**Search Rank Fraud and Malware Detection in Google Play**

**ABSTRACT:**

Fraudulent behaviors in Google Play, the most popular Android app market, fuel search rank abuse and malware proliferation. To identify malware, previous work has focused on app executable and permission analysis. In this paper, we introduce Fair Play, a novel system that discovers and leverages traces left behind by fraudsters, to detect both malware and apps subjected to search rank fraud. Fair Play correlates review activities and uniquely combines detected review relations with linguistic and behavioral signals gleaned from Google Play app data (87K apps, 2.9M reviews, and 2.4M reviewers, collected over half a year), in order to identify suspicious apps. Fair Play achieves over 95% accuracy in classifying gold standard datasets of malware, fraudulent and legitimate apps. We show that 75% of the identified malware apps engage in search rank fraud. Fair Play discovers hundreds of fraudulent apps that currently evade Google Bouncer’s detection technology. Fair Play also helped the discovery of more than 1,000reviews, reported for 193 apps, that reveal a new type of “coercive” review campaign: users are harassed into writing positive reviews, and install and review other apps.

**EXISTING SYSTEM:**

Google Play uses the Bouncer system to remove malware. However, out of the 7, 756 Google Play apps we analyzed using Virus Total, 12% (948) were flagged by at least one anti-virus tool and 2% (150) were identified as malware by at least 10 tools.

Sarma et al. use risk signals extracted from app permissions, e.g., rare critical permissions (RCP) and rare pairs of critical permissions (RPCP), to train SVM and inform users of the risks vs. benefits tradeoffs of apps.

Peng et al. propose a score to measure the risk of apps, based on probabilistic generative models such as Naive Bayes.

Yerima et al. also use features extracted from app permissions, API calls and commands extracted from the app executables.

**DISADVANTAGES OF EXISTING SYSTEM:**

Previous work has focused on app executable and permission analysis only.

Not Efficient

Lower percentage of detection rate

Takes more time.

**PROPOSED SYSTEM:**

We propose Fair Play, a system that leverages to efficiently detect Google Play fraud and malware. Our major contributions are:

To detect fraud and malware, we propose and generate relational, behavioral and linguistic features, that we use to train supervised learning algorithms

We formulate the notion of co-review graphs to model reviewing relations between users.

We develop PCF, an efficient algorithm to identify temporally constrained, co-review pseudo-cliques — formed by reviewers with substantially overlapping co-reviewing activities across short time windows.

We use temporal dimensions of review post times to identify suspicious review spikes received by apps; we show that to compensate for a negative review, for an app that has rating R, a fraudster needs to post at least positive reviews. We also identify apps with “unbalanced” review, rating and install counts, as well as apps with permission request ramps.

We use linguistic and behavioral information to (i) detect genuine reviews from which we then (ii) extract user-identified fraud and malware indicators.

**ADVANTAGES OF PROPOSED SYSTEM:**

We build this work on the observation that fraudulent and malicious behaviors leave behind telltale signs on app markets.

Fair Play achieves over 97% accuracy in classifying fraudulent and benign apps, and over 95% accuracy in classifying malware and benign apps.

Fair Play significantly outperforms the malware indicators of Sarma et al. Furthermore, we show that malware often engages in search rank fraud as well: When trained on fraudulent and benign apps, Fair Play flagged as fraudulent more than 75% of the gold standard malware apps

Fair Play discovers hundreds of fraudulent apps.

Fair Play also enabled us to discover a novel, coercive review campaign attack type, where app users are harassed into writing a positive review for the app, and install and review other apps

**HARDWARE REQUIREMENTS:**

System : Pentium Dual Core.

Hard Disk : 120 GB.

Monitor : 15’’ LED

Input Devices : Keyboard, Mouse

Ram :

**SOFTWARE REQUIREMENTS:**

Operating system : Windows 7.

Coding Language : NET,C#.NET

Tool : Visual Studio 2008

Database : SQL SERVER 2005