Privacy score

Privacy

Aghiles DJOUDI

Sorbonne University

August 2, 2019

Outline

Outline

Outline

1. Introduction

2. Approaches
   1. Behavioral
   2. Social
   3. Technical

3. Trust Models

Outline

Behavioral

Privacy Detective: Detecting Private Information and Collective Privacy Behavior in a Large Social Network [1]

res/2_1_2_0.png

Figure 1: User privacy score-1

res/2_1_2_1.png

Figure 2: User privacy score-2

res/2_1_2_2.png

Figure 3: User privacy score-3

- Content based features (Timelines)
- Amazon mechanical turk annotations (labeling)
  - Annotate the publicly available data which is used for calculating the privacy scores.
- 3-class supervised learning
  - Timelines are classified with privacy scores by using AdaBoost with Naive Bayes classifier.
- Study the correlation between Users Privacy Score and:
  - Users Friends Privacy Score (fig 1, 2, 3)
    - R value is 0.41, and a two-tailed P value is 0.005.
  - Mentioned (CC) Users Privacy Score
    - R value is 0.37 and a two-tailed P value is 0.01.
    - Users prefer to follow users that have similar privacy revealing habits.
  - Number of Friends
    - There is no statistically significant correlation between a users privacy score and the number of friends.

Behavioral

Detecting and resolving privacy conflicts for collaborative data sharing in online social networks [2]

- Input
  - Number of privacy conflicts $controllers_{ut}(i)$
    - number of the untrusting controllers
  - General privacy concern of an untrusting controller pc_j
  - Sensitivity of the data item sl_j
  - Visibility of the data item
  - Trust of an accessor tl_k (MTA)
- Measuring Privacy Risk:

  res/2_1_3_0.png

  res/2_1_3_1.png
- Measuring Sharing Loss:

  res/2_1_3_3.png
- Privacy Conflict Resolution on the Tradeoff between Privacy Protection and Data Sharing:

  res/2_1_3_4.png

res/2_1_3_5.png

Trust Model

Computational Trust Model for Repeated Trust Games [3]

res/2_1_4_0.png

res/2_1_4_5.png

Behavioral

Styx: Privacy risk communication for the Android smartphone platform based on apps' data-access behavior patterns [**bal_styx_2015**]

res/2_1_5_0.png

Figure 4: Cag.

Behavioral

Exploring nuances of user privacy preferences on a platform for political participation [4]

res/2_1_6_0.png

Behavioral

Prometheus: User-controlled P2P Social Data Management for Socially-aware Applications [5]

res/2_1_7_0.png

Figure 7: Geo-social Graph Representation

- Trusted Peer Group Management

Behavioral

Computing Privacy Risk and Trustworthiness of Users in SNSs [6]

res/2_1_9_0.png

Outline

Social

A Study of Online Social Network Privacy Via the TAPE Framework [7]

res/2_2_1_0.png

Figure 10: Cag.

res/2_2_1_1.png

- Node Information Spreading (NISP)
  - How likely a friend will spread other's PI ?
- Methods
  - TAPE: The friend with the largest Birnbaum's measure is blocked.
    - Evaluate the sensitivity of a friend link
  - Friend Degree: The friend that has the largest degree is blocked.
    - Evaluate the importance of a friend link
  - V-Index: The friend that has the largest V-Index is blocked.
    - Evaluate privacy setting of a friend ...
  - Random: Random friends are blocked.
    - Privacy risk decrease as undesirable destination (NISP) blocked
- Privacy risk decrease as undesirable destination (NISP) blocked

- Link Information Spreading (LISP)
  - How likely a friend will be in the path of PI diffusion

Social

Algorithm to trade off between utility and privacy cost of online social search [8]

res/2_2_2_0.png

Figure 12: Cag.

res/2_2_2_1.png

- Input:
  - p: Probability of influence from u to v.
  - dv: Degree of the node v.
  - sv: Number of neighbors of v who are seeds.
  - tv: Number of neighbors of v who are seeds and experts
- Method:
  - Utility Degree Discount Algorithm:
    - If (expert) $d_{dv} = (1-p)^{sv}$ [1 + (dv - tv)]
    - Else $d_{dv} = (1-p)^{sv}$ (dv - tv)
  - Utility Privacy Cost Ratio Discount Algorithm:
    - If (expert) $d_{dv} = (1-p)^{sv}$ [1 + (dv - tv)] / (dv - sv)
    - Else $d_{dv} = (1-p)^{sv}$ (dv - tv) / (dv - sv)
- Output:
  - Privacy: Number of seeds activated (FP)
  - Utility: Number of expert activated (TP)

Social

Privacy scoring of social network users as a service [9]

- Input
  - l0 [0, 1] : Disposition to privacy:
    - Attitude of an user towards privacy of his information.
    - l0 = 0,1 : Lax privacy orientation
  - h0 [0, 1] : Disposition to communication:
    - Attitude of an user towards communication online.
    - h0 = 0.1 : User who is very communication oriented
  - Friend Attitude Calculator (FACT):
    - Pn: The friends position in the sorted trust list.
    - Cn: The percentage of total communication.
    - tx: Total number of friends.

res/2_2_3_0.png

Figure 14: Experiment results with varying l0 and h0

res/2_2_3_2.png

Social

Privacy scoring of social network users as a service [9]

- Input
  - l0 [0, 1] : Disposition to privacy:
    - Attitude of an user towards privacy of his information.
    - l0 = 0,1 : Lax privacy orientation
  - h0 [0, 1] : Disposition to communication:
    - Attitude of an user towards communication online.
    - h0 = 0.1 : User who is very communication oriented
  - Friend Attitude Calculator (FACT):
    - Pn: The friends position in the sorted trust list.
    - Cn: The percentage of total communication.
    - tx: Total number of friends.

res/2_2_3_4.png

Figure 16: Experiment results with varying l0 and h0

res/2_2_3_2.png

Social

Privometer: Privacy protection in social networks [10]

res/2_2_4_2.png

Figure 18: Information Visibility in User Profile

res/2_2_4_1.png

res/2_2_4_3.png

Social

Privacy impact assessment for online social networks [11]

res/2_2_5_0.png

Figure 21: Data loss and Privacy Impact

- Direct Data Loss (Access control models)
  - I-BAC: Individual-Based Access Control
  - A-BAC: Authority-Based Access Control
  - T-BAC: Team-Based Access Control
    - R-BAC: Role-Based Access Control
    - Or-BAC: Organization-Based Access Control
    - Re-BAC: Relationship-Based Access Control
- Indirect Data Loss
  - Inference, aggregation, and de-anonymization.
- Potential Data Loss
  - Social engineering, phishing.

Social

Privacy-triggered communications in pervasive social networks [12]

- Input:
  - s: Device privacy (state)
  - b: Message privacy (action)
  - R: Reward
  - u: Stationary policy
- Method:
  - P_{ij} is the probability to transition from state si to sj at time t

    res/2_2_6_1.png

  - Random variable

Social

A Framework for Computing the Privacy Scores of Users in Online Social Networks [**liu_framework_2010**]

		Sensitivity	β_1	...	β_n
Privacy	Attitude	User/item	item 1	...	item n
P_1	θ_1	User 1	...	...	...
...	...	...	...	R(i,j)	...
P_N	θ_N	User N	...	...	...

Table 1: An example table.

res/2_2_7_1.png

res/2_2_7_0.png

Social

Predicting friendship levels in online social networks [**ahmad_predicting_2010**]

res/2_2_8_0.png

Figure 23: Levels of OSN

res/2_2_8_2.png

Social

Risks of Friendships on Social Networks [13]

res/2_2_10_0.png

Figure 26: H

- Social Frequency Matrix for friends: N x F x n
  - N: user, F: friends, n: friends features
- Transformation:
  - Transform friends features into numerical form
  - Hometown = Rome: Hometown = 15/100
- Baseline Estimation:
  - Logistic regression analysis of features.
  - Ex: %0.9 very risky, %0.09 risky and %0.01 not risky.
- Learning Friend Impacts:
  - Past Labeling Parameter
    - PS: Profile similarity
  - Friend Impact Parameter
    - Single Impact for the Friend Cluster
    - Multiple Impact for the Friend Cluster

Social

unfriendly: Multi-party privacy risks in social networks [**thomas_unfriendly_2010**]

res/2_2_11_0.png

Outline

Technical

Privacy-Aware Web Service Composition and Ranking [**costante_privacyaware_2013**]

res/2_3_2_0.png

Figure 28: Privacy-Aware Architecture

Technical

Ostra: Leveraging trust to thwart unwanted communication [14]

Technical

On the Design of Socially-Aware Distributed Systems [15]

res/2_3_4_0.png

Figure 30: different system levels

Technical

A privacy self-assessment framework for online social networks [16]

res/2_3_6_0.png

Figure 31: Privacy scores

Technical

A privacy awareness system for facebook users [17]

res/2_3_9_0.png

Technical

Identifying hidden social circles for advanced privacy configuration [**squicciarini_identifying_2014**]

res/2_3_10_0.png

Figure 35: hghg

Outline

models.png models.png models.png models.png models.png models.png models.png models.png
models.png models.png models.png models.png models.png models.png models.png models.png

res/trust models.png

References

[1] Aylin Caliskan Islam, Jonathan Walsh, and Rachel Greenstadt. “ Privacy Detective: Detecting Private Information and Collective Privacy Behavior in a Large Social Network ”. In: *Proceedings of the 13th Workshop on Privacy in the Electronic Society*. WPES ’14. 00019. New York, NY, USA: ACM, 2014, pp. 35–46 (p. 6).

[2] Hongxin Hu, Gail-Joon Ahn, and Jan Jorgensen. “ Detecting and Resolving Privacy Conflicts for Collaborative Data Sharing in Online Social Networks ”. In: *Proceedings of the 27th Annual Computer Security Applications Conference*. 00095. ACM, 2011, pp. 103–112 (p. 7).

[3] Quang-Vinh Dang and Claudia-Lavinia Ignat. “ Computational Trust Model for Repeated Trust Games ”. In: *Trustcom/BigDataSE/I SPA, 2016 IEEE*. 00002. IEEE, 2016, pp. 34–41 (p. 8).

[4] Aigul Kaskina. *Exploring Nuances of User Privacy Preferences on a Platform for Political Participation*. 00001. Université de Fribourg, 2017 (p. 10).

[5] Nicolas Kourtellis et al. “ Prometheus: User-Controlled P2P Social Data Management for Socially-Aware Applications ”. In: *Proceedings of the ACM/IFIP/USENIX 11th International Conference on Middleware*. Middleware ’10. 00070. Berlin, Heidelberg: Springer-Verlag, 2010, pp. 212–231 (p. 11).

[6] Akansha Pandey et al. “ Computing Privacy Risk and Trustworthiness of Users in SNSs ”. In: 00002. IEEE, Sept. 2015, pp. 145–150 (p. 12).

[7] Yongbo Zeng et al. “ A Study of Online Social Network Privacy Via the TAPE Framework ”. In: *IEEE Journal of Selected Topics in Signal Processing* 9.7 (Oct. 2015). 00003, pp. 1270–1284 (p. 14).

[8] Yan Li, Zhiyi Lu, and Victor OK Li. “ Algorithm to Trade off between Utility and Privacy Cost of Online Social Search ”. In: *Communications (ICC), 2016 IEEE International Conference On*. 00000. IEEE, 2016, pp. 1–6 (p. 15).

[9] B. S. Vidyalakshmi, Raymond K. Wong, and Chi-Hung Chi. “ Privacy Scoring of Social Network Users as a Service ”. In: *Services Computing (SCC), 2015 IEEE International Conference On*. 00004. IEEE, 2015, pp. 218–225 (p. 16, 17).

[10] Nilothpal Talukder et al. “ Privometer: Privacy Protection in Social Networks ”. In: *Data Engineering Workshops (ICDEW), 2010 IEEE 26th International Conference On*. 00067. IEEE, 2010, pp. 266–269 (p. 18).

[11] Yong Wang and Raj Kumar Nepali. “ Privacy Impact Assessment for Online Social Networks ”. In: *Collaboration Technologies and Systems (CTS), 2015 International Conference On*. 00002. IEEE, 2015, pp. 370–375 (p. 19).

[12] Murtuza Jadliwala et al. “ Privacy-Triggered Communications in Pervasive Social Networks ”. In: *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2011 IEEE International Symposium on a*. 00005. IEEE, 2011, pp. 1–6 (p. 20).

[13] Cuneyt Gurcan Akcora, Barbara Carminati, and Elena Ferrari. “ Risks of Friendships on Social Networks ”. In: 00020. IEEE, Dec. 2012, pp. 810–815 (p. 23).

[14] Alan Mislove et al. “ Ostra: Leveraging Trust to Thwart Unwanted Communication ”. In: (2008). 00193, p. 16 (p. 27).

[15] Nicolas Kourtellis. “ On the Design of Socially-Aware Distributed Systems ”. In: (2012). 00011, p. 193 (p. 28).

[16] Ruggero G. Pensa and Gianpiero Di Blasi. “ A Privacy Self-Assessment Framework for Online Social Networks ”. In: *Expert Systems with Applications* 86 (Nov. 2017). 00002, pp. 18–31 (p. 29).

[17] Charles Hélou, A. Guandouz, and Esma Aïmeur. “ A Privacy Awareness System for Facebook Users ”. In: *Journal of Information Security Research* 31 (2012). 00006, pp. 15–29 (p. 30).