

Trust and Privacy Attacks in Online Social Networks

Yuhong Liu

Associate Professor, yhliu@scu.edu Department of Computer Science and Engineering Santa Clara University 2022/01/19

IEEE SF/OEB Computer Society Kick-off meeting

Santa Clara University







- Located at Santa Clara, CA
- A Jesuit private university
- The first high education operating institution in California (founded in 1851)



Research Interests – Trustworthy Computing



Energy efficient IoT security





Secure and fair digital trading based on Blockchain



Social Network

- Feedback based Online Reputation attack and defense
- Friendship Privacy
- Disinformation/misinformation propagation



Popularity of Online Social Media

HOW SCREEN TIME IS SPENT

Ranked by average minutes per day





https://www.zdnet.com/article/americans-spend-far-more-time-on-their-smartphones-than-they-think/

- YouTube users are uploading <u>500 hours of new videos every minute as of 2020, with more</u> <u>than 2 billion</u> logged-in monthly users
- Twitter: <u>187 million</u> monetizable daily active users, <u>59% users</u> regularly get news from Twitter
- Online Review systems: <u>89%</u> consumers worldwide read reviews before buying products.



Untrustworthy User Generated Content



Images from online sources

"When I realized that people believe what the Internet says more than reality, I discovered that I had the power to make people believe almost anything." - Andres Sepulveda, a political cyber hacker who digitally rigged elections across Latin America countries for eight years by spreading false information on online social media.

SCHOOL OF ENGINEERING



Arising User Privacy Concerns



Images from online sources



Various Ways to Attack





https://www.medpagetoday.com/infectiousdisease/covid19/91296



About 411,000,000 results (0.19 seconds)

Buzzoid - Buy Instagram Followers from \$2.97 only!

buzzoid.com/buy-instagram-followers/
*
**** Rating: 5 - 8,539 votes

Scouting around for a site to **buy** Instagram **followers** from? What more can we offer than cheap prices, instant delivery and fully secure purchase?

Buy Instagram Followers from \$2.97

socialroar.com/buy-instagram-followers/ ▼ ★★★★★ Rating: 5 - 7,823 votes Looking to buy instagram ronowers with instant delivery, quality service, and great customer support? Look no more, give us a try today.



SHARE YOUR SHOPPING EXPERIENCE ON AMAZON!

Thank you for your purchase, we hope you enjoy this product!

If you are satisfied with this purchase, would you like to share your experience on Amazon? This will help other customers to learn more about our product.

As our sincere appreciation for your kindly support, we will send a \$15 Amazon Gift Card.



Promoting?





Attack in Online Reputation Systems

Efficiently Promoting Product Online Outcome: An Iterative Rating Attack Utilizing Product and Market Property

Friendship Privacy in Online Social Network

Retrieving Hidden Friends: A Collusion Privacy Attack Against Online Friend Search Engine

Diversity of Social Groups V.S. Misinformation Propagation

Correlating Diversity and Resistance to Misinformation in Social Media Groups



Efficiently Promoting Product Online Outcome: An Iterative Rating Attack Utilizing Product and Market Property

Yuhong Liu, Wenqi Zhou and Hong Chen, "Efficiently Promoting Product Online Outcome: An Iterative Rating Attack Utilizing Product and Market Property", IEEE Transactions on Information Forensics and Security, Vol. 12, No. 6, pp. 1444-1457, 2017.



Online Reputation Systems



Significance:

- 79% of shoppers say they trust online reviews as much as personal recommendations
- Product pages with customer reviews bring 3.5 times more conversions than those without

Source: https://www.oberlo.com/blog/online-review-statistics



Challenging Issue

Online ratings can be easily manipulated!

Resident Evil: Afterlife (2010) More at IMDbPro »

Right after Released



User Rating:



- MOVIEmeter: 2 Up 64
- Up 64% in popularity this week. See why on IMDbPro.





While still out to destroy the evil Umbrella Corporation, Alice joins a group of survivors who want to relocate to the mysterious but supposedly unharmed safe haven known only as Arcadia.

Dir: Paul W.S. Anderson With: Milla Jovovich, Ali Larter, Wentworth Miller Action | Adventure | Horror | Sci-Fi

97 mins. 頂

Add to Watchlist



Challenging Issue

There are companies providing fake ratings for very cheap price !



http://www.socilab.net/buy-youtube-views



Existing Studies

- Diverse attacks:
 - Self-boosting
 - Alternative behavior
 - Bad mouthing
 -



Research Gap

- There are many rating attack studies mainly focusing on
 - How to <u>boost</u> their own products' rating as much as possible without being detected.
- Some aspects are underestimated:
 - Assume high rating values/volumes => increase product sales
 - Treat all products equally
 - Considering only external boost; not the market's "internal feedback"

Can we propose an advanced attack by re-examining these aspects?



Step 1: What factors influence product sales and how?



Influential factor for Online User Choices

Influential Factors	Rating Value	Rating Volume	Network Effect	Herding Effect
Impact	Non-linear	Larger volume => more downloa d/sales	Greater user base -> more download/s ales	Online consumers follows others' purchase
Additional Feature (Product Ranking)	The impact of each factor differs over products with different rankings			

CLNRA UNITERSTIT

l

The Proposed Quantile Regression Model

$$og(d_t^i)(\alpha) = \beta_0(\alpha) + \beta_1(\alpha) * Rev_u_{t-1}^i + \beta_2(\alpha) * \overline{r}_{t-1}^i + \beta_3(\alpha) * \overline{r}_{t-1}^i * \overline{r}_{t-1}^i + \beta_4(\alpha) * R_{t-1}^i + \beta_5(\alpha) * log(\widetilde{v}_{t-1}^i) + \beta_6(\alpha) * log(\widetilde{d}_{t-1}^i) + \beta_x(\alpha)Controls_{x,i,t} + \xi_{i,t}(\alpha)$$

Variable	Description		
	number of Weekly downloads of		
d_t^i	software i at week t		
	total number of downloads of		
\widetilde{d}_t^i	software i by week t		
	average user rating of software i by week t		
\bar{r}_t^i			
	total number of user rating of		
\widetilde{v}_t^i	software i by week t		
	the rank of software i at week t		
$R^i_{-\iota}$	measured by weekly sales/downloads		
	a binary variable to measure if software i		
$Rev_u_t^i$	is reviewed by users at week t		



Data Set

- In particular, we collect weekly data of software downloads and online user ratings from CNETD over 26 weeks in four categories.
 - Anti-virus
 - Download Managers
 - File Sharing
 - Web Browser



=

Impact of Rating Volume



Fig. 2: Impact of Rating Volume Change

Observations:

- the increase of rating volumes will always lead to positive impact on improving future downloads.
- the downloads of top ranked products are influenced most by rating volume changes. the impact of rating volume change dramatically drops for lower ranked products.



=

Impact of Rating Value



Observations:

- top ranked products will not be influenced by the rating value changes.
- Overly inflating the rating value of a product with low original ratings may even hurt its next week's downloads.

Fig. 1: Impact of Rating Value Change



An Example of "Internal Self-exciting"

The software in the File Sharing market named "BadBlue Personal Edition 2.7" was originally ranked as 47.



SCHOOL OF ENGINEERING



Observations

Product sales increase can be caused by

• External manipulations - rating value and volume change

◆ Internal consecutive self-exciting power



Step 2: Proposed Attack

SCHOOL OF ENGINEERING



Attack Design

In particular, we design the attack strategy by considering two aspects:

(1) how to determine the unfair rating values and volume

(2) how to take advantage of the market's internal selfexcitation power



Proposed Attack – Rating Value & Volume

Hence, we propose a rating value $r_c(\alpha)$, calculated as $r_c(\alpha) = -\frac{\beta_2(\alpha)}{2\beta_3(\alpha)}$, as the critical rating value, which changes across different product quantiles.

	Feasible Attacks	Optimal Attack
Туре І	$\bar{r}_{mal} \in (\bar{r}_o - \lambda, 5], (\lambda > 0)$	$\bar{r}_{mal} = 5$
$(\bar{r} > r_c(\alpha))$	$v_{mal} > 0$	$v_{mal} = N$
Type II	$\bar{r}_{mal} = any value$	
$(\bar{r} = r_c(\alpha))$	$v_{mal} > 0$	$v_{mal} = N$
		S1: $\bar{r}_{mal} = \bar{r}_o$
Type III	$\bar{r}_{mal} \in [1, \ \bar{r}_o - \lambda), \ (\lambda < 0)$	$v_{mal} = N$
$(\bar{r} < r_c(\alpha))$	$v_{mal} > 0$	S2: $\bar{r}_{mal} = 1$
		$v_{mal} = N$



Proposed Attack – Consecutive Market Self-excitation



26



Comparison to All-together Strategy



Fig. 11: Comparison between S_{iter} and S_{all}



Key Takeaway

- Customized attacks are more effective
- Market's internal self-excitation power can be utilized



Retrieving Hidden Friends: A Collusion Privacy Attack Against Online Friend Search Engine

Yuhong Liu, Na Li, "Retrieving Hidden Friends: A Collusion Privacy Attack Against Online Friend Search Engine", IEEE Transactions on Information Forensics and Security, 14, no. 4 (2018): 833-847.



Facebook Privacy Scandal



The Facebook data privacy scandal 2017 centers around the collection of personally identifiable information of "*up to 87 million people*" by the political consulting and strategic communication firm Cambridge Analytica. That company— and others—were able to gain access to personal data of Facebook users.



F

Friend Search Engine

Various online social network applications are developed for people to interact with family, friends and colleagues.

Friend Search Engine



SCHOOL OF ENGINEERING



Control # of Friends To Release

How about users do not want to share all of their friends?





Which Friend to Release?



Defense: keep track of the released friends' privacy

It works effectively against any *individual* malicious attacker.



This Work: Collusion Attacks

Attack Goal: multiple malicious requestors coordinately query the system => mislead the system to <u>leak additional</u> <u>friends</u>.



Step 1: A Toy Example – Attacks against a social clique



Attacks in a Social Clique (Dense Network)

 $I_{N_1} > I_{N_2} > I_{N_3} > I_{N_4} > I_{N_5} > I_{N_6} \qquad \text{Malicious requestor MR1}$

Assume:

- N3 is victim node
- K = 2



Violation fails !





Attacks in a Social Clique

$$I_{N_1} > I_{N_2} > I_{N_3} > I_{N_4} > I_{N_5} > I_{N_6}$$

Assume:

- N4 is victim node
- K = 2



Violation succeeds!



SCHOOL OF ENGINEERING



Observations

In a social clique,

- Top k+1 nodes: cannot be directly violated
- Other nodes: can be violated by <u>occupying</u> at least one of its friends.

Inspiration – violating privacy through occupation







Definition IV.2. Popular Node: A node that is on the top k influential friend list of **ALL** its top k influential friends.

Definition IV.3. Non-Popular Node: A node that is **NOT** in the top k influential friend list for **AT LEAST ONE** of its top k friends.

Non-Popular Node: can <u>always be violated</u> through occupation.

Popular Node: may be violated by recursively occupying friends' friends.



Step 2: Attacks in General Networks

SCHOOL OF ENGINEERING

Attack against a Non-popular node in a General Network



 $\begin{array}{l} \mathbf{MR_1}:\\ \mathbf{Query}\ N_0 - > \ \mathrm{retrieve}\ E_{(N_0,N_1)}, E_{(N_0,N_2)}, E_{(N_0,N_3)}\\ \mathbf{MR_2}:\\ \mathbf{Query}\ N_1 - > \ \mathrm{retrieve}\ E_{(N_1,N_{1.1})}, E_{(N_1,N_0)}, E_{(N_1,N_{1.2})}\\ \mathbf{MR_3}:\\ \mathbf{Query}\ N_2 - > \ \mathrm{retrieve}\ E_{(N_2,N_{2.1})}, E_{(N_2,N_{2.2})}, E_{(N_2,N_0)}\\ \mathbf{MR_4}:\\ \mathbf{Query}\ N_3 - > \ \mathrm{retrieve}\ E_{(N_3,N_{3.1})}, E_{(N_3,N_{3.2})}, E_{(N_3,N_{3.3})}\\ \mathbf{Query}\ N_0 - > \ \mathrm{retrieve}\ E_{(N_0,N_1)}, E_{(N_0,N_2)}, E_{(N_0,N_4)} \end{array}$

SCHOOL OF ENGINEERING



Attacks against a popular node in a General Network



 MR_1 : Query $N_0 - >$ retrieve $E_{(N_0,N_1)}, E_{(N_0,N_2)}$ MR_2 : Query $N_1 - >$ retrieve $E_{(N_1, N_{1,1})}, E_{(N_1, N_0)}$ MR_3 : Query $N_2 - >$ retrieve $E_{(N_2, N_{2,1})}, E_{(N_2, N_0)}$ MR_4 : Query $N_{1,1} - >$ retrieve $E_{(N_{1,1},N_{1,1,1})}, E_{(N_{1,1},N_{1,1,2})}$ Query $N_1 - >$ retrieve $E_{(N_1, N_{1,2})}, E_{(N_1, N_0)}$ MR_5 : Query $N_{1,2}$ -> retrieve $E_{(N_{1,2},N_{1,2,1})}, E_{(N_{1,2},N_{1})}$ Query $N_1 - >$ retrieve $E_{(N_1, N_{1,2})}, E_{(N_1, N_{1,1})}$ Query $N_0 - >$ retrieve $E_{(N_0, N_2)}, E_{(N_0, N_3)}$ Attack Result: Succeed

43



Attack Effectiveness





Summary



Privacy protection is challenging.

Your privacy may be in the hands of your friends



SCHOOL OF ENGINEERING



Correlating Diversity and Resistance to Misinformation in Social Media Groups

I Chang, Orion Sun, Jasper Ahn, Yuhong Liu, "Correlating Diversity and Resistance to Misinformation in Social Media Groups", IEEE Global Humanitarian Technology Conference (GHTC), 2021



day

Social Network Groups

Q Search Groups





Chinese Young Professionals Networkin... 12K members • 2 posts a week



SCHOOL OF ENGINEERING

47





<u>Greater diversity</u> in social media groups correlates with <u>greater</u> <u>resistance</u> to misinformation

Diversity: the measure of <u>how much variety</u> is present in the characteristics of a group. (not include race/age, but in terms of vocabulary range, content engagement, interactions with other social groups)

Misinformation resistance: how likely a social media group will *internalize and interact* with sources of misinformation once being exposed



Ę

Ground Truth Media Bias / Fact Check

Media Bias / Fact Check	Support MBFC: Become an Ad-Free Member		
Home Transparency · News Search · Pseudoscience Left-Center Blas Right-Center Blas Right Blas MBFC NEWS JANUARY 18, 2022 DAILY SOURCE BLAS CHECK: CANADALAN	Country Profiles Extensions RSS Re-E Conspiracy-Pseudoscience Questionable So	valuated Sources MORE + Least Blased Left Blas urces Pro-Science Satire Journalists SEARCH	
WHAT WE DO Ve are the most comprehensive media bias resource on the intr ources and journalists listed in our database and growing every Jse the search feature above (Header) to check the bias of any	rmet. There are currently 4200+ media day. Don't be fooled by Fake News sources. source. Use name or URL.	RECENTLY ADDED SOURCES OR PAGES Hickory Daily Record January 17, 2022 The Serrour Tolbune	
Read Factual News @	NFN 2 Easy Steps 1. Click "Start Now" 2. Add Protecto for Chrome™	January 16, 2022 La Junta Tribune-Democrat January 16, 2022 WMSN – Madison News January 15, 2022 WHO – Des Moines News January 15, 2022 Investor Times January 18, 2022 Wichita Standard January 12, 2022	
ATC CHECK, ORGINAL TRUTCHECK, ORGINAL THE Latest Fact Check Check 01/18/2022 Last updated on July 22nd, 2021 selects and publishes fact check	ts curated by Media Bias Fact at 08:52 am Each day Media Bias Fact Check s from around the world. We Templates that make it <i>simple</i> to design a <i>sehsite</i> for any idea.	ULCX - Biloxi News January 12, 202	
I meula didS/		Extreme	

Factual Reporting
Very High
High
Mostly Factual
Mixed
LOW
Very Low

	Mixed					
	LOW					
Very Low						
Left-Center	Least Biased	Right-Center	Right			

3000 pairs of domain names and factual accuracy scores

SCHOOL OF ENGINEERING

Extreme



Data Collection

FaceBook CrowdTangle

🔤 Q 🛧 👫 Y 🦎 🎙 者 G 🖸 📚 🗏 📣 🔃 🖬 🗐



Acco

SCHOOL OF ENGINEERING



Average factual accuracy score of associated sources



CLARA UNITERSITY

=

Proposed Entropy based Diversity Metrics

- Word entropy
 - Base form of words
- Post type entropy
 - Link posts, image posts, video posts, etc

- Average/Total reaction entropy
 - Like, Love, Haha, Angry, etc.
- Top level domain/domain entropy
 - .com, .org, .int, .edu, etc
 - cnbc.com
- Mutual Network Analysis (MNA) Entropy score







Key Metrics Correlated with **Misinformation Vulnerability**

- **Diversity Metrics**
 - **MNA** Score
 - Average Reaction Entropy
- **General Metrics**
 - Top Level Domains
 - .org
 - Reactions
 - Love and Angry

Misinformation Resist. vs. Avg. Reaction Entropy

Misinformation Resistance vs. .org Proportion







0.15

0.20 Love Proportion

0.25

Misinformation Resistance vs. Angry Proportion

.org Proportion



Misinformation Resistance vs. MNA Score





Key Takeaways

 The diversity of social groups is related to their resistance to misinformation.



Conclusion

- Online social networks are facing various security challenges
- The fast evolving arm race between attacks and defenses requires continuous future researches.





Thank You ! Questions ?

Yuhong Liu Associate Professor Computer Science and Engineering Department, Santa Clara University 500 El Camino Real Santa Clara, CA, 95053

Email: <u>yhliu@scu.edu</u> Tel: <u>408-551-3513</u>

Students/Researchers/Alumni at Our Lab













SCHOOL OF ENGINEERING