Security Risk Estimation of Social Network Privacy Issue

Xueqin Zhang
School of Information Science and Engineering
East China University of Science and Technology
Shanghai 200237, China
zxq@ecust.edu.cn

Li Zhang
School of Information Science and Engineering
East China University of Science and Technology
Shanghai 200237, China
y30150590@mail.ecust.edu.cn

Chunhua Gu
School of Information Science and Engineering
East China University of Science and Technology
Shanghai 200237, China
chgu@ecust.edu.cn

ABSTRACT

Users in social network are confronted with the risk of privacy leakage while sharing information with friends whose privacy protection awareness is poor. This paper proposes a security risk estimation framework of social network privacy, aiming at quantifying privacy leakage probability when information is spread to the friends of target users' friends. The privacy leakage probability in information spreading paths comprises Individual Privacy Leakage Probability (IPLP) and Relationship Privacy Leakage Probability (RPLP). IPLP is calculated based on individuals' privacy protection awareness and the trust of protecting others' privacy, while RPLP is derived from relationship strength estimation. Experiments show that the security risk estimation framework can assist users to find vulnerable friends by calculating the average and the maximum privacy leakage probability in all information spreading paths of target user in social network. Besides, three unfriending strategies are applied to decrease risk of privacy leakage and unfriending the maximum degree friend is optimal.

CCS Concepts

• **Security and privacy → Social aspects of security and privacy.**

Keywords

privacy leakage; security estimation; relationship strength; trust; unfriending

1. INTRODUCTION

Considering the prevalence and influence of social networking, potential security risk of privacy problems when sharing personal information in social network stemmed from social network have become increasingly grievous and thought-provoking[1].So quantifying the privacy leakage risk is significant and meaningful for each user in social network.

Accordingly, some articles composed to reveal the potential threat and vulnerability in online social network [2]. Measuring individuals' vulnerability according to their friends' privacy settings and their network is proposed in [3] [4]. Vulnerability index was proposed to measure how vulnerable online social network (OSN) users are [5]. In [6], the author introduces TAPE framework to estimate privacy risk of social network based on the similarity between the reliability analysis in wireless sensor networks and the privacy risk estimation in online social network. Despite defining and analyzing privacy risk partly, these articles didn't consider the effect of human behaviors on privacy leakage, meanwhile individual's privacy leakage risk is influenced by relationship in online social network.

This manuscript proposes a security risk estimation framework of social networking privacy to calculate probability of individual privacy leakage through social graph. The framework composes of two parts, which are the calculation of Individual Privacy Leakage Probability and the Relationship Privacy Leakage Probability which considers the factors of relationship strength and interactive behaviors. Individual Privacy Leakage Probability is regarded as the probability user would gossip others' privacy in his/her moments, while the user has heard and been attracted by others' personal information, calculated from vectors, privacy protection awareness(PPA) and privacy protection trust (PPT). Relationship Privacy Leakage Probability depends on relationship strength estimation, under the premise of the stronger relationship strength can reveal more privacy information to each other. On the basis of [7], IPLP is quantified, furthermore, relationship strength estimation algorithm proposed is applied to estimate RPLP.

2. RELATED WORK

2.1 Definition of privacy leakage risk

In online social network, when the individual' private information of person P is divulged from his/her friend FP to another one FFP (FFP is not P's friend), then it is called privacy leakage, shown as Figure 1.

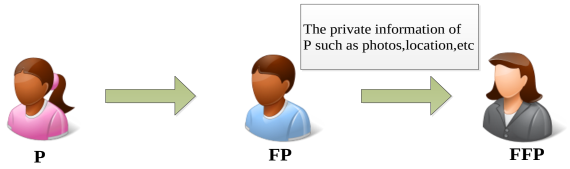

Figure 1. An example of privacy leakage

2.2 Individual Privacy Leakage Probability

Individual Privacy Leakage Probability(IPLP) describes the probability that a user divulge his/her friends' privacy based on his/her subjective consciousness. Inspired by [7], two vectors,

ICCNS 2017, November 24–26, 2017, Tokyo, Japan.
© 2017 Association for Computing Machinery.
ACM ISBN 978-1-4503-5349-6/17/11 …$15.00.
https://dx.doi.org/10.1145/3163058.3163073

namely privacy protection awareness(PPA) and privacy protection trust(PPT) are proposed in this paper to estimate IPLP.

2.2.1 PPA

PPA is denoted as the privacy caring level of a user. It depends on the user's privacy settings $S_u = \{s_{u,j} | j = 1,2, \cdots, J\}$ where u is the user and $s_{u,j}$ is the privacy setting in item of user profile I_j. Usually, in a social network, privacy setting has options {public, friends of friends, friends, self}, corresponding to value {1,2,3,4}. Then, individual privacy protection awareness *IPPA* is calculated as following:

$$IPPA_{u,j} = \frac{1}{2}\left(rank_{u,j}^{+} - rank_{u,j}^{-}\right) + \frac{1}{2} \quad (1)$$

Where $rank_{u,j}^{+}$ represents the proportion of users whose privacy setting $s_{u,j}$ is looser than that of user u , in contrary, $rank_{u,j}^{-}$ represents the proportion of users with tighter privacy setting $s_{u,j}$ than user u .

Calculating the *IPPA* for all types of information, the *PPA* of u is calculated as following:

$$PPA_u = \frac{1}{J}\sum_{j=1}^{J} IPPA_{u,j} \quad (2)$$

2.2.2 PPT

Privacy protection trust (PPT)is applied to evaluate how much a user should be trusted by others in protecting privacy. This indicator is acquired based on the synthesize evaluation of friends. The trust evaluation levels of friend f_j to a user u_i is T_{ji}.T_{ji} has options {never, hardly, neutral, pretty, very} corresponding to value {0.2,0.4,0.6,0.8,1}. Considering the evaluation of friends with high *PPA* is more reliable, PPT can be estimate as following:

$$\mathrm{PPT}(u_i) = \frac{\sum_{j=1}^{J} T_{ji}^{+}}{J} \quad (3)$$

Where T_{ji}^{+} represents T_{ji} evaluated by friends whose PPA is higher than the given threshold *e*. When there doesn't exist high *PPA* (PPA > e)friends,the user's PPT is evaluated by top3 PPA friends without high *PPA* (PPA > e) friend, otherwise it is set as 0.1 with less than 3 friends.

2.2.3 Estimation of IPLP

IPLP is resulted from PPA and PPT. Personal privacy disclosure is related to the degree of self-protection and the trustworthiness of the surrounding friends. PPA reflects the degree of privacy protection , and PPT refers to the trust whose friends contribute to him/her. But specific algorithms can't be raised to determine the importance between them according to the known information. So the estimation of IPLP is

$$\mathrm{IPLP}(u_i) = w * \mathrm{PPA} + (1 - w) * \mathrm{PPT} \quad (4)$$

Where w is a weight factor between 0 and 1.In the experiments, it is set as 0.5.

2.3 Relationship Privacy Leakage Probability

RPLP describes the probability of privacy leakage based on the relationship of friends. Typically, individuals tend to reveal more private information to friend online with stronger relationship strength. RPLP is quantified by estimation of relationship strength.

2.3.1 Estimation of Relationship Strength

This article postulates a probabilistic model according to similarity of users' profiles, degree of interaction, similarity of interest to measure relationship strength.

2.3.1.1 Similarity of User Profile

The homophily principle manifests that people are inclined to form ties with other people who have similar characteristics [8]. $S^{ij} = \{s_1^{ij}, s_2^{ij}, \cdots, s_M^{ij}\}$ represents the similarity of user profile between user u_i and u_j.There exists a positive correlation between relationship strength T_{ij} and user profiles similarity S_{ij}.Here, M stands for the number of attributes in the profile. If user u_i and u_j share the identical value at *K*-th item, then $s_K^{ij} = 1$, else $s_K^{ij} = 0$.

The dependency between T_{ij} and S_{ij} subjects to Gaussian distribution [3], denoted as following

$$\mathrm{P}\left(T_{ij} | S_{ij}\right) = \mathrm{N}(w^T S_{ij}, \mathrm{v}) \quad (5)$$

Where w is a *M*-dimensional weight vector to be learned, and ν is set to 0.5 as the variance of Gaussian Model.

2.3.1.2 Degree of Interaction

Relationship strength T_{ij} can contribute to distinct interaction, such as like, comment and forward, impacting degree of interaction, denoted as D_{ij} .There exists stronger relationship strength between different users with more interactive behaviors. The degree of interaction depends on two factors. Firstly, the count of comments, forwards and likes between users is pivotal, which is specified as $Comment(i,j)$. The other is standard deviation of interactive frequency within a specific time interval T,denoted as $Frequency(i,j)$. This article holds that three times a week within a month leads to stronger relationship strength than twelve times in a week in the premise of interaction behaviors up to twelve times a month. D_{ij} reflects the strength of interactive behaviors, which is calculated as following:

$$D_{ij} = \lambda_1 * Comment(i,j) + \lambda_2 * Frequency(i,j) \quad (6)$$

$$\mathrm{Comment(i,j)} = 0.5 * (\frac{comment(i,j)}{set(j)} + \frac{comment(j,i)}{set(i)}\Big) \quad (7)$$

$$\mathrm{Frequency(i,j)} = 1 - \sqrt{\frac{1}{N}\sum_{n=1}^{N}(w_i - \overline{w})^2} \quad (8)$$

Where $\lambda_1 + \lambda_2 = 1$, $set(i)$ represents the count of interactive documents in a specific period of time T,such as one month, w_i and $\overline{w}$ is shown as following:

$$w_i = \frac{\text{the interactive frequency in } i\text{th week}}{\text{the interactive frequency in } one\ month} \quad (9)$$

$$\overline{w} = \frac{comment(i,j) + comment(j,i)}{4} \quad (10)$$

2.3.1.3 Similarity of Interest

Similarity of interest between the user u_i and u_j ,denoted as C_{ij} ,is depicted by judging whether the friends have common posts in some information domains such as work, learning, travel, diet, sports, etc. Information domain vector is described as $\mathrm{d} = \{d_1, d_2, \cdots, d_N\}$, N represents the count of information domains. If the users u_i and u_j both have posts in domain $n(n = 1,2 \ldots N)$,then $d_n^{ij} = 1$,else $d_n^{ij} = 0$.Similarity of interest is calculated as following:

$$C_{ij} = \frac{\sum_{n=1}^{N} d_n}{N} \quad (11)$$

The interactive behaviors strength depends on the relationship strength and similarity of interest. The dependency among D_{ij},T_{ij} and C_{ij} is modeled as following [3]:

$$\mathrm{P}\left(D_{ij} | T_{ij}, C_{ij}\right) = \mathrm{N}(\alpha T_{ij} + \beta C_{ij}) \quad (12)$$

Where α, β are two coefficients. The relationship strength T_{ij},parameters α and β are obtained by training with the vectors D_{ij},S_{ij} and C_{ij}.

2.3.1.4 Estimation of Relationship Strength

From equations (5) and (12), $\mathrm{P}(T_{ij}, D_{ij})$ can be derived from $\mathrm{P}(T_{ij}|S_{ij})$ and $\mathrm{P}(D_{ij}|T_{ij}, C_{ij})$,the joint probability distribution is as following considering the conditional dependency

$$\mathrm{P}(T_{ij}, D_{ij}|S_{ij}, C_{ij}) = P(T_{ij}|S_{ij})P(D_{ij}|T_{ij}, C_{ij}) \qquad (13)$$

To avoid over-fitting,L_2 regularizes on the parameters w and α, β , which can be regarded as Gaussian priors

$$\mathrm{P}(w) \propto e^{-(\lambda_1/2)w^T w} \qquad (14)$$

$$\mathrm{P}(\alpha, \beta) \propto e^{-(\lambda_1/2)(\alpha^2+\beta^2)} \qquad (15)$$

The vectors D_{ij} ,S_{ij} and C_{ij} are all visible, w and α, β can be learned from the probability model. Given N pairs of users with friendship, Eq. (13) is converted as following:

$$\mathrm{P}(w, \alpha, \beta)\mathrm{P}(w)\mathrm{P}(\alpha, \beta)$$
$$\prod_{(i,j)\epsilon N} P(T_{ij}|S_{ij}, w)\, P(D_{ij}|T_{ij}, C_{ij}, \alpha, \beta)P(w)P(\alpha, \beta)$$
$$\propto \prod_{(i,j)\epsilon N} e^{\left(-\frac{1}{2v}\right)(w^T S_{ij}-T_{ij})^2}\, e^{\left(-\frac{1}{2v}\right)(\alpha T_{ij}+\beta C_{ij}-D_{ij})^2} \times$$
$$e^{-(\lambda_1/2)w^T w} e^{-(\lambda_1/2)(\alpha^2+\beta^2)} \qquad (16)$$

Point estimation of the parameters is applied to maximize the joint likelihood when T_{ij} is regarded as a parameter. The log-likelihood is estimated based on Eq. (16):

$$\mathcal{L}\left(T^{(\{(i,j)\epsilon N\})}, w, \alpha, \beta\right) = -\frac{1}{2v}\sum\nolimits_{(i,j)\epsilon N}\left(\alpha T_{ij} + \beta C_{ij} - D_{ij}\right)^2 - \frac{\lambda_1}{2}w^T w - \frac{1}{2v}\left(w^T S_{ij} - T_{ij}\right)^2 - \frac{\lambda_2}{2}(\alpha^2 + \beta^2) + C \qquad (17)$$

The function $\mathcal{L}$ is concave, a gradient-based method is adopted to optimize the parameters w, α, β and variable T_{ij} .The Newton-Raphson method will update , α, β and variable T_{ij} iteratively until convergence.

$$T_{ij}^{new} = T_{ij}^{old} - \frac{\partial \mathcal{L}}{\partial T_{ij}} \Big/ \frac{\partial^2 \mathcal{L}}{\partial (T_{ij})^2} \qquad (18)$$

$$\alpha^{new} = \alpha^{old} - \frac{\partial \mathcal{L}}{\partial \alpha} \Big/ \frac{\partial^2 \mathcal{L}}{\partial \alpha^2} \qquad (19)$$

$$\beta^{new} = \beta^{old} - \frac{\partial \mathcal{L}}{\partial \beta} \Big/ \frac{\partial^2 \mathcal{L}}{\partial \beta^2} \qquad (20)$$

$$w^{new} = (\lambda_1 wI + S^T S)^{-1} S^T T \qquad (21)$$

Description of the optimization procedure is in Algorithm 1.

Algorithm 1. The optimization procedure.

```
While not converged do
For each Newton-Raphson step do
Update $w$ according to equation (21)
For $(i,j)\epsilon N$ do
Update $T_{ij}, \alpha, \beta$ according to (18) - (20)
until Convergence.
```

2.3.2 Estimation of RPLP

RPLP expounds that privacy tends to be unintentionally leaked through intimate people, and a greater value of. RPLP aggravate the likelihood of privacy disclosure. There is a positive correlation between relational intensity and RPLP. According to the learning algorithm from [9] by equations (5) and (12), relationship strength T_{ij} is calculated, and RPLP is determined by T_{ij} as following:

$$\mathrm{RPLP(ij)} = T_{ij} \qquad (22)$$

3. SECURITY RISK ESTIMATION FRAMEWORK OF PRIVACY

Security risk estimation of privacy in social network is shown as Figure 2.A Miniature prototype of online social network is depicted as Figure 3. $\mathrm{A} = \{\mathrm{F1}, \mathrm{F2}, \mathrm{F3}, \mathrm{F4}\}$ is a set of Alice's friends. $\mathrm{B} = \{\mathrm{FF1}, \mathrm{FF2}, \mathrm{FF3}, \mathrm{FF4}, \mathrm{FF5}, \mathrm{FF6}\}$ represents Alice's friends . Alice is exposed to privacy disclosure while private information being disseminated from set *A* to any element of set *B*, that is,$\{\mathrm{Alice} \rightarrow \mathrm{F2} \rightarrow \mathrm{FF4}\}$ is one of paths to leak the privacy of Alice, and probability of privacy leakage is

$$L_{Alice,FF4} = RPLP(c1) * IPLP(F2) * RPLP(c2)$$

Where IPLP represents individual privacy leakage probability, RPLP represents relationship privacy leakage probability, which have been elaborated in 2.2 and 2.3, $c1$ is the connection between Alice and F2, $c2$ is the connection between F2 and F4 in Figure 3.

4. EXPERIMENTS

4.1 Data Collection

Dataset of 46 Facebook users' privacy settings is obtained by questionnaire. The users' profiles items and interactive documents in one month are downloaded from Facebook website. The items of user privacy settings include gender, birth date, phone number, education, current city, hometown, life events, professional skill, college. Friendship between 46 users is shown as Figure 4.

4.2 Experiments and Results

4.2.1 Experiment 1

In this experiment, the IPLP of 46 users is shown as Figure 5. The user with the higher IPLP more likely divulges the privacy of friends online. From Figure 5, the result that users numbered 44 and 45 are more vulnerable in divulging others' privacy is obtained, attributed to the number of friends belonged to target users and various evaluation of numerous friends with high PPA.

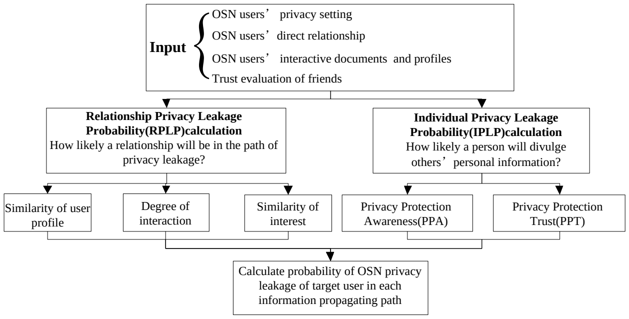
Input
OSN users' privacy setting
OSN users' direct relationship
OSN users' interactive documents and profiles
Trust evaluation of friends
Relationship Privacy Leakage Probability(RPLP)calculation
How likely a relationship will be in the path of privacy leakage?
Individual Privacy Leakage Probability(IPLP)calculation
How likely a person will divulge others' personal information?
Similarity of user profile
Degree of interaction
Similarity of interest
Privacy Protection Awareness(PPA)
Privacy Protection Trust(PPT)
Calculate probability of OSN privacy leakage of target user in each information propagating path

Figure 2. Risk estimation Framework of privacy leakage

4.2.2 Experiment 2

Normalized Discounted Cumulative Gain (nDCG)[10] is applied to estimate the relationship strength calculation model, which depicts the relevance between users and the returned relationship strength. All the users are required to score the relationship strength of their friends with one from the collection $\{0.1, 0.2, \ldots, 1\}$. When the difference between each side of friends is more than 0.2, these two users is requested to re-score the relationship strength. On a scale of 1-4, 1 represents terrible, 2 represents bad, 3 represents fair, and 4 represents good. Top50 strength values are selected to calculate the nDCG. For optimizing the parameters to obtain the optimal nDCG,λ_1, λ_2 are adjusted to attend maximum when $\lambda_1 = 0.1, \lambda_2 = 0.7$,shown as Figure 6. Besides the average nDCG is prior to 0.9.

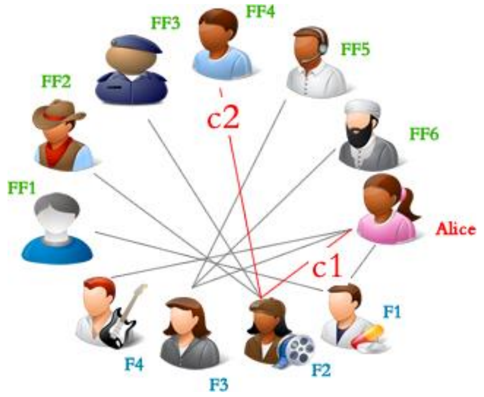

Figure 3. Miniature prototype in online social network

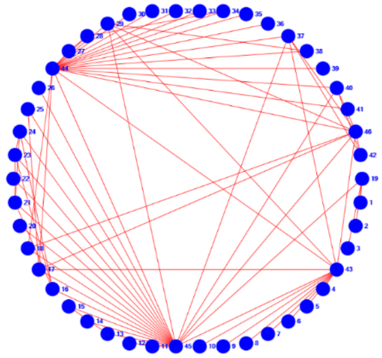

Figure 4. Friendship between 46 users in Facebook

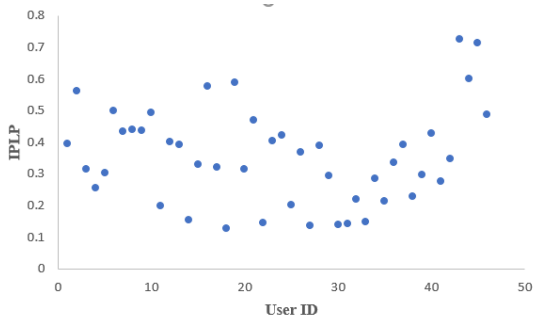

Figure 5. The IPLP of 46 users

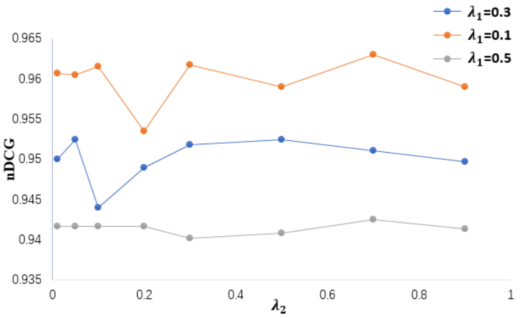

Figure 6. The nDCG of Top50 strength values

4.2.3 Experiment 3

In this experiment, we calculate the average and maximum probability of privacy disclosure in all spreading paths. The average privacy leakage probability, the maximum privacy leakage probability and the corresponding spreading path is given in Table 1. Subjected to the constraint of convergence, the result of 10 users randomly selected is shown as Table 1.

Table 1. Probability of privacy disclosure and corresponding path

User ID	Average probability	Maximum probability	Corresponding path
18	0.2637	0.4764	[18 → 44 → 37]
21	0.3088	0.4146	[21 → 45 → 20]
23	0.4123	0.5535	[23 → 45 → 20]
24	0.3462	0.4648	[24 → 45 → 20]
29	0.1118	0.2888	[29 → 46 → 17]
37	0.206	0.4764	[37 → 44 → 18]
40	0.2174	0.449	[40 → 45 → 20]
43	0.272	0.5477	[43 → 45 → 20]
44	0.3108	0.5561	[44 → 45 → 20]
46	0.3032	0.5483	[46 → 45 → 20]

It can be concluded that we can quantify the probability of privacy leakage and find the maximum leakage path by calculating. The users' privacy is more possibly divulged by friends numbered 44 ,45 and 46 to unfamiliar people online.

4.2.4 Experiment 4

In this experiment, 10 users are selected to evaluate the unfriending methods, which decrease the privacy disclosure probability with respect to the max degree, IPLP and RPLP of friend connections. The concrete strategies are as following:

1.Unfriend Facebook users' friend with the maximum degree.

2.Unfriend Facebook users' friend with the maximum IPLP.

3.Unfriend Facebook users' friends with maximum RPLP.

The experiment results of unfriending the user's friend in column 1 is shown in Table 2.

Table 2. Three unfriending strategies in Facebook

User ID	Average probability reduction		
	Maximum degree	Maximum IPLP	Maximum RPLP
18	0.123	0.103	0.103
21	0.267	0.267	0
23	0.368	0.368	0
24	0.307	0.307	0
29	0.008	0.014	0.011
37	0.010	0.06	0.010
40	0.134	0.012	0.006
43	0.162	0.04	0
44	0.184	0.184	0.
46	0.132	0.013	0.063

From the Table 2, unfriending the user' maximum degree friend is optimal in three unfriending strategies, which can diminish the risk of privacy disclosure at utmost.

5. CONCLUSION AND FUTURE WORK

In online social network, privacy leakage may remain all the time while personal information is shared by interaction with friends. This manuscript proposes a security risk estimation framework of privacy issue in online social network by quantifying the probability of privacy leakage in each disseminating path of information. Besides, three unfriending strategies in real dataset of Facebook are conducted to decrease the rate of privacy leakage in online social network. In the future, a large-scale social networking should be established with more complicated relationship to guarantee a more reliable privacy security analysis of social networking.

6. REFERENCES

[1] Krishnamurthy B, Wills C E. On the leakage of personally identifiable information via online social networks[C]// ACM Workshop on Online Social Networks, Wosn 2009, Barcelona, Spain, August. DBLP, 2009:7-12.

[2] Zeng Y, Sun Y, Xing L, et al. A Study of Online Social Network Privacy Via the TAPE Framework[J]. IEEE Journal of Selected Topics in Signal Processing, 2015, 9(7):1270-1284.

[3] Larionovs A, Teilans A, Grabusts P. CORAS for Threat and Risk Modeling in Social Networks [J]. Procedia Computer Science, 2015, 43:26-32.

[4] Laorden C, Sanz B, Alvarez G, et al. A Threat Model Approach to Threats and Vulnerabilities in Online Social Networks[C]// Computational Intelligence in Security for Information Systems 2010 - Proceedings of the, International Conference on Computational Intelligence in Security for Information Systems. DBLP, 2010:135-142.

[5] Gundecha P, Barbier G, Liu H. Exploiting Vulnerability to Secure User Privacy on Social Networking Site[J]. Acm Sigkdd, 2011:511-519.

[6] Gundecha P, Barbier G, Tang J, et al. User Vulnerability and Its Reduction on a Social Networking Site[J]. Acm Transactions on Knowledge Discovery from Data, 2014, 9(2):1-25.

[7] Y. Zeng, Y. Sun, L. Xing and V. Vokkarane, "Trust-aware privacy evaluation in online social networks," 2014 IEEE International Conference on Communications (ICC), Sydney, NSW, 2014, pp. 932-938.

[8] Xiang R, Neville J, Rogati M. Modeling relationship strength in online social networks[C]// International Conference on World Wide Web. ACM, 2010:981-990.

[9] Xiong L, Lei Y, Huang W, et al. An estimation model for social relationship strength based on users' profiles, co-occurrence and interaction activities[J]. Neurocomputing, 2016, 214:927-934.

[10] Bevan J L, Pfyl J, Barclay B. Negative emotional and cognitive responses to being unfriended on Facebook: An exploratory study[J]. Computers in Human Behavior, 2012, 28(4):1458-1464.