Understanding iOS-based Crowdturfing Through Hidden UI Analysis

이연준 교수님

진로

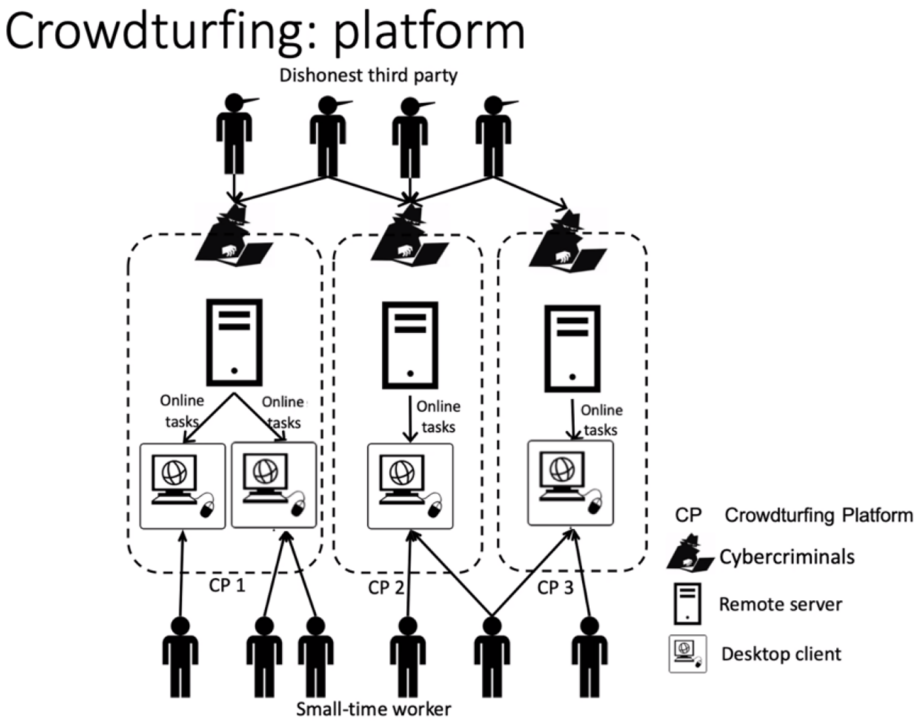
- **최대한 많이 지원**
  - 면접을 보면서 면접 실력 향상
  - 인적성을 보면서 인적성 실력 향상
- **최선을 다해서 정보수집** – 생각보다 좋은 회사가 많음
  - 네이버, 엔씨소프트, 삼성전자, 카카오 등
  - 코리아크레딧뷰로, NICE 신용평가, 코리안리, XX보험협회, 코스콤, 금융결제원 등 수 많은 기업이 있음

조사 많이 할 것

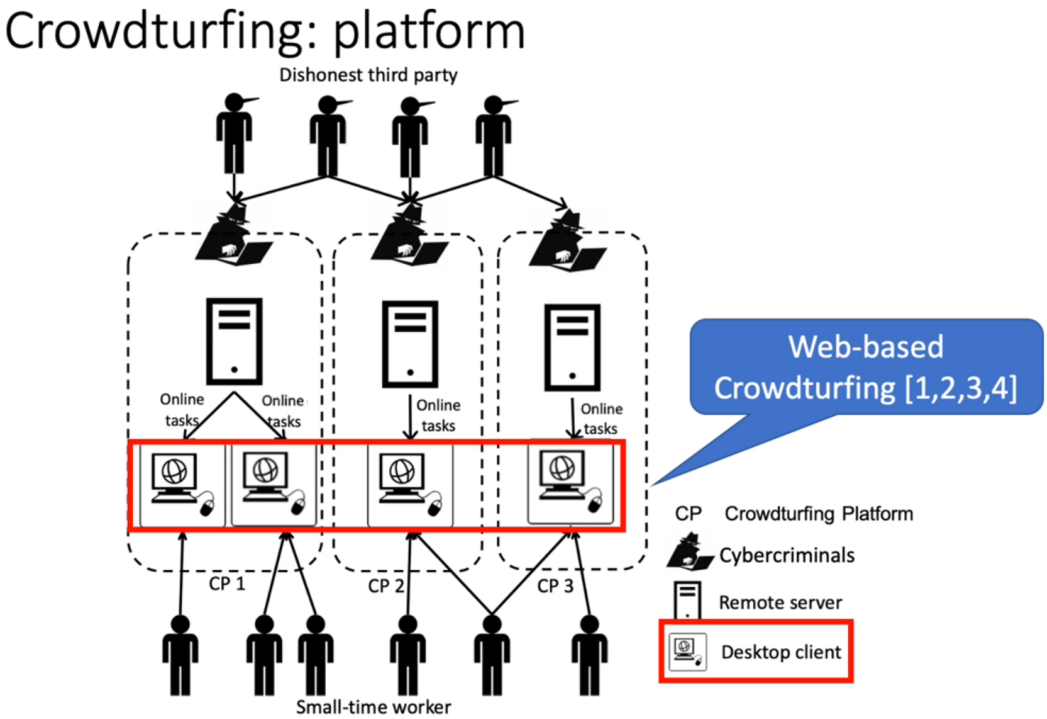
Crowdturfing: definition

- **Crowdturfing**: malicious crowdsourcing
  - It is an illicit business model, in which *Cybercriminals* recruit *small-time workers* to carry out *malicious tasks* for *dishonest third parties*.

- Crowdturfing : 악성 crowdsourcing(내부 x, 외부에게 outsourcing하는 것 ex. 아마존) 대중(small-time workers)에게 참여를 유도해서 불법적인 일을 행동
- Crowdsourcing : 대중 + 아웃소싱 합친말, 외부에게 문제 해결을 아웃소싱 하는 것



- Crowdturfing platform
- Dishonest third party 가 불법적인 의뢰 -> task단위로 쪼개서 small-time worker에게 push. -> push 된 task들에 기여.



- 모바일 crodturfing이 왜 중요한 문제인가
- 모바일 트래픽 증가

- 웹은 테스크를 웹사이트를 통하지만 모바일은 앱을 통해서 함
- 즉 앱이 설치가 되어있어야 한다는 것

Goal

- A triage methodology to identify crowdturfing apps.
- Understanding of the mobile crowdturfing ecosystem.

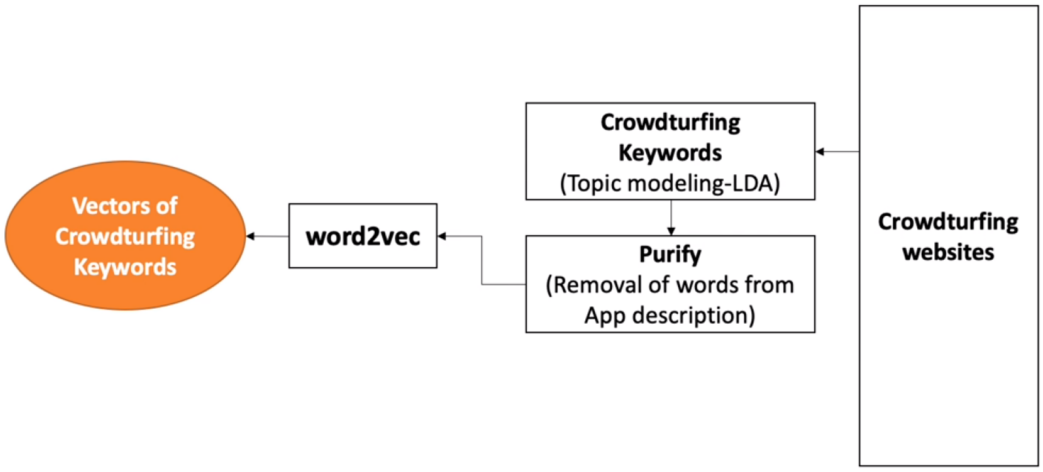
- 연구의 목적 : crowdturfing 앱을 identify 하기
- mobile ecosystem을 이해하는 것

Challenges in detecting such apps

- Crowdturfing UI are **hidden inside benign apps** and only get triggered when specific conditions are met.
- Their functionalities are **similar to legitimate apps**, without malware downloading or usage of private API.
- To detect such apps, human needs to read the content and understand its semantics.
  → not scalable during app vetting.

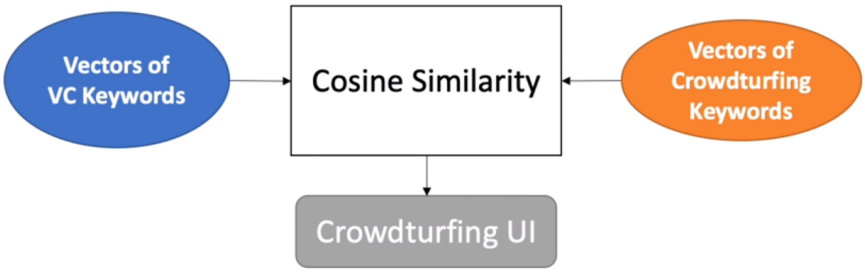
- 악성 코드 탐지하는 방법론으로는 잘 탐지 안됨 : crowdturfing UI가 다른 앱들과 비슷하기 때문
- 코드를 봤을때는 비슷해서 직접 코드 보고 판단하는 수 밖에..
- 그런 방법은 scalable 하지 않음

Semantic Analyzer – Crowdturfing keywords



- Crowdturfing keyword 크롤링 해둠
- keyword 추출 후 purify함

Semantic Analyzer



- 의미적으로 유사한지 비교

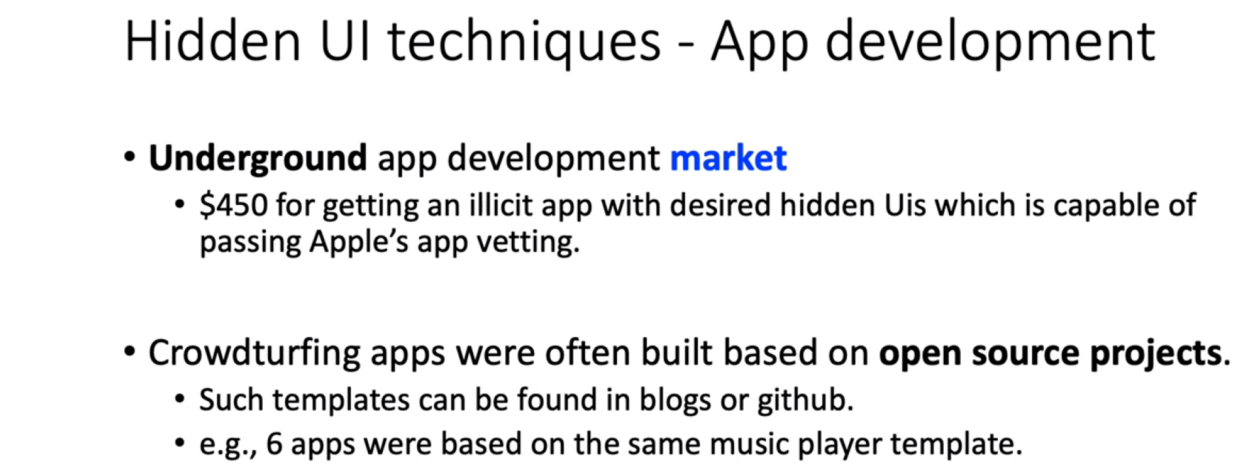
Result

- 102 crowdturfing apps were reported.
- **93 apps** were actual crowdturfing apps.
  - precision of 91.2% and FDR of 8.8%.
- All 93 apps were removed from the App Store.

- 정확도는 91.2%
- 93개의 malware 찾음

Understanding iOS-based Crowdturfing

- cyberCriminal이 앱 개발자에게 요청함
- 개발자가 개발해서 줌
- 앱을 올림
- 프로모션해서 많이 깔도록 함
- 사람들이 다운 받음
- 플랫폼이 형성 되면 cyber criminal이 이제 돈을 받고 task를 받음
- 해당 task 를 푸쉬



- 오픈 소스 프로젝트를 많이 사용