Can friends be trusted? Exploring privacy in online social networks

Frank Nagle, Lisa Singh
Georgetown University
Department of Computer Science
Washington, DC 20057
fen@georgetown.edu, singh@cs.georgetown.edu

***Abstract*— In this paper, we present a case study describing the privacy and trust that exist within a small population of online social network users. We begin by formally characterizing different graphs in social network sites like Facebook. We then determine how often people are willing to divulge personal details to an unknown online user, an adversary. While most users in our sample did not share sensitive information when asked by an adversary, we found that more users were willing to divulge personal details to an adversary if there is a mutual friend connected to the adversary and the user. We then summarize the results and observations associated with this Facebook case study.**

I. Introduction

Social network sites like Facebook and MySpace have gained considerable popularity over the past five years. These sites allow users to create 'active' online profiles to share with friends. Similar to real world social networks, as relationships change users can add and remove friends from their networks. Anyone can make a request to join a user's network - strangers, acquaintances, or established friends. Many disciplines are researching the role of privacy and trust in these networks [1], [3], [5], [10], [4]. Current literature supports the claim that people are more willing to share personal information with online aquaintances or strangers than they are in similar offline situations [2], [5], [3]. Additionally, research has shown that when a trust bond exists between individuals in online environments the perceived risks involved in revealing personal information are diminished [7]. However, allowing strangers or acquaintances to join a user's network can lead to a number of privacy risks, including cyber-stalking and identity theft.

In this paper, we explore the trust and privacy concerns of online social network participants. Do online users actively attempt to keep their personal information private? How is trust established online? This exploratory work begins analyzing these questions using a sample of Facebook users.

Specifically, our study sets up multiple adversary profiles that actively try to gather sensitive information by befriending a random set of people. We hypothesize that those who befriend a stranger have no expectation of privacy, while those who do not befriend a stranger have a higher expectation of privacy and actively try to maintain their privacy. We then look at trust by attempting to befriend people with whom the target user and the adversary share a common friend. We find support for the idea that most online users want to keep personal data private from strangers, but the majority implicitly trust friends of friends, revealing potentially sensitive information to strangers. This is consistent with the Dwyer et al survey finding that the Facebook site breeds a significant level of trust amongst its users [5]. Although other studies, including [1] and [10], have explored the types of personal information that users of Facebook are willing to divulge to strangers, our study goes one step further by looking at the percentage of users that are willing to accept a friend request from an unknown user that has a common friend.

II. Friendship Graphs

Online social networks can be represented as a graph G, where an individual's profile is considered a vertex or a node and a "friendship" between two nodes is considered an edge. Formally, $G = (V, E)$, where V is a set of vertices, $V = \{v_1, v_2, \ldots, v_n\}$, and E is a set of edges, $E = \{e_{ij} = (v_i, v_j) \mid v_i \epsilon V \text{ and } v_j \epsilon V\}$.

When a user creates a new Facebook profile, he/she must begin as a member of an existing social network G', where $G' \subseteq G$. These subgraphs are networks based on geographical location, academic affiliation, employer, etc. By default, the user profile is fully viewable by any other user in the same network. While the user has actively joined this network, he/she has not actively befriended each individual in G'. We will refer to an edge in G' as a *passive friendship link* and denoted as e^p. While this open setting can be changed to reduce the amount of data that non-friend users within the same network can see, by having the default setting as open, strangers (adversaries) within the same network can see the profile and a passive friendship graph $G'_p \subseteq G'$ has been created.

The user can change the privacy settings to only allow users he/she has an established friendship link with to see profile data. In this case, a passive friendship graph exists, but limited information is visible to friends in this network. By default, everyone in Facebook has limited access to everyone else's information. Therefore, we say that G_p is

Table I
BEFRIENDING ALGORITHM

befriend()
Input: v_a, G_p
Output: $G'_a v_a$

R = random sample of G_p
foreach v_i in R
  get public profile data
  send friend request, $f(v_a, v_i)$

  if $f(v_a, v_i)$ = accept
    get sensitive profile data
    befriend(v_a, $G'_a(v_i)$)

the passive friendship graph of the entire Facebook network G. Facebook also has a more private account setting that hides the 'existence' of a profile from everyone that is not a friend. In this case, a user's passive graph is empty, $G'_p = \emptyset$.

When a Facebook user receives a friend request from another user, he can confirm the friendship - thus creating a new edge between the two vertices. We will refer to an edge e^a initiated or accepted by the user as an *active friendship link*. An active friendship graph $G'_a \subseteq G'$ contains all the user's active friendship links. A user can also explicitly ignore the friend request, thus rejecting the request, or he/she can do nothing and let the request go unanswered. In both cases, a passive friendship link e^p still exists, but an active one is not established.

To summarize, each user v_i has two passive friendship graphs, $G_p(v_i)$ and $G'_p(v_i)$, established via a user profile setting, and an active friendship subgraph $G'_a(v_i)$, explicitly created by the user. We assume that since the user explicitly befriended the people in this graph, these are people that the user believes can be trusted with sensitive information. The goal of our adversary is to establish friendships on as many active friendship subgraphs as possible. We say a *friendship privacy breach* occurs for user v_i when an adversary becomes a member of v_i's active friendship graph. We say a *trust privacy breach* occurs if an adversary becomes a member of v_j's active friendship graph through v_i's active friendship graph.

III. CASE STUDY METHODOLOGY

In this study, our goal is to determine 1) the percentage of our sample Facebook population willing to befriend an unknown user or adversary, v_a; 2) the amount of information each user v_i reveals to members of his/her passive friendship network $G_p(v_i)$; 3) and the amount of sensitive data user v_i reveals to members of his/her active network $G'_a(v_i)$. Table I shows our high level befriending algorithm.

The input into the algorithm is the adversary profile, v_a and the Facebook passive friendship network G_p. The output will be v_a's active friendship network, $G'_a(v_a)$. Because G_p is large, the algorithm begins by selecting a random set of target users, R from G_p. For each user v_i in R, public profile data for v_i is collected and a friendship request $f(v_a, v_i)$ is sent by adversary, v_a. If user v_i accepts the friendship request, a friendship privacy breach occurs and sensitive profile data for v_i is collected. The befriending algorithm is then applied to v_i's active friendship network, $G'_a(v_i)$. This process is recursively applied to target users' active friendship networks. Friendship acceptance in the latter iterations results in a trust privacy breach.

IV. EXPERIMENTS AND RESULTS

The first task of the study was to setup various adversarial profiles to use during the automated friend request process. We designed four different profiles to see whether or not the type of person initiating the friend request affected the response rate. The four adversary profiles were a female in high school ("Izzie"), a female in college ("Kate"), a female who had graduated from college and was a working professional ("Jane"), and a well-known cartoon character Abe Simpson from the television show The Simpsons ("Abe"). The cartoon character profile was used to help determine whether or not realistic adversaries were important for users to accept a friendship request. We created each adversary's profile in a different initial network and began the befriending algorithm. We used an automated Python module based on [9] to send friend requests and collect statistics about the public and sensitive profile data. Here, we actively solicited friends, trying to gain access to users' active friendship graphs.

During the first iteration of the program, target users were chosen randomly from G_p using a distinct Facebook profile number. We were trying to investigate the question - will an online user allow a stranger to access his/her sensitive personal information, including his/her active friendship graph? We collected as much information about the target profile as the privacy settings of the target profile allowed. The amount of available data varied from the user's name and associated networks to the entire profile, including sensitive information.

After allowing this first iteration to run for a number of weeks, the second iteration was initiated. Here, we were trying to investigate the question - does having a common active friendship link improve the probability that a stranger will be added to a user's active friendship network? Is there an implicit trust associated with being a friend of a friend? More iterations of the befriend algorithm are part of future work.

A. Adversaries in the active friendship network

Table II shows the results by profile type for both the first and second iteration. For each column, the first iteration

Table II
NUMBER OF FRIENDSHIP AND TRUST BREACHES

Profile Id	Friend Requests Sent		Accepted Friend Requests		Acceptance Rate (%)	
	1	2	1	2	1	2
Izzie	1000	N/A	234	N/A	23	N/A
Kate	1972	1923	389	1125	20	59
Jane	1091	936	207	467	19	50
Abe	1000	650	125	371	13	54
Total	5063	3549	955	1963	19	55

has a 1 above it, and the second iteration a 2.[1] The first iteration results showed an acceptance rate of 19% across the four profile types. However, the type of profile affected the acceptance rate, especially in the case of the cartoon character Abe.

The second iteration of the program attempted establishing friendship links with a subset of a befriended target user's active friendship network. Our results show a 55% acceptance rate when there was at least one mutual friend between the test profile and the target profile. For our sample, the average number of active friendship graph neighbors is 127 and the full target population is 121,153. Due to the limitations on friend requests imposed by Facebook and the exponential growth in the number of target friends, it was not possible to send requests to the full target population during the second iteration.

The results from the second iteration show an average acceptance rate approximately three times higher than the first iteration. Interestingly, the known fake profile "Abe" had an acceptance rate that was much more in line with the other profiles, unlike the first iteration. We interpret these findings to mean that the majority of users want to maintain privacy of sensitive data (iteration 1), but do not perceive a privacy loss when befriending a friend of a friend because of pre-established trust with friends in their active friendship network. Govani and Pashley hypothesize that some level of the trust seen by users in online social networks stems from peer-pressure [8]. While this may apply to our situation, it is more likely that users inherently trust people they already have associations with.

B. Profiles of Accepted Friends

Facebook profiles contain a wealth of personal information including everything from address and phone number to political and sexual preferences. Figure 1 summarizes these findings.[2] Two of the more interesting findings were that 1958 profiles (94%) had either a partial (month and day), or full (month, day, and year) birthday listed and 1876 (90%) had at least one email address. Of the 70% that listed their gender, 60% were male and 40% were female. Similarly, of those that listed a mobile phone, 60% were male.

A few previous works have gathered demographic data from online social network users [1], [6], [10]. In 2006, Acquisiti and Gross gathered data from 4,540 user profiles of students that went to Carnegie Mellon University. Their research found that, unlike some other online social networking sites, their sample of Facebook users used a real name and accurate demographic information, with 88% revealing their birthdate and 40% revealing their phone number [1]. In a 2005, Charlie Rosenbury, a student at the University of Missouri, contacted 250,000 Facebook users of which 75,000 agreed to link to his network [6]. In his experiment, approximately 30% of the users contacted were willing to divulge their personal information to someone they had never met. Yu describes a smaller scale experiment run by Sophos, an anti-virus company, in 2007 with 200 users. They found that 41% of their sample of Facebook users were willing to accept a friend request from an unknown entity [10].

A number of factors may account for the differences between the studies. The Rosenbury study did not record statistics for profile information such as birthday, phone number, and e-mail address. Additionally, Rosenbury was able to request such a large number of friends because Facebook had not yet implemented restrictions on such actions when he performed his study. Acquisiti and Gross did not actually request their targets befriend them since they only studied the population of one university and were able to see the profile details of most users at that university without requesting a friendship link first. Finally, the Sophos study only targeted 200 people. In this study, 41% accepted a friendship request, 84% had their birthday listed and 23% listed a phone number.

Although we were unable to validate whether or not all of the information collected is factual, Facebook is designed to encourage users to enter accurate personal information. The type of personal information tracked by Facebook, such

[1]In Table II, there are no second iteration results for "Izzie" because her account was disabled by Facebook.

[2]Although 2918 people accepted a friend request from our adversary profiles, we were only able to gather details on 2094 profiles because some of the test profiles were disabled before the data for their friends could be collected.

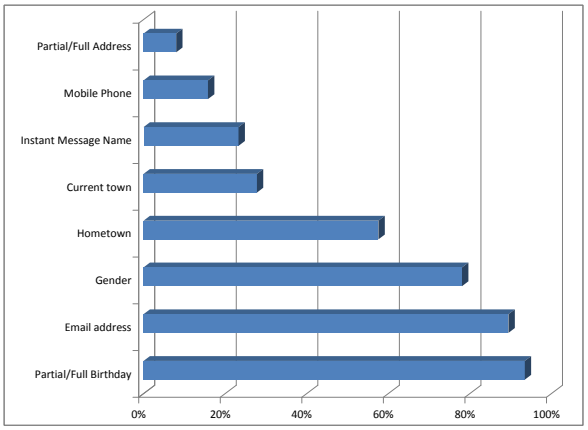

Figure 1. Profile information of Accepted Friends

as date of birth, gender, hometown, and address can easily be used for identity theft, while contact information such as email address, instant message contact name, or mobile phone can be used for stalking and spamming activities. It should be noted that the statistics above may be biased since users who are willing to accept a friend request from an unknown entity may also be disproportionately more willing to put sensitive information such as date of birth, phone number, and email address in their profile. Alternatively, it is possible that users who were not willing to accept a friend request from an unknown user are more likely to decline such requests because they have a disproportionate amount of sensitive information within their profile.

There are a few limitations of this study that we want to mention. One hurdle we ran into during the data gathering process was the limitations on friend requests established by Facebook. Due to spam-related problems faced in the past, Facebook has limited the speed with which any given profile can request new friends. As a result, we needed to request friends at a slow rate, thereby limiting our overall sample size. Further, some of the adversary profiles were either blocked from adding friends for a period of time, or shutdown completely. This was due to two factors. First, the exact thresholds that Facebook implements to limit friend requests are not publicly disclosed. Second, it is possible for a Facebook user to report another Facebook user when the user suspects malicious abuse of Facebook. Once an account has been reported for potential abuse, its thresholds can be lowered, its ability to request friends can be removed, and it can be disabled. Both of these factors influenced our outcomes.

V. Conclusions and Future Work

Our findings attempted to show the willingness of a user to share sensitive information in an online social network. Our efforts showed that our sample of Facebook users are much more likely to add a stranger to their active graph if there is a mutual friend between the requester and the target. A number of extensions upon this research are possible. First, this research did not attempt to compare the difference in likelihood between users who had tightened their privacy settings and those who had left them at the default setting. Presumably, users who tightened their privacy settings would be less likely to accept a friend request from an unknown entity. Second, this study only accounted for one or more mutual friends in the second iteration. Finally, this study had minimal user interaction on the parts of the researchers. Most messages received from the target profiles by the adversarial profiles went unanswered. It is likely that responding to user emails and adding Facebook applications would increase the probability of target users accepting friend requests. While this study is an interesting first step toward understanding users of online social networks, much work remains to understand the relationship between privacy and trust in this environment.

References

[1] A. Acquisiti and R. Gross, “Information revelation and privacy in online social networks (the facebook case),” in *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (WPES)*, November 2005.

[2] ——, “Imagined communities: Awareness, information sharing, and privacy on the facebook,” in *Proceedings of the 6th Workshop on Privacy Enhancing Technologies*, June 2006.

[3] N. F. Awad and M. S. Krishnan, “The personalization privacy paradox: An empirical evaluation of information transparency and the willingeness to be profiled online for personalization,” *MIS Quarterly*, vol. 30, no. 1, March 2006.

[4] L. Backstrom, C. Dwork, and J. Kleinberg, “Wherefore art thou r3579x? anonymized social networks, hidden patterns, and structural steganography,” in *ACM WWW Conference*, May 2007.

[5] C. Dwyer, S. R. Hiltz, and K. Passerini, “Trust and privacy concern within social networking sites: A comparison of facebook and myspace,” in *Proceedings of the Thirteenth Americas Conference on Information Systems*, August 2007.

[6] K. Jump, “A new kind of fame,” *Columbian Missourian*, September 2005.

[7] M. Metzger, “Privacy, trust, and disclosure: Exploring barriers to electronic commerce,” *Journal of Computer-Mediated Communication*, vol. 9, no. 4, 2004.

[8] G. Tabreez and H. Pashley, “Student awareness of the privacy implications when using facebook,” Website: http://lorrie.cranor.org/courses/fa05/tubzhlp.pdf, January 2009.

[9] K.-P. Yee, “scrape.py,” Website: www.zesty.ca/scrape.

[10] E. Yu, “Facebook users fall foul of fake frog id thief?” *ZDNet Australia*, August 2007.