect genuine reviews
- Can't identify fraud users and malware indicators.
- Time taking process with executing app and analysis of code permission methods

Proposed System:

In this, we introduce FairPlay, a novel system that discovers and leverages traces left behind by fraudsters, to detect both malware and apps subjected to search rank fraud. FairPlay correlates review activities and uniquely combines detected review relations with syntactical and behavioral signals gleaned from Google Play app data, in order to identify doubtful apps. FairPlay achieves over 95% accuracy in classifying gold standard datasets of malware, fraudulent and rightful apps. We show that 75% of the identified malware apps engage in search rank fraud. FairPlay discovers hundreds of fraudulent apps that currently evade Google Bouncer's detection technology. FairPlay also helped the discovery of more than 1,000 reviews, reported for 193 apps that reveal a new type of forceful review operation. We uncover these

malicious acts by picking out such trails. For instance, the high cost of setting up valid Google Play accounts forces fraudsters to reuse their accounts across review writing jobs, making them likely to review more apps in common than regular users. Resource constraints can compel fraudsters to post reviews within short time intervals.

Advantages:

- Can detect genuine reviews
- Can identify fraud users and malware indicators.
- Identifies forceful reviews operation.

System Configuration

Hardware Configuration:-

- ✓ Processor - Pentium –IV
- ✓ Speed - 1.1 Ghz
- ✓ RAM - 256 MB(min)
- ✓ Hard Disk - 20 GB
- ✓ Key Board - Standard Windows Keyboard
- ✓ Mouse - Two or Three Button Mouse
- ✓ Monitor - SVGA

Software Configuration:-

- ✓ Operating System : Windows XP
- ✓ Programming Language : JAVA
- ✓ Java Version : JDK 1.6 & above.

- ✓ Back end :MY SQL