Exploiting Vulnerability to Secure User Privacy on a Social Networking Site

Pritam Gundecha
Geoffrey Barbier
Huan Liu
Vulnerability

- Whether an individual is vulnerable or not depends on himself as well as his friends (or his social networks).
- Malicious individuals or groups may take advantage of openness and naivety of users by exploring vulnerability.
- Such exploration can cause physical and emotional distress to users, sometimes with dire consequences.
- Many a time, a user is unaware that he poses a threat to his friends or one of his friends does so.
- We are interested to know (1) how vulnerable a user is and (2) how we can find our vulnerable friends.
Importance to a Social Networking Site

• Users share a large amount of personal information through profile, status updates, messages, comments, etc.

• Not only a user but his friends also have responsibility to protect their privacy.
  – When a user shares personal information with friends, she implicitly places a certain degree of trust.

• User privacy depends on both individual attributes and community attributes
  – Individual attributes: gender, birth-date, phone number, address, etc.
  – Community attributes: photo tagging, wall interactions, friends trace, etc.
Main Questions

• Are there vulnerable friends on a social networking site? Why is it important to find them?
• How to define vulnerable users and find them?
• What measures can one take for effective protection?
• What is the impact of new friends on the vulnerability of a user? Or can we trust a new user?
• Can we make users less vulnerable without suggesting fundamental changes to its architecture?
User privacy on social networking sites is an active area of research in recent years (e.g., [Narayanan et al.'08, ’09], [Wondracek et al.’10], [Krishnamurthy et al.’10], [Squicciarani et al.’09], [Fang et al.’10], [Zhelva et al.’09], [Baden et al.’09]).

Most approaches either suggest the fundamental changes to social networking site’s existing architecture or try to show how vulnerable users are on social networking sites.

Our work identifies vulnerable friends of a user, and provide a mechanism to help secure users without suggesting any fundamental changes to social networking sites.
I-Index (Individual Index)

- It estimates how much risk to privacy a user can have by allowing individual attributes to be visible to other users

I-index for user, \( u \), is given by,

\[
I_u = F(A_u) = \frac{\sum_{i=1}^{n} w_i \cdot a_{u,i}}{\sum_{i=1}^{n} w_i}
\]
C-Index (Community Index)

- It estimates how much threat a user can pose to their friends by making community attributes visible to their users.

\[ C_u = G(B_u) = \frac{\sum_{i=1}^{m} \log(b_{u,i})}{c \times m} \]
• It estimates how public a user is on a social networking site

• P-index of a user, \( u \), is given by,

\[
P_u = \alpha \cdot I_u + (1 - \alpha) \cdot C_u,
\]

where \( \alpha \in [0,1] \)
V-index (User Vulnerability)

It estimates how vulnerable a user is on a social networking site.

V-index of a user, $u$, is given by,

$$V_u = J(P_u, P_{R_u}) = \frac{P_u + \sum_{i \in R_u} P_i}{|R_u| + 1},$$

where $R_u$ is the set of friends of user $u$. 

\[\sum\]
Relationships among Indexes

C-index + I-index

V-index + P-index
A vulnerable friend of a user is defined as a friend whose removal (unfriending) will lower the V-index score of a user.

The V-index of a user, $u$, upon removing the vulnerable friend, $v$, is given by

$$V_u' = \frac{P_u + \sum_{i \in R_u - \{v\}} P_i}{|R_u|},$$

and

$$V_u' < V_u.$$
K-Vulnerable Friends

- $k$-vulnerable friends of a user are $k$ friends whose removal (unfriending) will lower the V-index score of a user.

The V-index of a user, $u$, upon removing the $k$-vulnerable friends, $v_1, v_2, \ldots, v_k$, is given by

$$V_u' = \frac{P_u + \sum_{i \in R_u \setminus \{v_1, \ldots, v_k\}} P_i}{|R_u| + 1 - k},$$

and

$$V_u' < V_u$$
Performance Comparisons for Unfriending

(a) Most Vulnerable Friend
(b) Least V-Friend
(c) Random Friend
(d) Max V-Friend
Comparing Unfriending Schemes with M1

(a) Least V-Friend

(b) Random Friend

(c) Max V-Friend

(d) 2 Most Vulnerable Friends
Impact of New Friends

(a) C-attributes are not visible

(b) C-attributes are visible
Conclusions

• We propose a feasible approach to a novel problem of identifying a user’s vulnerable friends, which allows for experimenting with various scenarios.
• Privacy related efforts have concentrated on protecting mainly individual attributes.
  – Users can be vulnerable through community attributes.
• Unfriending vulnerable friends can help protect users against security risks.
• Less vulnerable users can become more vulnerable if they are not cautious when making new friends.
Future Work

• Many further directions to pursue. Some examples below.
• Can removing vulnerable friends from a user’s network decrease the utility of a social networking site?
• Can we suggest alternative/optimal strategies for unfriending vulnerable friends?
• What will be the impact of $K$-hop or fringe users on a user’s vulnerability?
• Exploring the tradeoff between a user’s degree of risk aversion and his public exposure.
Acknowledgments: We thank Dr. G. Fung for the data, and DMML members and anonymous reviewers for their comments. This work is, in part, supported by ONR and AFOSR.