Exploiting Vulnerability to Secure User Privacy on a Social Networking Site

Pritam Gundecha
Arizona State University
699 South Mill Avenue
Tempe, AZ 85281
pritam@asu.edu

Geoffrey Barbier
Arizona State University
699 South Mill Avenue
Tempe, AZ 85281
gbarbier@asu.edu

Huan Liu
Arizona State University
699 South Mill Avenue
Tempe, AZ 85281
huan.liu@asu.edu

ABSTRACT

As social network expands, a user's privacy protection goes beyond his privacy settings and becomes a social networking problem. In this research, we aim to address some critical issues related to privacy protection: Would the highest privacy settings guarantee a secure protection? Given the open nature of a social networking sites, is it possible to manage one's privacy protection? With the diversity of one's social media friends, how can one figure out an effective approach to balance between vulnerability and privacy? We present a novel way to define a vulnerable friend from an individual user's perspective is dependent on whether or not the user's friends' privacy settings protect the friend and the individual's network of friends (which includes the user). As a single vulnerable friend in a user's social network might place all friends at risk, we resort to experiments and observe how much security an individual user can improve by unfriending a vulnerable friend. We also show how privacy weakens if newly accepted friends are unguarded or unprotected. This work provides a large-scale evaluation of new security and privacy indexes using a Facebook dataset. We present and discuss a new perspective for reasoning about social networking security. When a user accepts a new friend, the user should ensure that the new friend is not an increased security risk with the potential of negatively impacting the entire friend network. Additionally, by leveraging the indexes proposed and employing new strategies for unfriending vulnerable friends, it is possible to further improve security and privacy without changing the social networking site's existing architecture.

Categories and Subject Descriptors

H.2.7 [**Information Systems**]: Security, integrity, and protection; J.4 [**Social and Behavioral Sciences**]: Sociology

General Terms

Security, Experimentation

KDD'11, August 21–24, 2011, San Diego, California, USA.

Keywords

Vulnerability, Social network, Privacy

1. INTRODUCTION

Social media [7] gives users an efficient way to communicate and network with one another on an unprecedented scale and at rates unseen in traditional media. The popularity of social media has grown exponentially resulting in evolution of social networking sites, blogs, micro-blogs, location-based social networks, wikis, social bookmarking applications, social news, media (photo, audio and video) sharing, product and business review sites, etc.

A *social networking site* [3] is a web-based service that allows web users to publish a public or semi-public profile within a bounded system, divulge a network of friends with whom they share a connection, and explore other users' profiles and friend networks. Networking through social networking sites is becoming a popular means for users to express feelings, communicate information, share thoughts, and collaborate. Social networking sites have reshaped business models [19], provided platform for communities to grow [18, 17], stimulated viral marketing [16, 9], provided trend analysis and sales prediction [15], and can be a grass-roots information source [5].

An individual user can share a large amount of personal and sometimes sensitive information with friends on a social networking site through the user's profile, status updates, messages, and status replies. Depending on individual choice, the user profile can reveal personal information to friends such as gender, birth date, relationship status, e-mail address, phone number, home address, and even political or religious affiliations. This puts an implicit responsibility on a user's social networking friends to keep shared information private and honor the implicit, and sometimes explicit, trust placed in friends by the user.

All social networking sites provide profile users a range of privacy settings to protect their personal information. These settings are often confusing and many times not well communicated to all users. Users can face a breach of privacy, unless these settings are properly used. In some cases, users' profiles are completely public, making information available and providing a communication mechanism to anyone who wants it. It is no secret that when a social networking profile is public, malicious individuals including stalkers, spammers, and hackers, can use sensitive information for their personal gain. Sometimes malevolent users can even cause physical or emotional distress to other users [13]. For example, Facebook's founder is a victim of stalking and has

publicly admitted to emotional distress[1]. It is interesting to consider whether or not a completely public profile is the only risk to personal information on a social networking site. In this paper, we show that privacy settings alone are not enough to protect privacy and achieve a high level of security. Profile users can also face a breach of privacy if their friends abuse their trust. Most social networking sites do not provide adequate means to protect trust between users and their friends.

Many times social networking users are unaware that they are a threat to their friends because they are *vulnerable*. Three factors can contribute to the reduction of user's vulnerability. First, user's privacy settings are enough to protect their personal information. Second, a user has adequate means to protect their friends. Third, a user's friends must have intentions to protect the user. As we draw parallels between users and their friends, we are intrigued by questions like how vulnerable users are, how to find their vulnerable friends, what are effective mechanisms that could make users less vulnerable?

Besides helping users of a social networking site become less vulnerable, this study of vulnerability is motivated by the desire to better understand the dynamics of social networks from a security and privacy perspective. Ultimately, this may help social networking sites become more trustworthy as a medium to exchange ideas and information, better enabling sites to connect people, simplify communications, and to help them stay in touch reliably and securely.

In this paper, we address a novel problem of identifying *vulnerable friends* on a social networking site and investigate related issues and challenges. Specifically, we work to resolve the following questions:

- Are there vulnerable friends on a social networking site? Why is it important to find vulnerable them?
- What measures should be used to define vulnerable friends?
- How can a user identify his vulnerable friends? What measures can he take for effective protection?
- What is the impact of each new friend on the vulnerability of a user? Can we trust a new user?
- What role does a social networking site play towards making users less vulnerable? Is it possible to further improve security and privacy without suggesting fundamental changes to the social networking site's existing architecture?

In Section 2, we study the statistics collectible from a social networking site and define the problem of identifying vulnerable friends. We propose a methodology and measures for evaluating whether or not a user is vulnerable and how to adjust a user's network to best deal with threats presented by vulnerable friends. In Section 3, we conduct an empirical study to evaluate methods that can be manipulated to make users less vulnerable, compare the performance of an optimal algorithm with that of intuitive heuristic methods, and discuss the approach can be used to assess the impact of new friends to a user's network. We review the literature highlighting the novelty of this effort in Section 4. Finally, we discuss possible future work in Section 5.

[1]http://www.tmz.com/2011/02/07/mark-zuckerberg-restraining-order-facebook-social-network-santa-clara-county-stalker-letters-priscilla-chan/

2. VULNERABLE FRIENDS

Attributes available for every user on a social networking site can be categorized into two major types: *individual attributes* and *community attributes*. Individual attributes characterize individual user information, including personal information such as gender, birth date, phone number, home address, etc. Community attributes characterize information about friends of a user, including friends that are traceable from a user's profile (i.e., a user's friends list), tagged pictures, wall interactions, etc. Both types of attributes are always accessible to friends but may not to other users. Using privacy settings of a profile, a user can control the visibility of most individual attributes, but cannot control the visibility of most community attributes. For example, Facebook users can control traceable link information about friends but cannot control exposure of friends through photo tagging and wall interactions.

On most social networking sites, privacy related efforts have been concentrated on protecting individual attributes only. Thus, users are often left vulnerable through community attributes. We propose a mechanism that enables users to protect against vulnerability. The mechanism is tunable to accommodate individual preferences across the spectrum, from reclusive users to gregarious users.

A novel way to define a vulnerable friend from an individual user's perspective is dependent on whether or not the user's friends' privacy settings protect the friend and the individual's network of friends (which includes the user). *An individual is vulnerable if any friend in the network of friends has insufficient privacy settings to protect the entire network of friends.* Thus, whether or not an individual reciprocates privacy settings with their friends within a friend network can impact the entire network. Before presenting a formal definition of vulnerable friends, we propose four indexes, I-index, C-index, P-index, and V-index, based on individual and community attributes for each user on a social networking site. These indexes can be used to estimate user's privacy, quantify how well a user protects friends, specify how public or private user profiles are, and compute the vulnerability of individual users on a social network.

2.1 I-Index

I-index (Individual index): I-index estimates how much risk to privacy a user can incur by allowing individual attributes to be accessible or visible to other users. A user who ignores or is unaware of privacy settings is a threat to self. I-index is defined as a function of individual attributes (I-attributes). Let n be the total number of I-attributes available via a social networking site profile. I-index for a user u is given by

$$I_u = F(A_u), \tag{1}$$

where $I_u \in [0,1]$, $A_u = \{a_{u,i} : a_{u,i} = \{0,1\}; 1 \leq i \leq n\}$ is I-attribute set for user u and $a_{u,i}$ is a status of a i-th I-attribute for user u. $a_{u,i} = 1$ indicates user u has enabled i-th I-attribute to be visible otherwise non-visible (may be sensitive for a user).

Table 1 shows statistics of commonly found I-attributes on the Facebook (Refer to Section 3.1 for details on Facebook dataset consists of 2,056,646 users). The last column

in the table lists the percentage of people who enable the particular attribute to be visible. For example, 7,430 (0.36%) Facebook users enabled their mobile phone numbers to be visible. We define the sensitivity (weight), of an attribute as a percentage of non-visibility. Hence, the sensitivity of a mobile phone number according to our Facebook dataset is 99.64. This means that users do not usually disclose their mobile phone number to other users. Users that do disclose phone numbers have a propensity to vulnerability because they disclose more sensitive information in their profiles.

Attributes	User Count	Percentage (%)
Total users	2,056,646	
I-attributes:		
Current City	620,401	30.17
Hometown	727,674	35.38
Gender	1,681,673	81.77
Birthday	67,834	3.30
Relationship status	539,612	26.24
Siblings	244,658	11.90
Education and work	516,848	25.13
Like and interests	1,369,080	66.57
Email	27,103	1.32
Mobile number	7,430	0.36
Website	128,776	6.26
Home address	7,580	0.37
Political Views	24,438	1.19
Religious Views	33,036	1.61
Children	86,609	4.21
Networks	284,482	13.83
Parents	73,887	3.49
Bio	199,070	9.68
Interested in	383,724	18.66
Looking for	449,498	21.86
Music	941,340	45.77
Books	281,346	13.68
Movies	574,243	27.92
Television	684,843	33.30
Activities	385,417	18.74
Interests	308,229	14.99
C-attributes:		
Friends trace (link)	1,481,472	72.03

Table 1: Attributes statistics on the Facebook

We used normalized weighted average to estimate I-index. I-index for each profile user u is given by,

$$I_u = F(A_u) = \frac{\sum_{i=1}^{n} w_i * a_{u,i}}{\sum_{i=1}^{n} w_i}, \quad (2)$$

where w_i is the sensitivity (weight) of an i-th I-attribute and $a_{u,i} = 1$ if i-th I-attribute is visible otherwise the attribute is not visible (i.e., sensitive to user u). $I_u \in [0, 1]$. $I_u = 1$ indicates user u has marked all I-attributes to be visible. On the other hand, $I_u = 0$ indicates user u has marked all I-attributes to be non-visible.

2.2 C-Index

C-index (Community index): C-index quantifies how much threat a user can pose to their friends by making community attributes accessible or visible to other users. Users who ignore and are unaware of privacy settings of community attributes can create risk to the entire community of friends. C-index is defined as a function of community attributes (C-attributes). Let m be the total number of C-attributes possible on a social networking site. C-index for a user u is given by

$$C_u = G(B_u), \quad (3)$$

where $C_u \in [0, 1]$, $B_u = \{b_{u,i} : b_{u,i} \in N; 1 \leq i \leq m\}$ is C-attributes set for user u, $b_{u,i}$ indicates the number of friends affected when a corresponding C-attribute is manifested, and N is the set of positive integers. We ignore attributes marked as non-visible. Our Facebook dataset has only one C-attribute (see Table 1) which suggests how many friends are traceable (via a friend relationship) from an individual user. 1,481,472 (72.03%) Facebook users in our dataset allowed friends to trace to other users. Thus, a large portion of users are *either not careful or not aware of the privacy concerns of their friends.*

A vulnerable user u can pose threat to his friends and the amount of the threat increases with the number of friends that are put at risk. However, the rate of the increment decreases as more friends are put at risk. To appropriately represent this threat change, we choose a convex, non-decreasing log function to estimate the threat for each user based on the number friends placed at risk by each C-attribute. Hence, C-index for a user u is calculated as

$$C_u = G(B_u) = \frac{\sum_{i=1}^{m} \log(b_{u,i})}{4 * m}, \quad (4)$$

where constant 4 is chosen because $C_u \in [0, 1]$ and none of the Facebook users in our dataset has more than 10^4 friends. $C_u > 0$ indicates user u has allowed everyone to trace friends through their own profile. On the other hand, $C_u = 0$ indicates that all the friends (except one) of a user u are non-traceable through a profile.

Figure 1(a) shows I-index and C-index for randomly chosen 100K Facebook users. Note that users are sorted in ascending order of their I-indexes. The X-axis and Y-axis indicate users and their corresponding I and C-index values, respectively.

2.3 P-index

P-index (Publicity/Visibility index): P-index shows how public (visible) or private (non-visible) a user is on a social networking site. This index also indicates how much an individual user aims to protect self as well as their friends. P-index is defined as a function of I-index and C-index. In other words, it is a function of I-attributes and C-attributes. P-index of a user u is given by

$$P_u = H(F(A_u), G(B_u)), \quad (5)$$

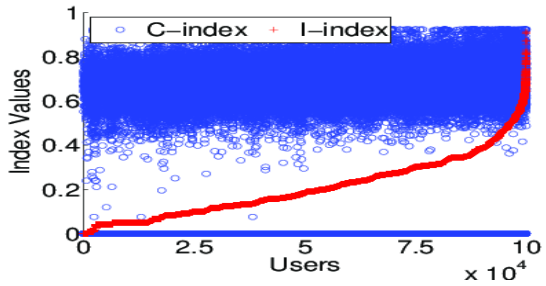
where $P_u \in [0, 1]$. We choose a simple, weighted average function to calculate P-index for each Facebook user in our dataset.

$$P_u = \alpha * F(A_u) + (1 - \alpha) * G(B_u), \quad (6)$$

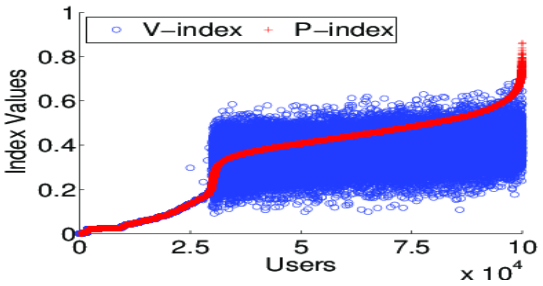
where $\alpha \in [0, 1]$. Substituting Eq(6) with Eq(2) and Eq(4), we get

$$P_u = \alpha * \frac{\sum_{i=1}^{n} w_i * a_{u,i}}{\sum_{i=1}^{n} w_i} + (1 - \alpha) * \frac{\sum_{i=1}^{m} \log(b_{u,i})}{4 * m} \quad (7)$$

Different users may have different priorities about friends and may have different perspectives about vulnerability. Tunable parameter α can be set to address the needs of different



(a) I-index (red) and C-index (blue) for each User.



(b) P-index (red) and V-index (blue) for each User.

Figure 1: Relationship among index values for each User.

users. For example, one may choose $\alpha < 0.5$ to deemphasize the individual attributes' visibility; or one may choose $\alpha > 0.5$ to emphasize the individual attributes' visibility. For our experiments, we set $\alpha = 0.5$ to put equal weights to individual and community attributes.

2.4 V-index

V-index (Vulnerability index): V-index shows how vulnerable a user is on a social networking site. Thus far, we have provided three indexes, I-index, C-index, and P-index, for a user based on the visibility of I-attributes and C-attributes. On a social networking site, vulnerability of a user depends on privacy settings of self, friends, their friends, and so on. Intuitively, as the distance between a user and other users on a social networking site increases, the marginal risk of vulnerability decreases rapidly the further away a user is from a vulnerable user. Hence, we only consider a user and friends in estimating the vulnerability of a user. V-index of a user depends on the P-indexes of a user's friends and the user's P-index. V-index of a user u is defined as:

$$V_u = J(P_u, P_{R_u}), \tag{8}$$

where R_u is the set of friends of user u and $V_u \in [0, 1]$. A simple, weighted average function is used to calculate V-index for each user,

$$V_u = \frac{P_u + \sum_{i \in R_u} P_i}{|R_u| + 1} \tag{9}$$

P-index, P_u, of user u is also part of the V-index, V_u.

Figure 1(b) shows the P-index and V-index for 100K randomly chosen users (the same users chosen for Figure 1(a)). Note that users are sorted according to P-index. The X-axis and Y-axis indicate users and their index values respectively.

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

$$V'_u = \frac{P_u + \sum_{i \in R_u - \{v\}} P_i}{|R_u|} \tag{10}$$

By definition of a vulnerable friend

$$V'_u < V_u \tag{11}$$

By substituting Eq(11) with Eq(9) and Eq(10), we can prove that

$$V_u < P_v \tag{12}$$

This means that the P-index of a vulnerable node is always greater than V-index of a user before unfriending.

The definition of vulnerable friends can be generalized to 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 k vulnerable friends $v_1, v_2, \cdots, v_k$ is given by

$$V'_u = \frac{P_u + \sum_{i \in R_u - \{v_1, \cdots, v_k\}} P_i}{|R_u| + 1 - k} \tag{13}$$

By definition of k-Vulnerable friends

$$V'_u < V_u \tag{14}$$

By substituting Eq(14) with Eq(9) and Eq(13), we can prove that

$$V_u < \frac{\sum_{i \in \{v_1, \cdots, v_k\}} P_i}{k} \tag{15}$$

This means that the average P-index of k-vulnerable nodes is always greater than V-index of a user before unfriending.

Having formulated the problem of identifying vulnerable friends, we now demonstrate the results in next section.

3. FURTHER STUDY AND EXPERIMENTS

The proposed methods are demonstrated in practice through experiments using a dataset derived from a real social networking site. The proposed experiments address the challenge of identifying vulnerable friends. With an approach for identifying vulnerable friends, we set out to investigate the following issues:

- How effective are the P-index and V-index measures in reducing vulnerability of users? How effective is random unfriending in reducing vulnerability of users?
- What is an effective way of reducing one's vulnerability?
- Do the indexes address the dynamics of social networks? We study the impact of new friend request and its effect on vulnerability of a user.

In the next sections, we set out to use the proposed index estimation methods in an empirical study, attempt to experimentally address these issues, report preliminary results, and suggest new lines of research in finding vulnerable users.

3.1 Data Collection

Facebook users can create a profile containing personal and sometimes sensitive information. Users add other users as friends to facilitate social activity with friends. Users may also join groups organized by workplace, school, college, or other interests. As of July 2010, Facebook registered more than half billion active users[2] who returned to the site in last 30 days. To put that number in perspective, this makes Facebook users the third largest in "population" behind China (1.33 billion) and India (1.15 billion). This "population" will soon be twice the population of the United States (307 million). Facebook experiences web traffic data from 130 million[3] unique United States visitors a month. In January 2010, the amount of time the average person spent on Facebook jumped to more than seven hours per day[4]. This statistic suggests that the amount of personal information available on Facebook is richer than any other social networking site. Thus we chose a Facebook dataset for our experiments.

Facebook dataset (100K users)	Count
Non-traceable user profiles	30,391
Avg. actual friends per user	488
Avg. crawled friends per user	42
Max. actual friends per user	4,998
Min. actual friends per user	1
Max. crawled friends per user	1,590
Min. crawled friends per user	0

Table 2: Facebook dataset statistics for randomly selected 100K users from 2M+ users

The Facebook dataset is created by crawling Facebook user profiles. The dataset contains profile information for 2,056,646 users. Profile information includes attribute information for users such as age, gender, mobile phone number, address, etc. For convenience, 100K Facebook users were randomly selected from the dataset for the experiments. The findings are validated using all 2M+ users. Table 2 shows statistics for randomly selected 100K users. Out of these 100K users, around 30K users mark friends non-traceable from their profiles. The average Facebook user has 130[5] friends but our data set shows 488 actual friends per user. The dataset contains profile information for 42 friends (crawled friends) per user on average. The difference between the actual friends and crawled friends does not affect the methodology. Figure 2 shows relationships between actual friends (A-friends) and crawled friends (C-friends).

3.2 Identifying Vulnerable Friends

For the first set of experiments, we compare V-index for each of user with two optimal algorithms and six intuitive strategies for unfriending to reduce vulnerability. For each graph in Figure 3, the X-axis and Y-axis indicate users and their V-index values, respectively. For simplicity, we sort all users in ascending order based on existing V-index, and then we plot their corresponding V-index before and after unfriending. Figure 3 indicates performance of all eight algorithms which will help us to decide whether unfriending makes users more or less vulnerable. The eight algorithms are,

[2]http://www.facebook.com/press/info.php
[3]http://www.quantcast.com/facebook.com
[4]http://mashable.com/2010/02/16/facebook-nielsen-stats/
[5]http://www.facebook.com/press/info.php?statistics

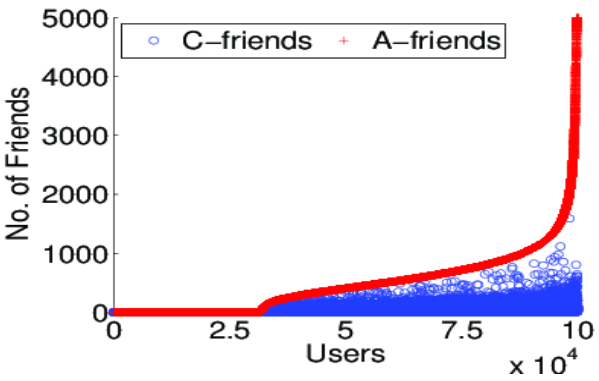


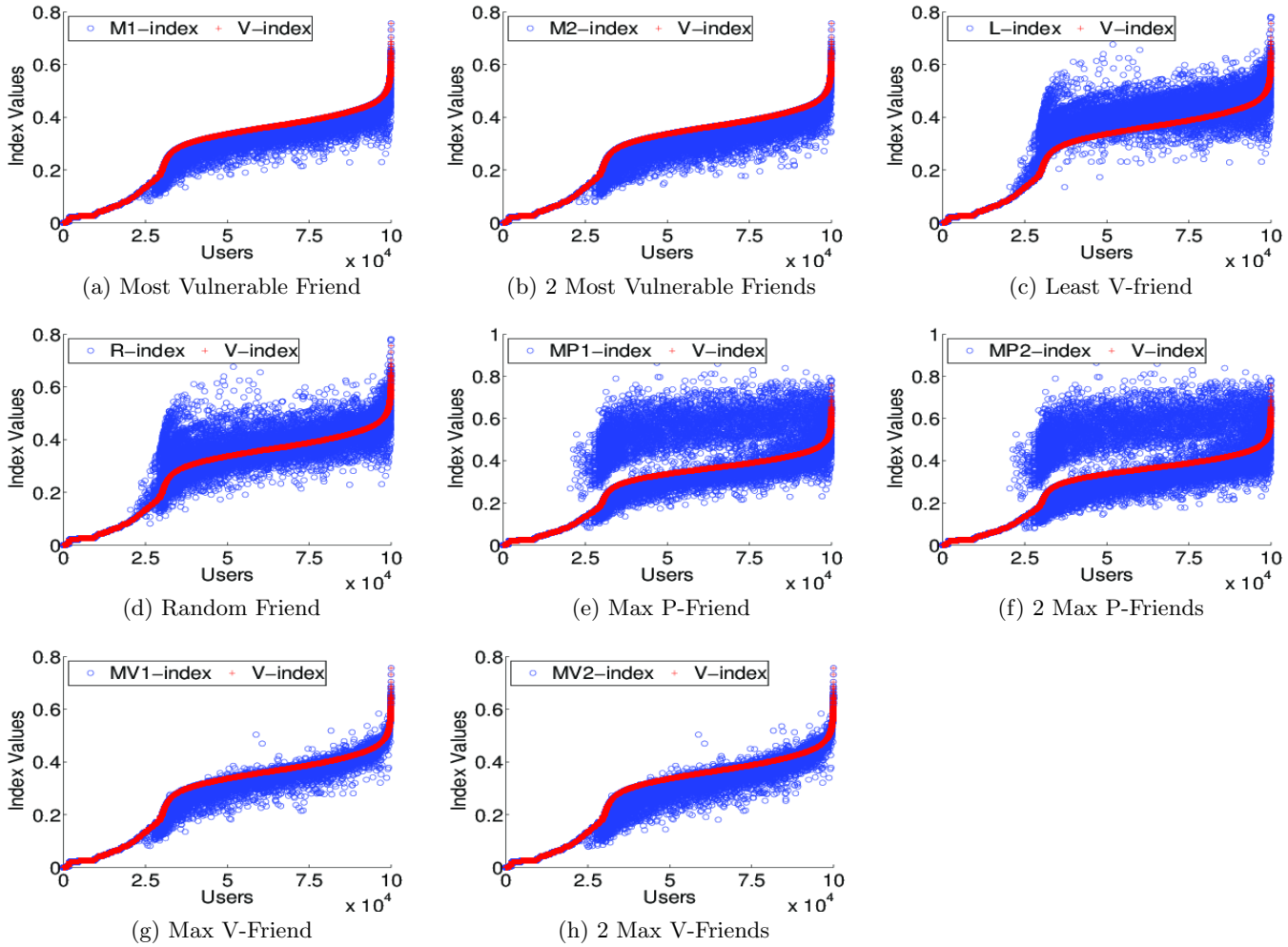
Figure 2: Actual (red) and crawled friends (blue)

- *Most vulnerable friend.* For a user, the most vulnerable friend is the one whose removal lowers the V-index score the most. For each user, we first find the most vulnerable friend and then estimate the new V-index value (M1-index) after unfriending him/her. As expected, see Figure 3(a), V-index values for users decrease in comparison with V-index values before unfriending the most vulnerable friend. Unfriending the most vulnerable friend makes all users more secure.

- *Two most vulnerable friends.* If we sort all of user's vulnerable friends in ascending order based on their new V-indexes (after unfriending), the top two in the list are the two most vulnerable friends. For each user, we first find two most vulnerable friends and then estimate the new V-index value (M2-index) after unfriending them. As expected, see Figure 3(b), V-index values for all users decrease in comparison with V-index values before unfriending the two most vulnerable friends. Unfriending the two most vulnerable friends also make all users more secure.

- *Least V-friend.* For each user, we choose to unfriend the friend whose V-index is the lowest among all friends. This friend is the least V-friend. V-index values increase for 65% of 100K users, and increase for 43% of the 2M+ users, in comparison with V-index values before unfriending the least V-friend. See Figure 3(c), L-index refers to the new V-index value after unfriending the least V-friend. $V'_u > V_u$ for some users because, $P_l < V_u$ where P_l is the P-index of the least V-friend. Unfriending the least V-friend does not make all users insecure.

- *Random friend.* For each user, we randomly choose to unfriend a friend. V-index values increase for 24% of 100K users, and increase for 23.5% of the 2M+ users, in comparison with V-index values before unfriending a random friend. See Figure 3(d), R-index refers to the new V-index value after unfriending a random friend. $V'_u > V_u$ because $P_r < V_u$, where P_r is the P-index of the random friend. Unfriending a random friend does not make all users secure.



(a) Most Vulnerable Friend (b) 2 Most Vulnerable Friends (c) Least V-friend

(d) Random Friend (e) Max P-Friend (f) 2 Max P-Friends

(g) Max V-Friend (h) 2 Max V-Friends

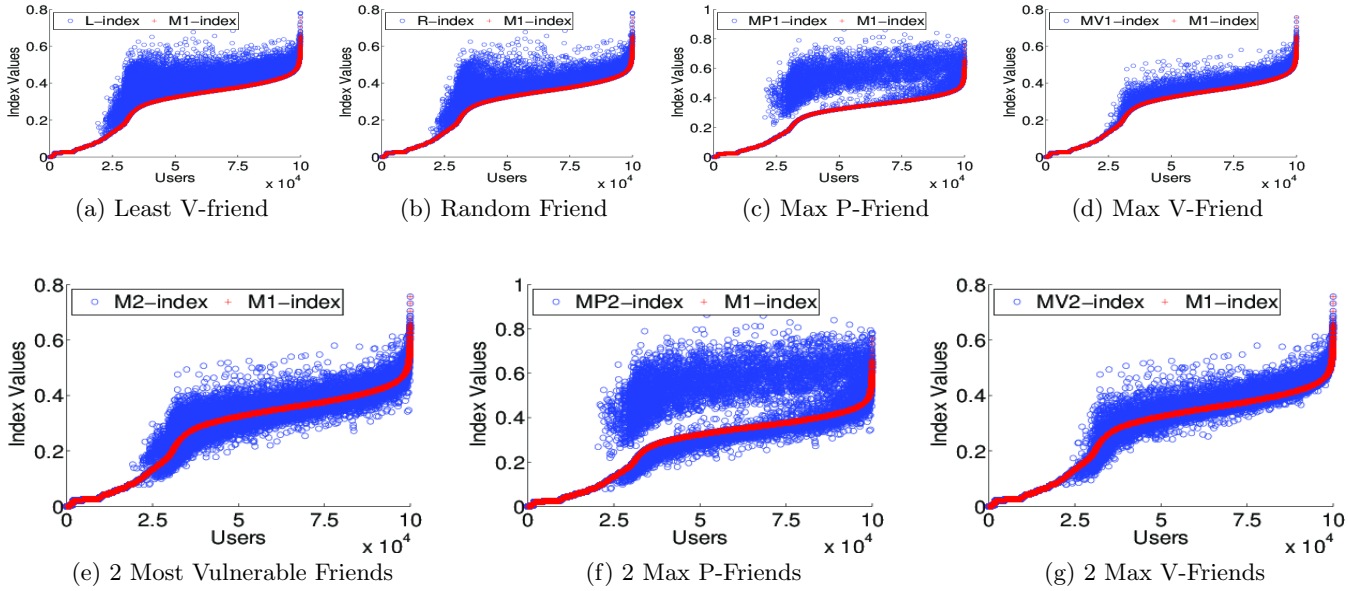
Figure 3: Performance comparisons of V-indexes for each user before (red) and after (blue) unfriending based on eight different algorithms.

- *Max P-friend.* For each user, we choose to unfriend a friend whose P-index is the highest among all friends. V-index values increase for 5% of 100K users, and increase for 11% of the 2M+ users, in comparison with V-index values before unfriending the max P-friend. See Figure 3(e), MP1-index refers to the new V-index value after unfriending the max P-friend. $V'_u > V_u$ for some users because $P_{mp_1} < V_u$, where P_{mp_1} is the P-index of the max P-friend. Unfriending the max P-friend makes a majority of users more secure.

- *Two max P-friend.* For each user, we choose to unfriend two friends whose P-index is the highest and second highest among all friends. V-index values increase for 5% of 100K users, and increase for 11% of the 2M+ users, in comparison with V-index values before unfriending the two max P-friends.See Figure 3(f), MP2-index refers to the new V-index value after unfriending the two max P-friend. $V'_u > V_u$ for some users because $(P_{mp_1} + P_{mp_2})/2 < V_u$, where P_{mp1_1} and P_{mp_2} are P-indexes of the two max P-friends. Unfriending the two max P-friends makes a majority of users more secure.

- *Max V-friend.* For each user, we choose to unfriend a friend whose V-index is the highest among all friends. V-index values increase for 3.6% of 100K users, and increase for 5% of the 2M+ users, in comparison with V-index values before unfriending max V-friend. See Figure 3(g), MV1-index refers to the new V-index value after unfriending the max V-friend. $V'_u > V_u$ for some users because $P_{mv_1} < V_u$, where P_{mv_1} is the P-index of the max V-friend. Unfriending the max V-friend makes a majority of users more secure.

- *Two max V-friend.* For each user, we choose to unfriend two friends whose V-index is the highest and second highest among all friends. V-index values increase for 2.5% of 100K users, and increase for 5% of the 2M+ users, in comparison with V-index values before unfriending the two max V-friends. See Figure 3(h), GV2-index refers to the new V-index value after unfriending the two max V-friends. $V'_u > V_u$ for some users because $(P_{mv_1}+P_{mv_2})/2 < V_u$, where P_{mv_1} and P_{mv_2} are P-indexes of the two max V-friends. Unfriending the two max V-friends make a majority of users more secure.



(a) Least V-friend (b) Random Friend (c) Max P-Friend (d) Max V-Friend

(e) 2 Most Vulnerable Friends (f) 2 Max P-Friends (g) 2 Max V-Friends

Figure 4: Performance comparisons of unfriending the most vulnerable friend (red) with seven different unfriending ways (blue).

In the second set of experiments, we compare the performance of unfriending most vulnerable friends with the seven intuitive unfriending strategies. For each graph in Figure 4, the X-axis and Y-axis indicate users and their associated V-index values after unfriending, respectively. We sort all users in ascending order based on V-index values after unfriending the most vulnerable friend and then plot corresponding V-index based on different unfriending strategies. We find unfriending the most vulnerable friend makes users more secure.

As expected, see Figure 4(a)-4(d), V-index values for each user based on unfriending the least V-friend, a random friend, the max P-friend, or the max V-friend increase for all users in comparison with their V-index values after unfriending the most vulnerable friend. In the case of unfriending the least V-friend, V-index values increase for 3% of users in comparison with the most vulnerable friend unfriending. Similarly, 1.7% of users increase for a random friend unfriending, 1.7% of users increase for the P-friend unfriend, and 1% of users increase for the V-friend unfriending. Thus, unfriending the most vulnerable friend makes all users more secure than all other schemes.

V-index values for each user based on unfriending the two most vulnerable friends, see Figure 4(e), do not decrease for 10% of 100K, and 21% of 2M+ users, in comparison with V-index values after unfriending the most vulnerable friend. V-index values for each user based on unfriending the two max P-friend, see Figure 4(f), do not decrease for 51% of 100K, and 81% of 2M+ users, in comparison with V-index values after unfriending the most vulnerable friend. V-index values for each user based on unfriending the two max V-friend, see Figure 4(g), do not decrease for 90% of 100K, and 75% of 2M+ users, in comparison with V-index values after unfriending the most vulnerable friend.

3.3 Impact of new friends

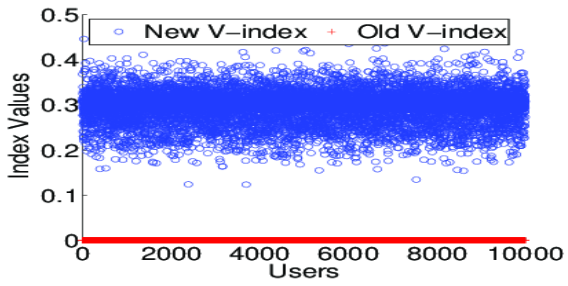
We now investigate the impact of new friendship on two types of secure users from vulnerable users. We select three sets of 10K users from 2M+ Facebook users: (S1) users with high V-indexes, (S2) users with low V-indexes, and (S3) C-attributes enabled users with low V-indexes. We randomly select a vulnerable user (i.e., selected from S1, 10K high V-index users) and a secure user (i.e., selected from S2, 10K low V-index users), and pair them and remove the pair from S1 and S2, respectively, until all 10K users from S1 and S2 are paired. We repeat the same with sets S1 and S3. The two sets of results are shown in Figure 5 (a) and (b). For each graph, the X- and Y-axis indicate users and their V-index values before and after the pairing of new friends, respectively. We sort all users in ascending order based on their old V-indexes. As shown in Figure 5(a), V-indexes of all users of S2 increase significantly and consistently; in Figure 5(b), V-indexes of users of S3 also increase, but vary from minor to large changes. The larger changes in the latter case occur on those users of S3 with fewer friends. The results in Figure 5 confirm that less vulnerable users can become more vulnerable if they are careless when making new friends, and reclusive users are more sensitive to the choice of new friends than less reclusive ones.

3.4 Discussions

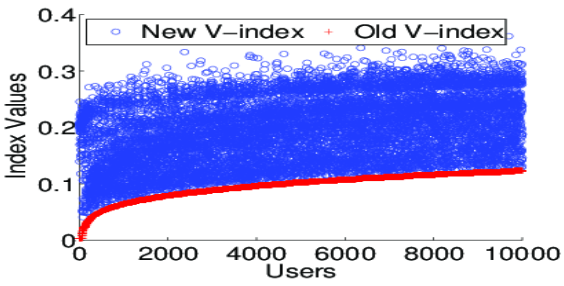
Our experiments demonstrate different strategies for improving a user's privacy on a social networking site. It is possible to tune the index estimation methods for a wide range of individuals, from reclusive users to gregarious users.

- We choose specific functions, F, G, H, and J, to estimate the I-index, C-index, P-index and V-index. If one changes these functions, it will significantly change the criteria used to identify vulnerable friends.

- We set the tunable parameter α to 0.5. Changing the value α based on user preference will significantly change the threshold for identifying vulnerable friends.



(a) C-attributes are not visible



(b) C-attributes are visible

Figure 5: Impact of new friendship (blue) on users with low V-indexes (red) from users with high V-indexes

- Based on our index estimation method, unfriending the most vulnerable friend iteratively for K times should achieve at least the same vulnerability reduction as unfriending most K-vulnerable friends. Using equations 9 and 13, we can prove that additive property does not hold. Hence, unfriending most K-vulnerable friends is better than K iterative removal of most vulnerable friends.

4. RELATED WORK

Work discussed in this paper is about *identifying vulnerable friends of a user at one social networking site* and differs from most previous efforts of securing users privacy on a social networking site.

User privacy on a social networking site has received considerable attention recently. Gross and Acquisti [6] evaluate the amount of information disclosed through a social networking site and study usage of privacy settings. This work revealed that only a few users change the default privacy preferences on Facebook. Narayanan and Shmatikov [11, 12] show that users are not well protected on a social networking site by successfully deannonymizing network data solely based on network topology. They also highlight the fact that privacy laws are inadequate, confusing, and inconsistent amongst nations making social networking sites more vulnerable. Wondracek et al. [20] propose a simple deanonymization scheme which exploits the group membership information to breach users privacy.

Liu and Maes [10] point towards lack of privacy awareness and find large number of social network profiles in which people describe themselves using a rich vocabulary of their passions and interests. This fact strengthen the need for vulnerability research on a social networking site to make users aware of privacy risks. Krishnamurthy and Wills [8] discuss the problem of leakage of personally identifiable information and how it can be misused by third parties [12].

There has been some research which suggests the fundamental changes to social networking sites to achieve user privacy. Squicciarini et al. [14] introduce a novel collective privacy mechanism for better managing the shared content between the users. Fang and LeFevre [4] focus on helping users to express simple privacy settings but they have not considered additional problems such as attribute inference [22], or shared data ownership [14]. Zheleva and Getoor [22] show how an adversary can exploit an online social network with a mixture of public and private user profiles to predict the private attributes of users. Baden et al. [2] present a framework where users dictate who may access their information and based on public-private encryption-decryption algorithms. Although the proposed framework address privacy concerns, it comes at the cost of increased response time from a social networking site. Our work does not suggest any fundamental changes to social networking sites. We find users can secure user privacy by unfriending the vulnerable friends. Unfriending[6] has been studied recently but we are the first one to propose unfriending to reduce the vulnerability of a user.

5. CONCLUSIONS AND FUTURE WORK

We propose a feasible approach to a novel problem of identifying a user's vulnerable friends on a social networking site. Our work differs from existing work addressing social networking privacy by introducing a vulnerability-centered approach to a user security on a social networking site. On most social networking sites, privacy related efforts have been concentrated on protecting individual attributes only. However, users are often vulnerable through community attributes. Unfriending vulnerable friends can help protect users against the security risks. Based on our study of over 2 million users, we find that users are either not careful or not aware of security and privacy concerns of their friends. Our model clearly highlights the impact of each new friend on a user's privacy.

There are vulnerable friends on social networking sites and it is important to find vulnerable friends so that users can improve their privacy and security. Removing vulnerable friends from a user's social network might decrease the utility of the social networking service from a social perspective but this strategy improves security and helps defend privacy. We are also interested in investigating the role of user vulnerability across social networks [21] and relationship between the influential user [1] and vulnerable user.

6. ACKNOWLEDGMENTS

We thank Dr.Gabriel Fung for providing the crawled Facebook dataset for experiments. We also thank the DMML members and anonymous reviewers for their helpful comments. This research was, in part, supported by grants of ONR (N000141010091) and AFOSR (FA95500810132), and AFRL.

[6]http://www.nytimes.com/2010/10/24/fashion/24Studied.html

7. REFERENCES

[1] N. Agarwal, H. Liu, L. Tang, and P. Yu. Identifying the influential bloggers in a community. In *the first ACM International Conference on Web Search and Data Mining (WSDM)*, 2008.

[2] R. Baden, A. Bender, N. Spring, B. Bhattacharjee, and D. Starin. Persona: An online social network with user-defined privacy. *ACM SIGCOMM Computer Communication Review*, 39(4):135–146, 2009.

[3] D. M. Boyd and N. B. Ellison. Social network sites: Definition, history, and scholarship. *Journal of Computer-Mediated Communication*, 13(1):210–230, 2008.

[4] L. Fang and K. LeFevre. Privacy wizards for social networking sites. In *the 19th International World Wide Web Conference (WWW)*, 2010.

[5] R. Goolsby. Social media as crisis platform: The future of community maps/crisis maps. *ACM Trans. Intell. Syst. Technol.*, 1(1):1–11, 2010.

[6] R. Gross and A. Acquisti. Information revelation and privacy in online social networks. In *the ACM workshop on Privacy in the electronic society*, pages 71–80. ACM, 2005.

[7] A. M. Kaplan and M. Haenlein. Users of the world, unite! The challenges and opportunities of Social Media. *Business Horizons*, 53(1):59–68, 2010.

[8] B. Krishnamurthy and C. Wills. On the leakage of personally identifiable information via online social networks. *ACM SIGCOMM Computer Communication Review*, 40(1):112–117, 2010.

[9] J. Leskovec, L. Adamic, and B. Huberman. The dynamics of viral marketing. *ACM Transactions on the Web (TWEB)*, 1(1), 2007.

[10] H. Liu and P. Maes. Interestmap: Harvesting social network profiles for recommendations. *Beyond Personalization*, 2005.

[11] A. Narayanan and V. Shmatikov. Robust de-anonymization of large sparse datasets. In *the 29th IEEE Symposium on Security and Privacy*, 2008.

[12] A. Narayanan and V. Shmatikov. De-anonymizing social networks. In *the 30th IEEE Symposium on Security and Privacy*, 2009.

[13] D. Rosenblum. What anyone can know: The privacy risks of social networking sites. *IEEE Security and Privacy*, pages 40–49, 2007.

[14] A. Squicciarini, M. Shehab, and F. Paci. Collective privacy management in social networks. In *the 18th international conference on World wide web (WWW)*, 2009.

[15] J. Sterne. *Social Media Metrics*. The New Rules of Social Media. John Wiley & Sons Inc., 2010.

[16] M. R. Subramani and B. Rajagopalan. Knowledge-sharing and influence in online social networks via viral marketing. *Communications of the ACM*, 46(12):300–307, 2003.

[17] L. Tang and H. Liu. Relational learning via latent social dimensions. In *the 15th ACM SIGKDD international conference on Knowledge discovery and data mining*, 2009.

[18] L. Tang, H. Liu, J. Zhang, and Z. Nazeri. Community evolution in dynamic multi-mode networks. In *the 14th ACM SIGKDD international conference on Knowledge discovery and data mining*, 2008.

[19] G. Vaynerchuk. *Crush It!: Why Now Is the Time to Cash in on Your Passion*. HarperCollins, 1st edition, 2009.

[20] G. Wondracek, T. Holz, E. Kirda, and C. Kruegel. A practical attack to de-anonymize social network users. In *the 31st IEEE Symposium on Security and Privacy*, 2010.

[21] R. Zafarani and H. Liu. Connecting corresponding identities across communities. In *the 3rd International Conference on Weblogs and Social Media (ICWSM)*, 2009.

[22] E. Zheleva and L. Getoor. To join or not to join: the illusion of privacy in social networks with mixed public and private user profiles. In *the 18th International World Wide Web Conference (WWW)*, 2009.