EAGER: An Open Mobile App Platform to Support Research on Fraudulent Reviews

PIs: Bogdan Carbunar, FIU

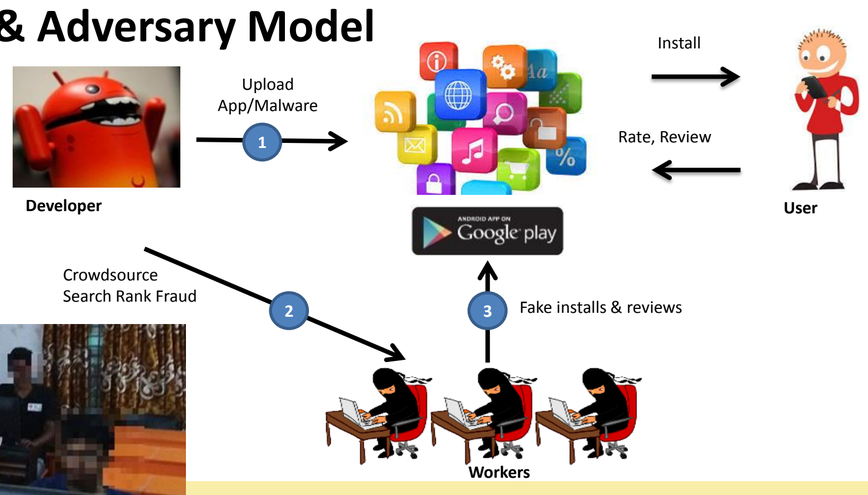
https://users.cs.fiu.edu/~carbunar/caspr.lab/socialfraud.html

Objective: **Understand fraud worker constraints and strategies**

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 censor-controlled

System & Adversary Model



Challenges

1. Fraud originates from diverse human workers and organizations
2. Lack of ground truth fraud and honest behavior data
3. No platform to evaluate developed solutions with live workers
4. State-of-the-art unable to curb **organized** online fraud

Photo reproduced with participant permission

Scientific Impact

- Develop relevant fraud defenses:
  - Protect against real (not assumed) adversaries
- Evaluate defenses online, with real adversaries
- Enable investigations into political trolls

Approach

- Structured interview study
  - 18 Black Hat App Search Optimization (ASO) workers
  - recruited from 5 freelancing sites
  - 118 questions about fraud they post on Google Play
- Quantitative investigation
  - 39 other ASO workers recruited from the same sites.
  - 1,164 Google Play accounts they revealed to control
  - 21,767 fake reviews posted from them, for 6,362 unique apps

Summary of Results: Organization

- Physical vs. online teams vs. **organic fraud**
- Software for team formation, communication, job automation

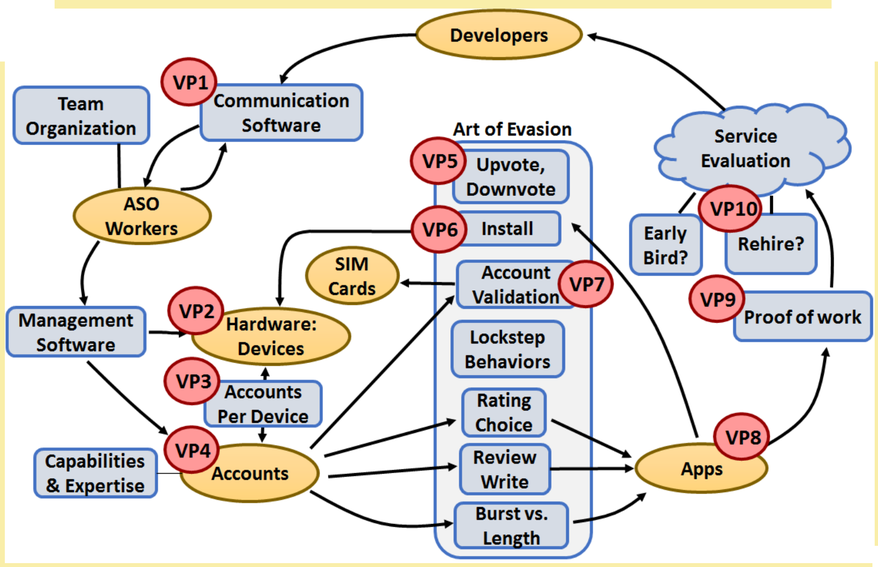
Fraud workers have evolved to
- Have access to substantial resources
- Avoid detection
- Leverage Google defenses for fraud

Myth busts:
- Some workers avoid review spikes
- Some workers avoid lockstep behaviors
- Fraud from singleton accounts, sticks
- Long reviews feel fake

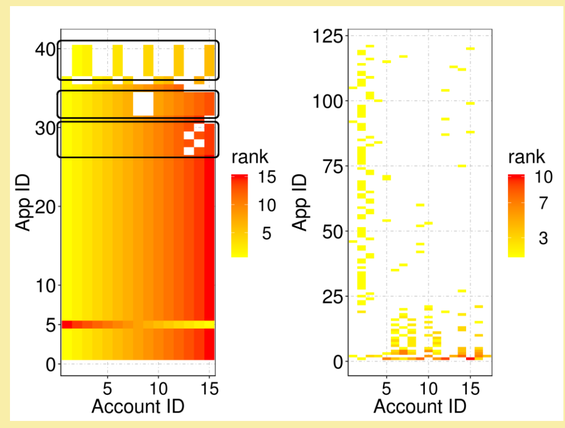
  Not all ratings are positive

Resources

Professional raters have access to
- Up to tens of thousands of accounts and devices
- Diverse device types
- Strategies to multiply SIM cards

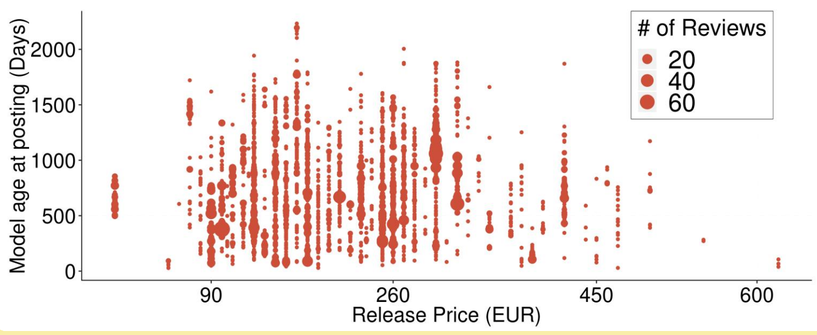


Map of Fraud

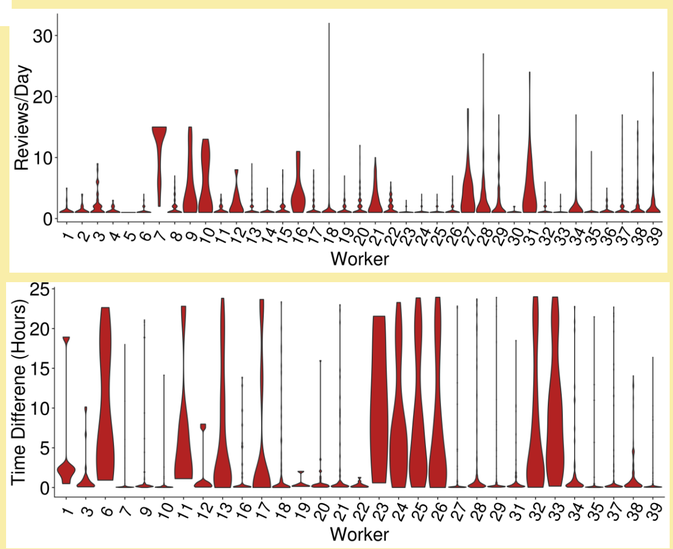


Device Types

Vulnerability in Google Play
- Query Google to find device type
- **Google Bug hunter hall of fame**



Evade detection
- Validate user accounts even without SIMs
- Reviews without installs, app interaction
- Upvote and downvote
- Singleton accounts – more expensive
- Noisy reviews, account blending
- VPN, emulator use



CaSPRLab
Cyber Security and Privacy Research

Award ID#: **1840714**