FairPlay: Fraud and Malware Detection in Google Play

Daniel Perez

創造情報専攻

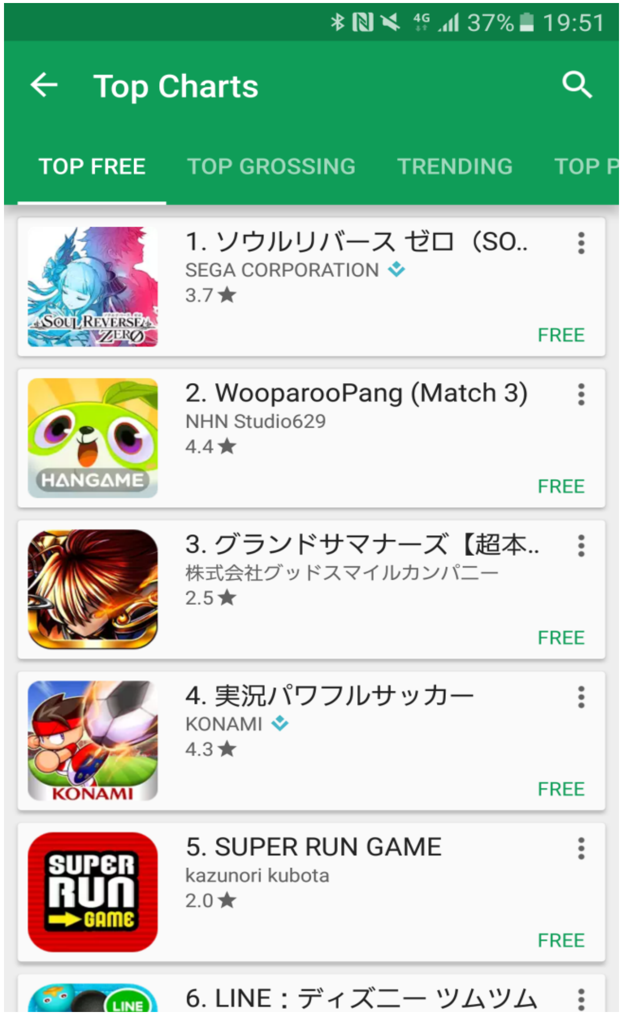
48-146619

Table of content

- Background
- FairPlay fraud detection systems
  - Overview
  - Training data
  - Modules presentation
  - Evaluation
- Summary

About Google Play

- Android official app market place
- One of the biggest app market place
- 30000+ new apps every month
- Plenty of malwares not detected



37% 19:51

Top Charts

TOP FREE TOP GROSSING TRENDING TOP P

1. ソウルリバース ゼロ（SO..
SEGA CORPORATION
3.7★
FREE

2. WooparooPang (Match 3)
NHN Studio629
4.4★
FREE

3. グランドサマナーズ【超本..
株式会社グッドスマイルカンパニー
2.5★
FREE

4. 実況パワフルサッカー
KONAMI
4.3★
FREE

5. SUPER RUN GAME
kazunori kubota
2.0★
FREE

6. LINE：ディズニー ツムツム

Android malwares

- Common types of malwares
  - Information collection
    - GPS tracking
    - Stealing contact information
    - Stealing banking info
  - Advertisement
    - Showing undesirable commercial ads
    - Sending ads to contacts
    - Posting ads on social networks

Malware detection approaches

- Static analysis
  - Analyze application permissions
  - Analyze the program source code
- Dynamic analysis
  - Check app CPU usage, packet sent, etc

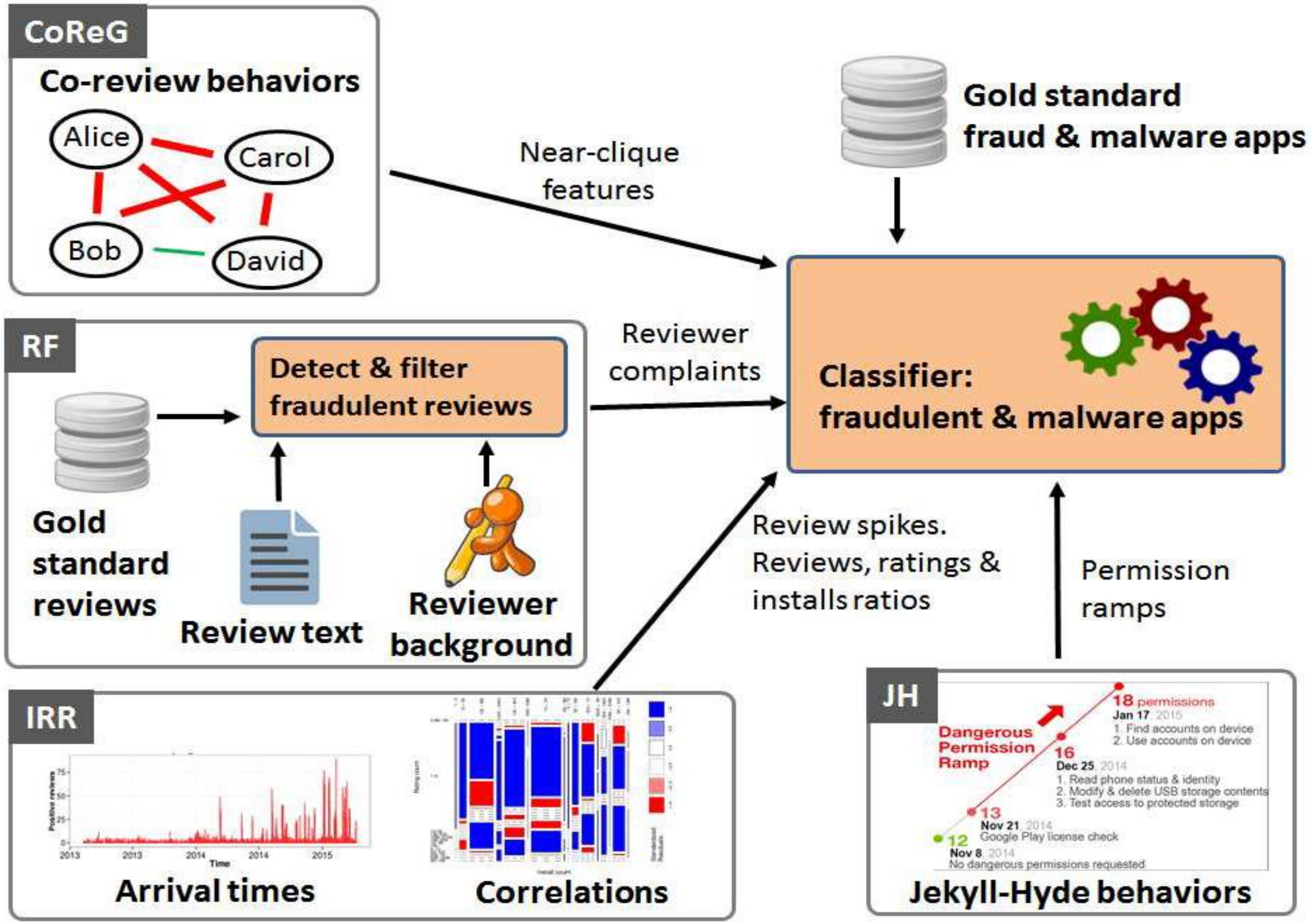
Android apps promotion

- Android search rank is based on many metrics
  - Users reviews
  - Number of downloads
  - Usage frequency
- Malware developers use search rank fraud
  - Fake reviews
  - Fake downloads and installs
  - Force users to write reviews

Proposed approach

- Detecting malwares through Google Play ecosystem
  - Co-review behaviors
  - Reviews text
  - Relationship between reviews and installs count
  - App permissions evolution

Approach overview



CoReG

Co-review behaviors

Alice

Carol

Bob

David

Near-clique features

Gold standard fraud & malware apps

RF

Detect & filter fraudulent reviews

Gold standard reviews

Review text

Reviewer background

Reviewer complaints

Classifier: fraudulent & malware apps

Review spikes. Reviews, ratings & installs ratios

Permission ramps

IRR

Arrival times

Correlations

JH

Jekyll-Hyde behaviors

Positive reviews
2013
2013
2014
2014
2015
Time
Dangerous Permission Ramp
18 permissions
Jan 17 2015
1. Find accounts on device
2. Use accounts on device
16
Dec 25 2014
1. Read phone status & identity
2. Modify & delete USB storage contents
3. Test access to protected storage
13
Nov 21 2014
Google Play license check
12
Nov 8 2014
No dangerous permissions requested

Apps data

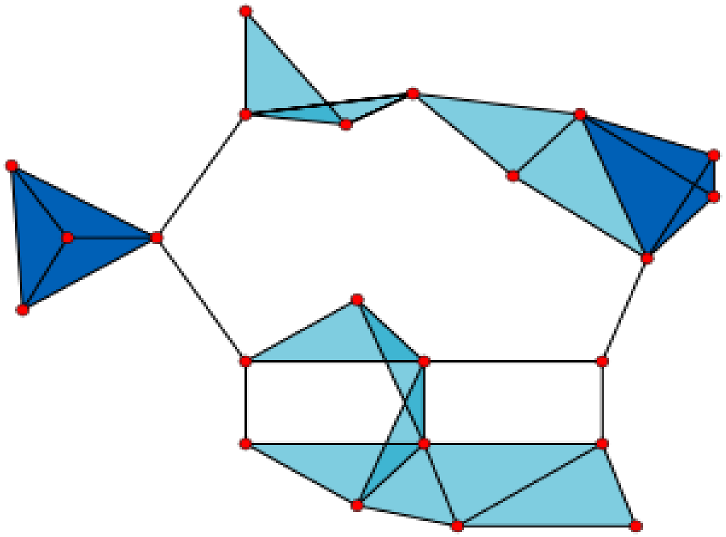
- Malware and fraudulent apps (from randomly selected 7756 apps)
  - 212 malware apps: detected as malware by 3+ tools with 10+ reviews
  - 201 fraudulent apps: apps reviewed by 15 fraudulent accounts (found by other research)
- Benign apps
  - Selected 925 apps from “top developers”
  - Chose 200 apps with 10+ reviews not flagged by any antivirus

Reviews data

- Fraudulent reviews
  - Collected 53625 reviews from 201 fraudulent apps
  - Found 188 accounts which reviewed at least 10/201 fraudulent apps, total of 6488 reviews
  - Used reviews from fraudulent accounts and above reviews
- Benign reviews
  - Manually chose 315 reviews with at least 150 characters from popular apps reviews

Graph reminder

- A complete graph is a graph where all vertices are connected
- A clique is a subset of vertices where the induced subgraph is complete



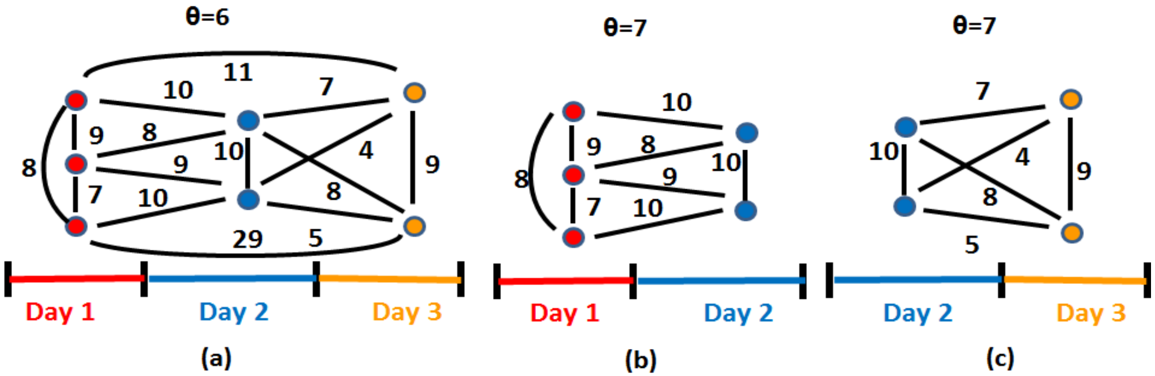
Co-Review Graph

- Undirected weighted graph
  - Vertices: users who reviewed the app
  - Edges: number of apps reviewed in common
- Identifying clique is NP-hard
  - Identify pseudo-cliques instead
  - Pseudo-cliques are identified greedily per-day
  - Pseudo-clique have a density θ greater than

$$\rho = \frac{\sum_{e \in E} w(e)}{\binom{n}{2}}$$

Co-Review Graph features

- Following features are extracted
  - Number of cliques with $\rho > \theta$
  - Maximum, median, SD of densities in pseudo-cliques
  - Maximum, median, SD of pseudo-clique sizes
  - Number of nodes that belong to at least 1 pseudo-clique



(a) (b) (c)

Reviewer feedback

1. Detect and filter fraudulent reviews
   - Reviewer based features
   - Text based features

2. Identify malware from remaining reviews
   - Reviews should be balanced
   - Review sentiment and rating should be related

Reviewer feedback features

- Following features are extracted
  - % of reviews with malware indicators
  - % of reviews with fraud words
  - % of reviews with benign words
  - Fraud review impact on rating

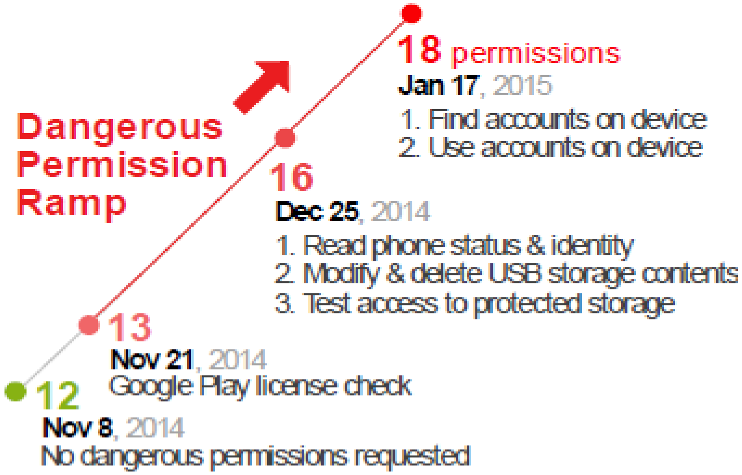
Inter-Review Relation

- Temporal relation between modules
  - Detect days with spikes of positive reviews
  - Detect amplitude of the spikes
- Relation between review, rating and install counts
  - Installations count / ratings count
  - Installations count / reviews count

Jekyll-Hyde App detection

Apps gradually asking for more dangerous permissions

- Extracted features
  - # of permissions
  - # of dangerous permissions
  - # of dangerous permission ramps
  - # of dangerous permissions added


Dangerous Permission Ramp
18 permissions
Jan 17, 2015
1. Find accounts on device
2. Use accounts on device
16
Dec 25, 2014
1. Read phone status & identity
2. Modify & delete USB storage contents
3. Test access to protected storage
13
Nov 21, 2014
Google Play license check
12
Nov 8, 2014
No dangerous permissions requested

Evaluation

- Evaluated with three algorithms
  - Decision tree
  - Multi-layer perceptron
  - Random Forest
- Evaluated for
  - Classifying reviews
  - Classifying fraudulent apps
  - Classifying malwares

Experimental results

Review classification results

Strategy	FPR%	FNR%	Accuracy%
Decision Tree (DT)	2.46	6.03	95.98
Multi-layer Perceptron (MLP)	**1.47**	6.67	96.26
Random Forest (RF)	2.46	5.40	96.26

Malware classification results

Strategy	FPR%	FNR%	Accuracy%
FairPlay/DT	4.02	4.25	95.86
FairPlay/MLP	4.52	4.72	95.37
FairPlay/RF	**1.51**	6.13	96.11
Sarma et al. / SVM	65.32	24.47	55.23

Generalization to new apps

1. Train FairPlay with Random Forest
2. Select 1600 apps with 10+ reviews from 8 categories
3. Collect data for reviewers and their reviews

➡ 372 apps (23%) were fraudulent

- 71% of apps have > 3 pseudo cliques with $\theta \geq 3$
- Fraudulent apps had at least 20 fraud indicator words

Coercive Campaign Apps

- New type of attack detected: harassing user to either
  - Write a positive review for the app
  - Install another app
  - Write a positive review for another app

Summary

- FairPlay uses Google play ecosystem to detect fraudulent apps and malwares
- A lot of malwares are involved in search rank fraud
- Both malware and search rank fraud can be identified with high accuracy