Tracking, Revealing and Detecting Crowdsourced Manipulation

http://digital.cs.usu.edu/~kyumin/cm
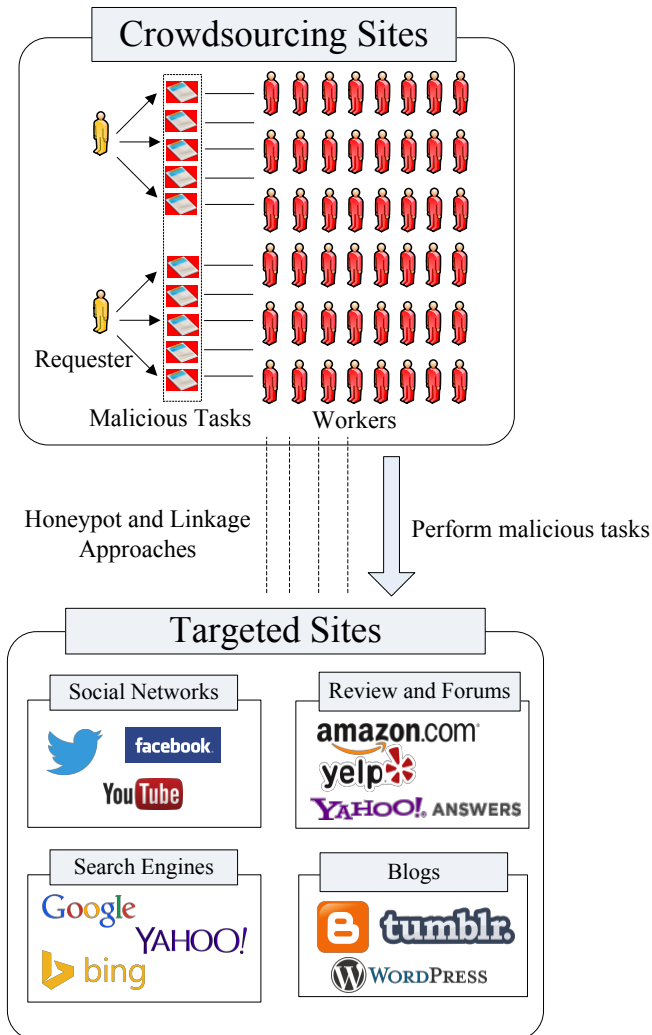
Utah State University

Challenge:

"Crowdturfers" spread malicious URLs in social media, form artificial grassroots campaigns ("astroturf"), manipulate search engines (e.g., via large-scale pay-per-click campaigns), write fake reviews, and create accounts for further attacks

Solution:

Create algorithms, frameworks, and systems for defending the open web ecosystem from these emerging threats.

Crowdsourcing Sites

Requester

Malicious Tasks   Workers

Honeypot and Linkage Approaches   Perform malicious tasks

Targeted Sites

Social Networks   Review and Forums

Search Engines   Blogs

Scientific Impact:

- Malicious task detector

- New blacklists for malicious tasks

- Detection of crowdturfers and other malicious participants

Broader Impact:

- Enable crowdsourcing service providers and targeted sites service providers to detect crowdsourced manipulation.

- Create future work force by creating Data Science courses, and actively recruit female students by working with USU's chapter of the ACM-W.