Social Circles: Tackling Privacy in Social Networks

Fabeah Adu-Oppong[†] Casey K. Gardiner[†] Apu Kapadia[†‡] Patrick P. Tsang[†]

[†]Department of Computer Science
Dartmouth College
Hanover, NH 03755, USA

[‡]Institute for Security Technology Studies
Dartmouth College
Hanover, NH 03755, USA

{fabs, ckg, akapadia, patrick}@cs.dartmouth.edu

ABSTRACT

Users of social-networking services share an abundance of personal information with a large number of "friends." Services such as Facebook have recognized the need for privacy mechanisms that allow users to control which friends see what information. For example, users on Facebook can group their friends into *Friend Lists*, and then selectively present different profiles to each of these lists. Grouping several hundred friends into different lists, however, can be a laborious process; on what basis should users construct the Friend Lists? And even if the user were to group friends into lists, are these lists meaningful for setting privacy policies?

To alleviate the burden of constructing meaningful lists manually, we propose to build—and evaluate the usability of—an automated grouping technique that analyzes the user's social graph for *social circles*, i.e., clusters of densely and closely connected friends. With the hypothesis that a user shares information (mostly) uniformly with friends within the same social circle, we believe that identifying these social circles will give users a usable and meaningful grouping of friends, which they can further refine. In this paper, we provide an overview of our proposed technique, followed by a description of our planned user study.

1. INTRODUCTION

Online social-networking services, which allow users to label other users as "friends," thereby sharing with them a wide variety of personal information ranging from favorite movies to resumes, have become incredibly popular. Facebook, for example, has over 70 million active users.[1] As social networks have grown in size, and as the term "friend" has become all-encompassing, it has become increasingly difficult for users to control which friends get to see what personal information. Despite the privacy controls available on such social-networking services, many users neglect to control their privacy because it is difficult to set privacy policies [1]. Also, a study shows that college students rarely utilize the different privacy settings on Facebook and are often unaware of their own privacy settings [3].

Facebook has recently implemented a feature called *Friend Lists*, which allows users to more easily set privacy policies for a collection of friends by manually creating a list of friends and setting privacy policies for the list. For example, a user may create friend lists called College, Workplace, and Salsa Club, and present a different view of their personal profile to friends on each of these lists.

Unfortunately, while Friend Lists are a step towards a more usable mechanism for controlling privacy in social-networking services, it has a major drawback: many users have more friends than they can categorize into lists effectively. Even if users were to perform this daunting task of categorization, on what basis would they categorize their friends *in a way that is meaningful for setting privacy policies*? For example, a College friend list might be too general for a user to set meaningful policies for, considering the list may consist of, e.g., his or her roommate and the TA in a course he or she took in the past.

[1]http://www.facebook.com/press/info.php?factsheet

Symposium On Usable Privacy and Security (SOUPS) 2008, July 23-25, 2008, Pittsburgh, PA, USA.

2. PROPOSED SOLUTION

To alleviate the burden of categorizing a large number of users into meaningful lists, we propose a technique called *Social Circles Finder* for generating these lists automatically. We posit that clusters of densely and closely connected friends, or *social circles* as we call them, can be viewed as uniform groups from the perspective of privacy settings. In other words, we believe that users would present (mostly) consistent profiles with all friends in a social circle, and therefore social circles provide a meaningful categorization of friends for setting privacy policies. As an example, members of a college athletic team are "friends" of one another and hence (personal) information propagates easily among them. Hence, team members would probably want to present the same profile to all other members and thus set the same privacy policy for all of them. *Social Circles Finder* will be able to identify the athletic team (possibly with a small chance of incorrect categorization) as a social circle.

2.1 Proposed Implementation

We plan to develop *Social Circles Finder*, a Facebook application which identifies social circles for users in their social networks, and provides the following features.

Social-graph visualization Visualize the social circles of users by rendering such an image as Figure 1, which would help users make more well-informed and hence better decisions about their privacy settings.

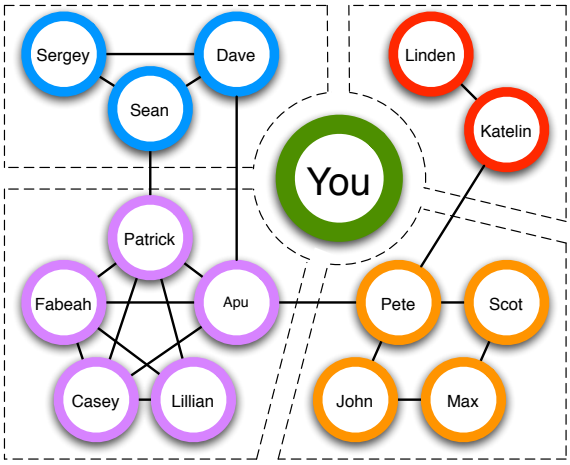

Figure 1: Our proposed Facebook application clusters a user's Facebook friends into social circles for easier privacy policy management.

Privacy-settings recommendation Recommend the set of friend lists users should create, and the friend lists into which they should put each of their current friends, based on the identified social circles.

Social Circles Finder would be able to, with proper integration into the Facebook platform, provide the above features not just when users are browsing their friends, but also when they are *adding new friends*. (Currently, Facebook applications cannot interact with the "Add Friend" page.)

2.2 Mathematical Tools

To build *Social Circles Finder*, we plan to make use of an algorithm due to Mishra et al. [2] for finding (α, β)-clusters with ρ-champions in undirected graphs so that any node in such a cluster is adjacent to at least a β-fraction of the cluster and any node outside of such a cluster is adjacent to at most an α-fraction of the cluster. This definition of clusters logically resembles our definition of social circles if we regard node adjacency as friendship. *Social Circles Finder* will thus use the social graph of the user as the input to the above algorithm, and regard the clusters returned by the algorithm as the social circles of the user.

3. USER STUDY

Our proposed user study has two aims. First, we want to discover whether social circles (as we have defined) actually exist on Facebook. Second, we want to discover whether these social circles would help users in social-networking applications such as Facebook to set effective privacy policies.

3.1 Study Design

In our user study, subjects will add *Social Circles Finder* to their Facebook pages. The application will identify the social circles of the subject but not show them to the subject. The subject will then be asked questions about their willingness to share a piece of their personal information with a Facebook friend of theirs, e.g., *"Do you wish to share information X with friend Y?"*, over a set of information X (e.g., cell phone number, email address, and favorite movies) and a set of friends Y.

Social circles are meaningful from a privacy standpoint—and thus *Social Circles Finder* is effective—if the subjects tend to choose to share the same combination of personal information with friends in the same social circle but different combinations with friends in different social circles. Using the data collected from the study, we will be able quantitatively determine the effectiveness of *Social Circles Finder* using the following two metrics:

1. The variance $\sigma^2_{X,Y}$ in the willingness to share information X with friends in social circle Y. *Social Circles Finder* is effective if $\sigma^2_{X,Y}$ is significantly low for significantly many (X, Y)-combinations.
2. The covariance cov_{X,Y_1,Y_2} between the willingness to share information X with friends in social circle Y_1 and that with friends in social circle Y_2. *Social Circles Finder* is effective if for any $Y_1 \neq Y_2$, there is at least an X such that cov_{X,Y_1,Y_2} is significantly negative.

3.2 Design Rationale

To prevent bias, we plan to reveal to subjects as little about the study as possible, such as the fact that we are evaluating the concept of *social circles* in the context of privacy. This is one of the reasons the study hides the identified social circles from the subjects. Also, this data collection method will provide us with quantitative results that we can statistically analyze. Hence, we can evaluate *Social Circles Finder* in a much more scientific manner than would be possible using a survey or a contrived social networking environment.

The study is designed with the subjects' privacy in mind. Subjects will consent to adding *Social Circles Finder* to their Facebook pages and will be able to delete it after they have completed the study. We will have no more access to personal information than any other registered Facebook application developer does, and will delete this information in compliance with the regulations set forth by Facebook. We will collect no more (anonymized) information than needed to quantify *Social Circles Finder*'s effectiveness.

4. ACKNOWLEDGMENTS

This research was supported in part by AT&T/Internet2, the Bureau of Justice Assistance under grant 2005-DD-BX-1091, the U.S. Department of Homeland Security under grant 2006-CS-001-000001 and the National Science Foundation under grant CNS-0524695. The views and conclusions do not necessarily reflect the views of the sponsors.

The authors would like to thank Sean Smith for his helpful comments.

5. REFERENCES

[1] A. Acquisti and R. Gross. Imagined communities: Awareness, information sharing, and privacy on the facebook. In *Privacy Enhancing Technologies*, volume 4258 of *LNCS*, pages 36–58. Springer, 2006.

[2] N. Mishra, R. Schreiber, I. Stanton, and R. E. Tarjan. Clustering social networks. In *Algorithms and Models for the Web-Graph, 5th International Workshop*, volume 4863 of *LNCS*, pages 56–67. Springer, 2007.

[3] K. Strater and H. Richter. Examining privacy and disclosure in a social networking community. In *SOUPS '07: Proceedings of the 3rd symposium on Usable privacy and security*, pages 157–158, New York, NY, USA, 2007. ACM.