

Privacy Wizards for Social Networking Sites

Lujun Fang and Kristen LeFevre
 Electrical Engineering & Computer Science, University of Michigan
 2260 Hayward Ave. Ann Arbor, MI 48109 USA
 ljfang@umich.edu, klefevre@umich.edu

ABSTRACT

Privacy is an enormous problem in online social networking sites. While sites such as Facebook allow users fine-grained control over who can see their profiles, it is difficult for average users to specify this kind of detailed policy.

In this paper, we propose a template for the design of a social networking *privacy wizard*. The intuition for the design comes from the observation that real users conceive their privacy preferences (which friends should be able to see which information) based on an implicit set of rules. Thus, with a limited amount of user input, it is usually possible to build a machine learning model that concisely describes a particular user's preferences, and then use this model to configure the user's privacy settings automatically.

As an instance of this general framework, we have built a wizard based on an active learning paradigm called *uncertainty sampling*. The wizard iteratively asks the user to assign privacy "labels" to selected ("informative") friends, and it uses this input to construct a classifier, which can in turn be used to automatically assign privileges to the rest of the user's (unlabeled) friends.

To evaluate our approach, we collected detailed privacy preference data from 45 real Facebook users. Our study revealed two important things. First, real users tend to conceive their privacy preferences in terms of *communities*, which can easily be extracted from a social network graph using existing techniques. Second, our active learning wizard, using communities as features, is able to recommend high-accuracy privacy settings using less user input than existing policy-specification tools.

Categories and Subject Descriptors

H.2.7 [Information Systems]: Security, integrity, and protection

General Terms

Security

Keywords

Social Network Privacy, Usability, Active Learning

1. INTRODUCTION

Social networking sites (e.g., Facebook, MySpace, Friendster, Orkut, etc.) are websites that enable people to share information and communicate with friends online. At the

Copyright is held by the International World Wide Web Conference Committee (IW3C2). Distribution of these papers is limited to classroom use, and personal use by others.
 WWW 2010, April 26–30, 2010, Raleigh, North Carolina, USA.
 ACM 978-1-60558-799-8/10/04.

same time, users typically do not want to share all of their information with everyone, and privacy has emerged as a serious concern.

A growing number of social networking and social media sites allow users to customize their own privacy policies. For example, Facebook has a "Privacy Settings" page, which allows users to specify which pieces of profile data each friend is allowed to view. Facebook also allows users to create friend *lists*, and then specify whether a piece of profile data is visible or invisible to all friends in a particular list.

Unfortunately, studies have consistently shown that users struggle to express and maintain such policies [4, 13, 22, 27, 39], due in part to complex and unusable interfaces [39]. On Facebook, for example, the user must manually assign friends to lists; because the average Facebook user has 130 friends [2], the process can be very time-consuming. Worse, numerous lists may be required since a user's privacy preferences can be different for different pieces of profile data (e.g., *Home Address* vs. *Religious Views*).

Clearly, there is a need for something better. In this paper, we propose the first *privacy wizard* for social networking sites. The goal of the wizard is to automatically configure a user's privacy settings with minimal effort from the user.

1.1 Challenges

The goal of a *privacy wizard* is to automatically configure a user's privacy settings using only a small amount of effort from the user. The design and implementation of a suitable wizard present a number of difficult challenges. Ideally, the wizard should satisfy the following requirements:

- **Low Effort, High Accuracy:** The wizard may solicit input from the user. Research has shown, however, that users have trouble reasoning holistically about privacy and security policies [35, 27]. Thus, the user's input should be simple in form, and also limited in quantity.

At the same time, the settings chosen by the wizard should accurately reflect the user's true privacy preferences. A naive approach would ask the user to manually configure her privacy settings for all friends. While this approach may produce perfect accuracy if carried to completion, it also places an undo burden on the user.

- **Graceful Degradation:** It is difficult to predict the amount of input that a particular user will be willing to provide. As the user provides more input, the accuracy of the resulting settings should improve. However, the wizard should assume that the user can quit at any time.
- **Visible Data:** In addition to the user's input, the wizard may also use information that it can gather and process

