A Framework for Computing the Privacy Scores of Users in Online Social Networks

February 4, 2011

Problem Description

How to measure privacy risk of social network users

- Privacy protection Related works.
  - Spamming and Phishing.
  - Social network Attacks.
  - Access control privacy control.
  - Multi-party collaborative privacy control.
  - ...
- How to evaluate the risk level?

Contributions of This Paper

- A privacy score computation model.
- Model validation method.

General Observations and Intuitions

- Different profile items have different contribution to privacy score.
- The visibility of information can affect the privacy score.

Modeling Social Network Users

$$\Longrightarrow R_{n,N} = \begin{pmatrix} R_{1,1} & R_{1,2} & \cdots & R_{1,N} \\ R_{2,1} & R_{2,2} & \cdots & R_{2,N} \\ \vdots & \vdots & \ddots & \vdots \\ R_{n,1} & R_{n,2} & \cdots & R_{n,N} \end{pmatrix}$$

The Item Response Theory(IRT) Model

$$P_{ij} = \frac{1}{1 + e^{-\alpha_i(\theta_j - \beta_i)}}$$

Definition of the Privacy Score

$$\textsc{Pr}(i,j) = \beta_i \times V(i,j) \quad (1)$$

$$\textsc{Pr}(j) = \sum_{i=1}^{n} \textsc{Pr}(i,j) = \sum_{i=1}^{n} \beta_i \times V(i,j). \quad (2)$$

$$V(i,j) = P_{ij} \times 1 + (1 - P_{ij}) \times 0 = P_{ij} \quad (3)$$

where

$$P_{ij} = Prob\{\mathbf{R}(i,j) = 1\}.$$

GOAL: β_i and $V(i,j)$.

Use Maximum Likelihood Estimation(MLE).

$$\begin{aligned}
\xi_i^{MLE} &= \arg\max_{\xi} \prod_{j=1}^{N} P_{ij}^{R(i,j)} (1 - P_{ij})^{1-R(i,j)} \\
&= \arg\max_{\xi} \sum_{j=1}^{N} R(i,j) log(P_{ij}) + (1 - R(i,j)) log(1 - P_{ij}) \\
&= \arg\max_{\xi} \sum_{g=1}^{K} [r_{ig} log P_i(\theta_g) + (f_g - r_{ig}) log(1 - P_i(\theta_g))] \quad (4)
\end{aligned}$$

Estimating sensitivity $\xi_i = (\alpha_i, \beta_i)$ when $\overrightarrow{\theta} = (\theta_1, \ldots, \theta_N)$ is unknown.

Use Expectation Maximization (EM) method.

E-Step: Compute $E[f_g]$ and $E[r_{ig}]$ as follows:

$$E[f_g] = \overline{f_g} = \sum_{j=1}^{N} P(\theta_g | R^j, \overrightarrow{\xi})$$

$$E[r_{ig}] = \overline{r_{ig}} = \sum_{j=1}^{N} P(\theta_g | R^j, \overrightarrow{\xi} \times R(i,j)).$$

M-Step: Estimate $\overrightarrow{\xi}$ with the values of $\overline{f_g}$ and $\overline{r_{ig}}$.

Calculating the Posterior Probability of Attitudes

$$P(\theta_j|R^j, \overrightarrow{\xi}) = \frac{P(R^j|\theta_j, \overrightarrow{\xi})g(\theta_j)}{\int P(R^j|\theta_j, \overrightarrow{\xi})g(\theta_j)d\theta_j}$$

By partitioning user attitude into different groups, we can transform the $\int$ to $\sum$ as show below:

$$P(\theta_j|R^j, \overrightarrow{\xi}) = \frac{P(R^j|X_t, \overrightarrow{\xi})g(X_t)}{\sum_{t=1}^{K} P(R^j|X_t, \overrightarrow{\xi})g(X_t)}$$

In this formula, K is the number of groups of user attitudes, and user attitudes are partitioned into points $\{X_1, X_2, \ldots, X_K\}$. $A(X_t)$ is the attribute probability value determined by X_t and $\sum_{t=1}^{K} A(X_t) = 1$.

Computation of Visibility

Estimating $\overrightarrow{\theta}$ by:

$$\overrightarrow{\theta^{MLE}} = \arg\max_{\xi} \sum_{i=1}^{n} [R(i,j) log P_{ij} + (1 - R(i,j)) log(1 - P_{ij})]$$

And then,

$$V(i,j) = P_{ij} = Prob\{R(i,j) = 1\} = \frac{1}{1 + e^{-\alpha_i(\theta_j - \beta_i)}}$$

A naive privacy score computation method

Naive computation of Sensitivity:

$$\beta_i = \frac{N - |R_i|}{N}$$

$|R_i|$ is the number of users who set item i as visible.

Naive computation of Visibility:

$$P_{ij} = \frac{|R_i|}{N} \times \frac{|R^j|}{n}$$

Experiment results

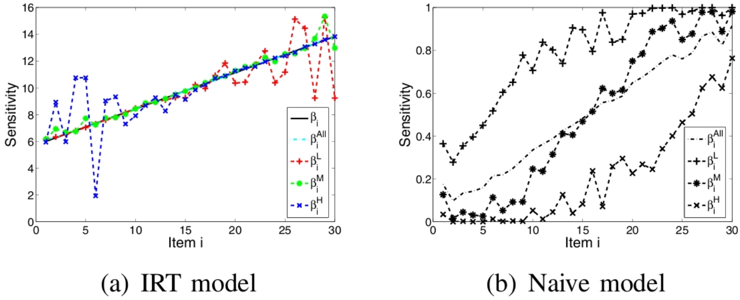

Figure 2. Testing the group-invariance property of item parameter estimation using IRT (Figure 2(a)) and Naive (Figure 2(b)) models.

Weakness of this paper

1. This paper fails to explicitely consider the effects of social graph.
2. This paper doesn't consider the balance between privacy and utility. Utility here is not clearly defined.

The End, Thanks!