

SaTC: CORE: Small: Deconstructing and Neutralizing Search Rank Fraud

PIs: Bogdan Carbunar, FIU

<https://users.cs.fiu.edu/~carbunar/caspr.lab/socialfraud.html>

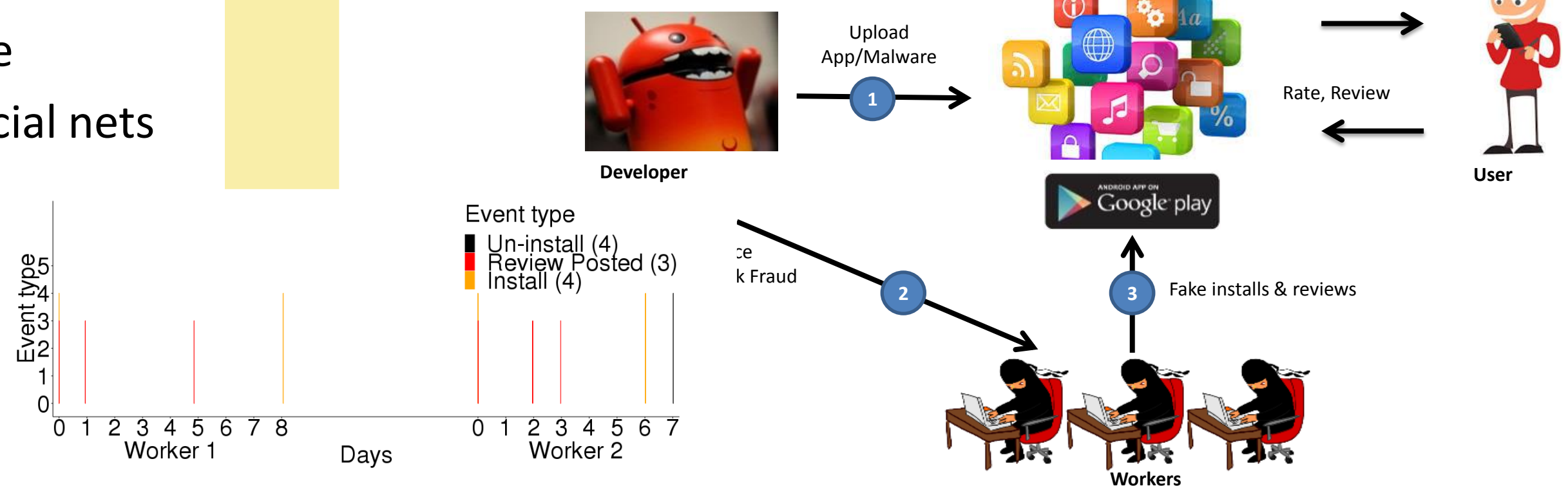


Objective: Understand strategies of influence operation participants

Search Rank Fraud and Its Impact

- Fraud workers hired to promote products online
- Peer-opinion systems (Google, Amazon) and social nets (Facebook, Twitter)
- Top 10 VPN apps on Google Play likely censored

System & Adversary Model



The Problem: (Mis)Understanding Fraud

- ❑ Detection based on ASO worker assumptions:
 1. Control many accounts
 2. Post fake reviews in bursts
 3. Exhibit lockstep behaviors
 - ...
- ❑ Organic ASO workers break assumptions

Scientific Impact

- Develop relevant fraud defenses:
 - Protect against real adversaries
- Investigate influence operations

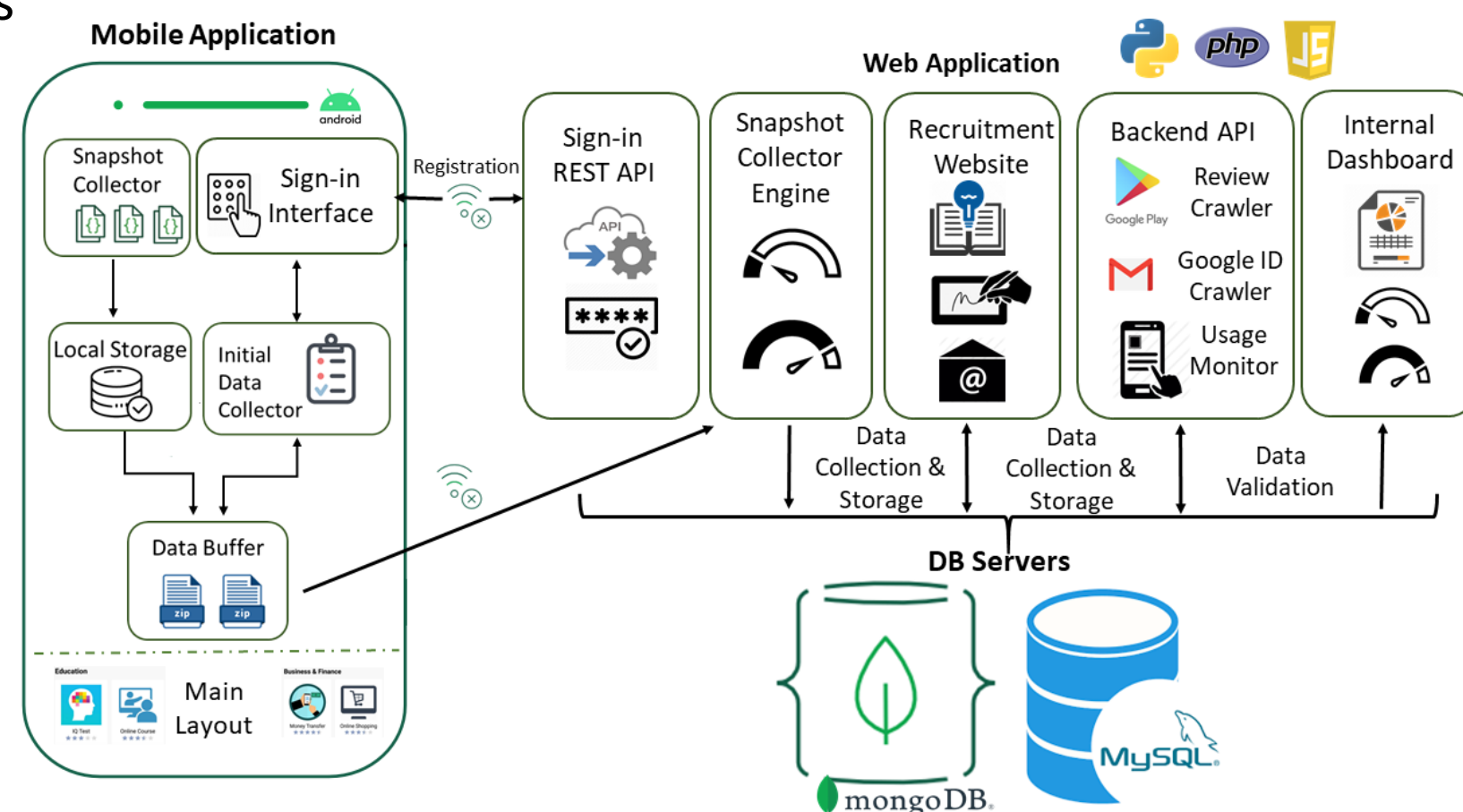
Approach

- ❑ Worker recruitment
 - ❑ 672 installs from 587 ASO workers (Facebook groups)
- ❑ Regular user recruitment:
 - ❑ 233 installs (Instagram Ads)
- ❑ 12,341 installed apps; 10,310 Gmail accounts
- ❑ 110 million reviews

Data collected:

- Registered accounts
- (Other) Installed apps; app install and uninstall events
- Foreground app

RacketStore



Previously available only to app market providers (Google, Apple)

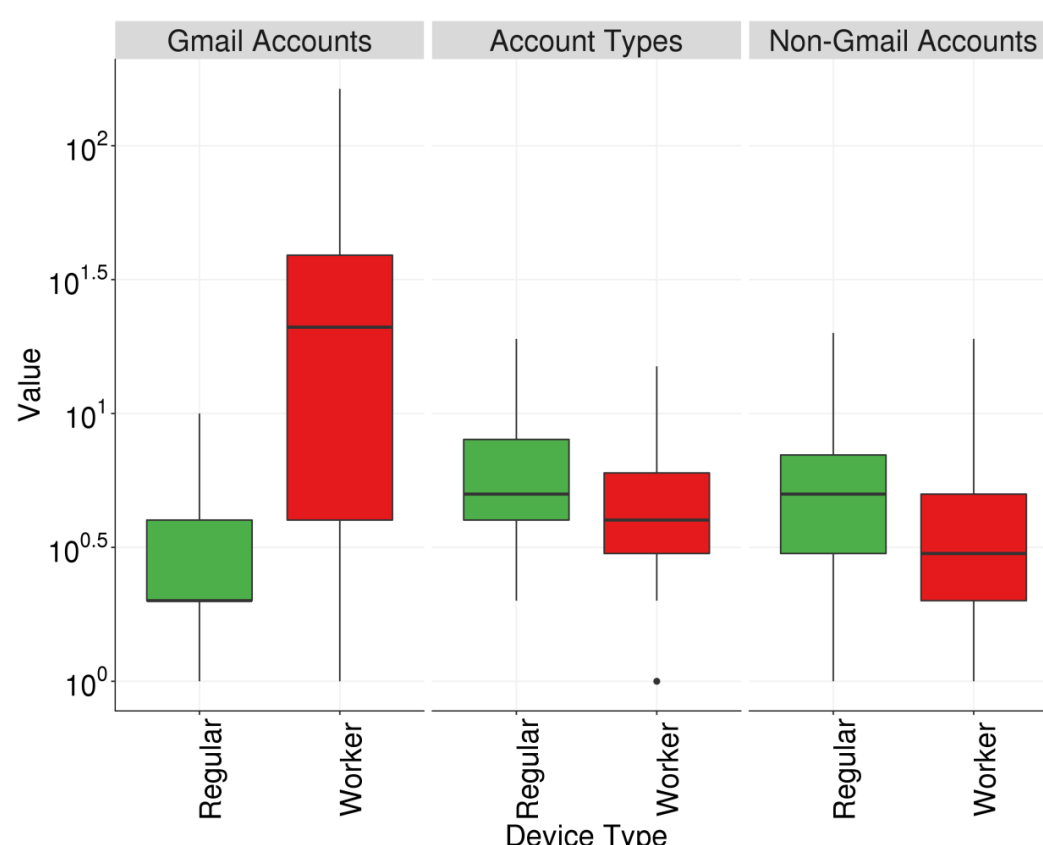
- ❑ Workers and regular people differ in their use of devices
 - ❑ Registered accounts, stopped apps, ...
 - ❑ Device usage can identify worker-controlled devices
 - ❑ Including workers with low ASO-work

Apps Installed and Reviewed



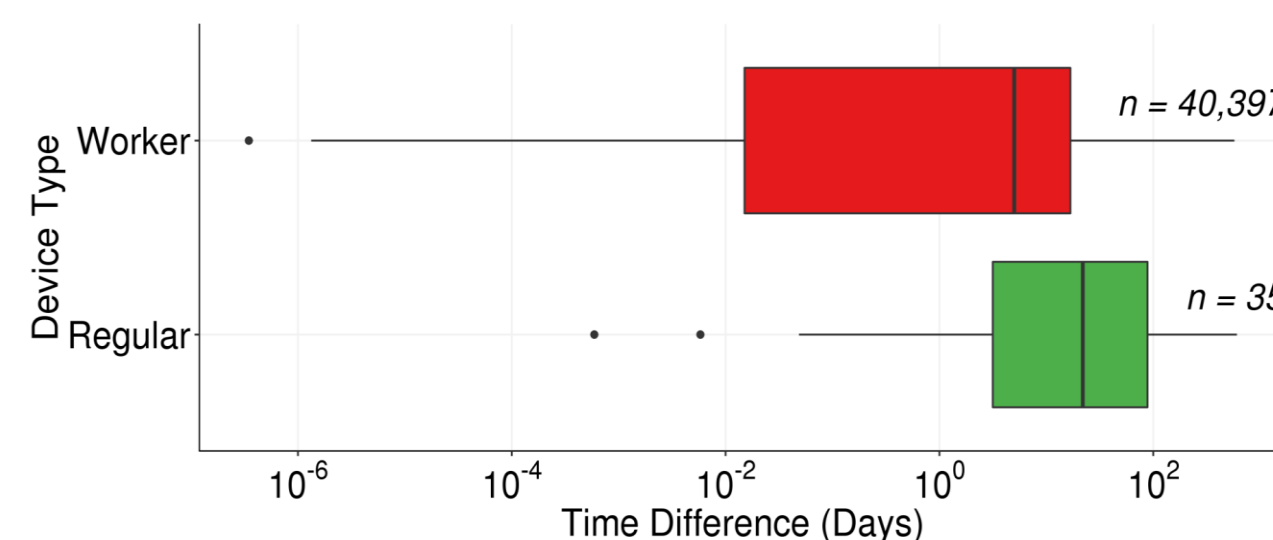
Workers write more reviews
208.91 vs. 1.91

Summary of Results: Accounts



Workers register more accounts:
28.87 vs. 2.87

Install-to-Review Time



- ❑ Regular users take longer to post reviews
- ❑ 85.09 vs 10.4 days
- ❑ Workers review apps soon after install

App Classification: Is App Usage Suspicious

- ❑ Features:
 - ❑ Install-to-review time
 - ❑ Number of device-registered accounts used to review the app
 - ❑ Daily app usage
 - ❑ Number of installs

ML Algorithm	Precision	Recall	F1
XGB	99.78%	99.67%	99.72%
RF	99.33%	99.23%	99.27%
LR	99.22%	99.00%	99.11%
KNN	96.88%	96.88%	96.88%
LVQ	90.99%	94.54%	92.73%

Device Classification Worker vs. Regular

- ❑ Features:
 - ❑ App suspiciousness:
 - ❑ Stopped apps
 - ❑ Number of registered accounts
 - ❑ Total reviewed apps

ML Algorithm	Precision	Recall	F1
XGB	96.81%	93.81%	95.29%
RF	93.95%	96.06%	94.99%
SVM	96.64%	89.03%	92.68%
KNN	94.29%	90.58%	92.40%
LVQ	96.40%	82.84%	89.11%

