Access Control Policy Misconfiguration Detection in Online Social Networks

Yousra Javed, Mohamed Shehab
College of Computing and Informatics
University of North Carolina at Charlotte
{yjaved,mshehab}@uncc.edu

***Abstract*—The ability to stay connected with friends online and share information, has accounted for the popularity of online social networking websites. However, the overwhelming task of access control policy management for information shared on these websites has resulted in various mental models of sharing with a false sense of privacy. The misalignment between a user's intended and actual privacy settings causes access control misconfigurations, raising the risk of unintentional privacy leaks. In this paper, we propose a scheme to extract the user's mental model of sharing, enhance this model using information learned from their existing policies, and enable them to compose misconfiguration free policies. We present the possible misconfiguration patterns based on which we scan the Facebook user's access control policies. We implemented a prototype Facebook application of our scheme and conducted a pilot study using Amazon Mechanical Turk. Our preliminary results show that the users' intended policies were significantly different than their actual policies. Our scheme was able to detect the misconfiguration patterns in album policies. However, the reduction in the number of misconfigurations after using our approach was not significant. Participants' perceptions of our proposed policy misconfiguration patterns *and* the usability of our scheme was positive.**

Keywords*—Policy, Access Control, Privacy, Social Network

I. Introduction

Online social networks have attracted a large user base over the recent years. Due to the vast amount of information being shared on these websites daily, effective data privacy management by users is a major concern on these websites[1]. To enable the customization of access control policies on user data, most social networks provide a privacy settings interface to manage the privacy of various profile items [2]. An *access control policy* represents the permissions set by a user to allow or deny access to a particular item. End-users are inexperienced in authoring access control policies, and therefore, struggle to express and maintain fine-grained policies for different data items [3][4][5][6][7]. Recently, tools to improve the usability of current privacy settings interface, *and* aid the users in understanding how their information is visible to their friends on Facebook style social networking websites, have been proposed [8][9][10].

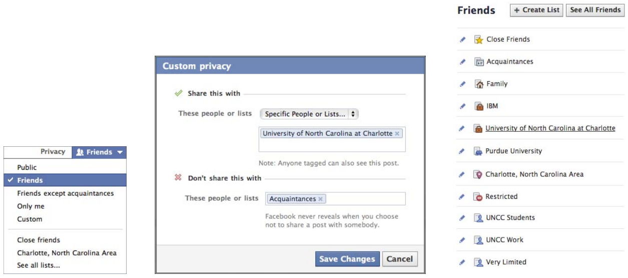
The biggest challenge in effective data privacy management on social networks is to capture a user's sharing mental model, and enhance it so as to reduce access control policy misconfigurations [11]. For example, Alice intends to give access to her Facebook albums to only those friends who studied with her in college *and* are close to her. Therefore, she includes the two friend lists, namely, *Close friends* and *College friends* in her access control policy. This gives Alice a false perception of sharing the albums with the intended audience since in Facebook, access is allowed/denied to the union (and not intersection) of friends in the allow/deny fields. Thus, leading to unintended sharing of information. It is therefore, essential to collect user intentions first, in order to help them reduce misconfigurations in their policies.

Existing social network data privacy checking tools focus on scanning of user's profile, mainly by searching for the visibility of user's data outside their friend network, and providing recommendations to the users for limiting access on privacy sensitive items such as location, friend lists and relationship status [12][13][14]. However, to the best of our knowledge, there is little work w.r.t capturing user mental model of sharing in order to detect and resolve misconfigurations. Madejski et al. have made an effort to collect user's sharing intentions [15]. However, their approach requires extensive user input in the form of intended audience for each profile item category. Secondly, they have not evaluated their scheme for privacy leaks. Also, the approach does not cater data objects such as albums; the privacy settings for each album can be drastically different and therefore, can not be handled as a single category.

In this paper, we propose a scheme to capture the user mental model of sharing Facebook albums, and enhance this mental model through data learned from the user's existing policies, in order to reduce the policy misconfigurations. The possible misconfiguration patterns in Facebook users' access control policies were formulated through the analysis of Facebook privacy settings interface and users' policy patterns. We focus on Facebook, since it is one of the most popular online social networking websites today with over 955 million active users [16]. Through the Facebook API, applications can access the user's privacy settings which enabled us to extract and analyze real user privacy policies. Currently, our approach only focuses on photo albums, which can be easily extended to other types of information objects. Due to the large number of albums per user, they are vulnerable to access control policy misconfigurations. Our scheme involves the user in the process of misconfiguration detection in order to increase their understanding and awareness of the detected misconfigurations.

The rest of the paper is organized as follows: In Section II, we discuss access control and policy composition in online social networks. Section III, explains our access control policy misconfiguration detection framework in detail. The pilot study

978-0-7695-5137-1 2013
U.S. Government Work Not Protected by U.S. Copyright
DOI 10.1109/SocialCom.2013.82



✓ Share this with

These people or lists: Specific People or Lists...

University of North Carolina at Charlotte ×

Note: Anyone tagged can also see this post.

✗ Don't share this with

These people or lists: Acquaintances ×

Facebook never reveals when you choose not to share a post with somebody.

(a) Default (b) Custom (c) Friendlists

Fig. 1: Facebook privacy settings interface

design to test our proposed scheme is described in Section IV-B and the results are detailed in Section V. We discuss the related work in Section VI. Finally, we conclude the paper.

II. Access Control in Online Social Networks

Access control enables a user to define how other users will access the information items they share. In online social networks, access control is achieved using the privacy settings interface provided by their websites. When a user shares an object, they define the privacy settings consisting of the friends who should be allowed and denied access to it.

The objects in social networks represent various information items that the users share. These objects consist of user's personal information i.e., profile, and posts such as status, photos and videos. There are two types of permissions on objects in social networks, namely, read, and write. The *read* permission enables the user to view an object's content. If access to objects under the profile category is allowed, the allowed friends can view but can not like/comment on the object. The *write* permission enables the user to like and comment on the object as well.

Facebook provides a user interface to compose and edit the privacy settings of an information object. Figure 1, shows the Facebook's privacy settings interfaces. The user can either choose from a list of default policies, which are more generic policies (See Figure 1(a)), or create custom access control policies by specifying both the specific users or groups of users who should be allowed, and the users who should be denied; exceptions (See Figure 1(b)). Friends can be organized using the Facebook friend list feature. (See Figure 1(c)). Currently, three types of friend lists are supported by Facebook:

1) *Default:* They are present by default when the user creates their Facebook account. The user adds/deletes the friends inside these lists.
2) *Custom:* They are created and populated by the user at their will.
3) *Smart:* They are automatically created when a user updates their home, work or education. Moreover, they populate themselves without user interaction. For example, if a user adds University of North Carolina at Charlotte to their Education, a smart list for this education category will be created and the user's friends who listed this school under their education will be added to the list.

Information object categories in Facebook include wall posts, profile information, photos and videos. Each of these categories is further sub-divided into object types. For example, wall posts can be a status update, check-in, photo, video or a life event. Similarly, profile information consists of basic information, home, work, education and interests etc.

III. Misconfiguration Detection Scheme

Detecting policy misconfigurations in social networks is a hard problem because 1) we do not know what a user considers as a misconfiguration and what are their sharing intentions 2) it is not guaranteed that the user understands the purpose and context of the detected misconfigurations. The user is likely to ignore or forget them. Therefore, we approach this problem by involving the user in the process of capturing their mental model of sharing intentions, and guiding them in order to compose better policies.

A. *Sharing Intention Collection*

The first module of our scheme focuses on capturing the user's sharing intentions for their information items i.e., the photo albums. Our sharing intention collection approach is a three step process through which the users express their sharing intentions for each album.

1. Album grouping

An average Facebook user has a minimum of 10 albums, many of which are shared with the same audience depending on the events related to the photos. Grouping these similar albums can therefore, reduce the number of objects that the user has to focus on, by treating the albums within a group as one object. Although this step can be automated using data mining and clustering schemes, we choose manual grouping, in order to maintain accuracy. The user is asked to group their albums based on sensitivity; albums to which they would like to assign the same permissions. They can create any number of groups as they require. The user drags each album into a particular group container. In order to have one policy per album, each album must be placed into one group only. To help the user in grouping, a tooltip containing the album's information is displayed when the user rolls the mouse over an album icon. The album information in the tooltip includes its name, privacy settings, number of access control misconfigurations related to the album's policy, and the number of photos.

2. Metadata extraction

The number of album groups created in the first step implies the number of different policies the user has in mind. We attempt to enhance this sharing intention model such that it results in secure policies. For this purpose, we extract the following additional information from user's existing policies:
Frequency of use: Number of times a particular policy was set by the user
Misconfigurations: Number of misconfiguration patterns detected in the policy
This information is presented to the user in the next step in order to influence their decisions.

3. Album policy composition

The next step in the intention collection process is policy composition for the user created album groups. The users express the access control criteria based on which they grouped their albums together, by setting permissions for each album group. Instead of using Facebook's existing privacy settings interface for policy composition, we present the users with their existing policies to choose from, based on the following propositions:

- These policies are representative of the set of friends with whom the user usually shares their items. Hence, the user is most likely to use a combination of the same friends in their new album policies.
- These policies can be complemented with the extracted metadata to influence the decisions

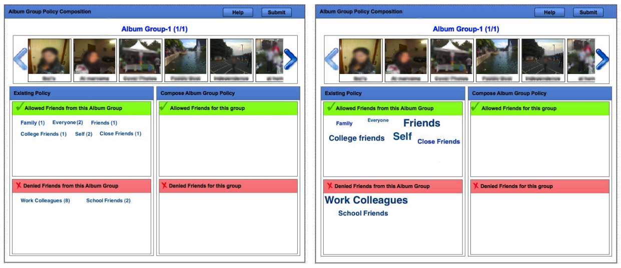
In order to avoid the textual policies from looking verbose and unreadable, we present the user's existing policies in a visually appealing manner. We use Tag cloud visualization for this purpose. Tag cloud [17] is a visual representation of a set of words related to a particular topic. The attributes of text such as size, weight, or color are used to represent features, such as frequency of the associated terms. Tag clouds have been used by researchers for various purposes. Hearst et al. [18] state that the main role of Tag cloud is as a social signaler to attract peoples' attention rapidly. Eda et al. [19] have proposed an entropy based scheme to increase emphasis on emotional tags. We split each policy into its allowed and denied components to extract tags. For example, if an album's privacy settings allow two friend lists and deny a particular friend, then this album's policy comprises of three tags.

We customize the user's existing policies using the extracted metadata and create two types of Tag clouds. In the first Tag cloud, we include the frequency of use of each policy along with its tag. However, policy usage frequency can bias the user to select a policy containing misconfigurations. For example, if most of the user's albums are public, then the size of tag related to public policy will be big, attracting the user attention towards it. Therefore, instead of increasing the tag size based on usage frequency, we keep the tag size fixed and combine the tag usage frequency with its label in order for the user to differentiate between the tags. This is shown in Figure 2(a). For the second Tag cloud, we incorporate the misconfigurations related to each tag using the equation 1. In this Tag cloud, the tags of an album policy, which are causing the access control misconfigurations are decreased in size according to the cumulative sensitivities of all the misconfigurations related to the respective tags. Each misconfiguration is assigned a sensitivity weight on a scale from 0 to 1 based on the extent of privacy leak that it can cause. The access control misconfigurations caused by each tag are calculated by scanning the user's existing album policies based on our misconfiguration patterns. For example, suppose a user has three albums with the following policies: *allow friends*, *allow public* and *allow only me* respectively. Since, the access control misconfigurations corresponding to "public" tag has the highest privacy leak, this tag will be very small in size as compared to the other two tags. Figure 2(b) shows the visual representation of album policy tags using Equation 1.

The Tag clouds for the allowed and denied part of the policies are calculated separately. The user composes the policy for each album group by dragging the respective tags into the *allowed* and *denied* fields. We incorporate both Tag clouds in our prototype to compare their effectiveness. The number of tags shown in a Tag cloud is also varied to study whether presenting tags only from the current album group's existing policies is better than presenting tags from all albums' existing policies.

$$TagSize_i = f_{max} - (f_{max} - f_{min}) * \frac{\sum_{j=1}^{No.\,MC} MCSen_j}{MCSenMax} \quad (1)$$

Where, f_{max} = Maximum font size of a tag
f_{min} = Minimum font size of a tag
$MCSen_j$ =Sensitivity of $Misconfiguration_j$
$MCSenMax$ = Misconfiguration with highest sensitivity amongst those caused by Tag_i


Album Group Policy Composition
Help
Submit
Album Group-1 (1/1)
Existing Policy
Compose Album Group Policy
Allowed Friends from this Album Group
Allowed Friends for this group
Family (1)
Everyone (2)
Friends (1)
College Friends (1)
Self (2)
Close Friends (1)
Denied Friends from this Album Group
Denied Friends for this group
Work Colleagues (8)
School Friends (2)
Album Group Policy Composition
Help
Submit
Album Group-1 (1/1)
Existing Policy
Compose Album Group Policy
Allowed Friends from this Album Group
Allowed Friends for this group
Family
Everyone
Friends
College friends
Self
Close Friends
Denied Friends from this Album Group
Denied Friends for this group
Work Colleagues
School Friends

(a) Frequency of use

(b) Misconfigurations

Fig. 2: Tag cloud visualization of existing album policies

B. Misconfiguration Scanning

After acquiring the user's sharing intentions in the form of album policies, we scan them based on our misconfiguration patterns and present the detected misconfigurations to the user. Our analysis of Facebook users' policy patterns (described in Section II) revealed the following possible access control misconfiguration patterns.

P1 The information item is visible to people outside the friend network

P2 A friend has been explicitly denied access to this information item, but is allowed access to other information items

P3 A Facebook smart list, which updates without user's interaction, has been used

P4 There are common friends between friend lists, which might have been the intended audience

P5 An empty friend list has been allowed or denied, resulting in unintended denial of access, and unintended sharing respectively

P6 One or more friends exist in both the allowed and denied fields, resulting in unintended denial of access

P7 The information item is empty

C. *Prototype Architecture*

We implemented a prototype of our proposed access control misconfiguration detection scheme. The prototype was built as a Facebook application called AlbumPrivacyScanner[1]. The application is hosted on our server and the back-end is based on PHP and MySQL. The client-side was implemented using Adobe Flex as a flash application. Upon installing the application, REST like Facebook APIs and Facebook Query Language are used to retrieve the user's album data, privacy settings and social connections. The collected data is transmitted over secure HTTPS based APIs to our server and stored in a MySQL database.

IV. Pilot Study

In designing our user study[2], we set out to answer the following questions:

Q1 What are the participants' sharing intentions?

Q2 How effective is our misconfiguration detection scheme w.r.t reducing policy misconfigurations?

Q3 What are the participants' perceptions of our proposed access control misconfiguration patterns?

A. *Design*

In order to answer our research questions, we built three tasks and a survey into our prototype application. For the first two tasks, we divided the participants into four groups. Group 1 was shown the frequency of policy use based Tag cloud constructed from the policies of albums within an album group, to serve as an indicator for helping them in policy selection. Group 2 was shown the frequency of policy use based Tag cloud constructed from the policies of all the user albums. Group 3 was shown misconfiguration based Tag cloud constructed from the policies of albums within an album group while Group 4 was shown misconfiguration based Tag cloud constructed from the policies of all the user albums. Task 1 and 2 involved only a subset of the participant's albums (for the purpose of the study). This subset was limited to 15 and included all the albums with access control misconfigurations (so that we can later compare the two Tag cloud approaches w.r.t reducing misconfigurations). These two tasks were intended to collect user's sharing intentions for album policies. Each participant was asked to group these albums according to the privacy settings that they wanted to assign to each group. In Task 2, the participants set permissions for the first album group using one of the assigned policy based Tag cloud. Then the participant was presented with the differences between the old and new policies of albums within this group, based on which they determined whether they want to adopt the new policy for that album or not. Task 2 was repeated for all the album groups. In Task 3, the participant's original album policies were scanned on our access control misconfiguration patterns described in Section III-B and they were asked to review and rate the detected misconfigurations. For each detected misconfiguration, the participant gave a rating by specifying whether they considered it a misconfiguration for that particular album or not and how serious it was. The seriousness responses were collected on a Likert-scale from 1(Low Seriousness) to 7(High Seriousness). Upon completion of the four tasks, the participant was asked to complete a short survey. First half of the survey comprised of demographic questions while the second half was focused on usability of our tool. Each question was designed to capture the participant's perceptions in the following areas:

Ease of Use: The participant should be able to detect the misconfigurations in their album policies easily and intuitively.

Readability: In addition to being easy to use, it should be understandable. An average user should be able to comprehend the involved tasks.

B. *Participants*

We recruited our participants from Amazon Mechanical Turk[3]. Amazon Mechanical Turk is a crowd sourcing marketplace which pairs requesters of work and workers. Requesters formulate work into Human Intelligent Tasks (HIT) which are individual tasks that workers complete. We set up our prototype Facebook application as a HIT. To better control the quality of the recruited participants, we mandated that each worker have a 95% HIT approval rating, or better. The HIT took approximately 10-15 minutes to complete, for which each worker was paid a fee of $0.50. A total of 96 participants successfully completed the pilot study, 49 male and 47 female. Most of our participants were young, fairly well educated and active Facebook users who were members for more than 2 years.

V. Study Results

This section discusses our pilot study results.

A. *Participants' Sharing Intentions*

We calculated the following metrics to evaluate our intention collection approach:

Number and size of album groups: Our sharing intention collection approach is based on the assumption that the users tend to have some albums with similar privacy settings. These albums can therefore be grouped together. For this purpose, we calculated the number of album groups created by a participant and the number of albums placed in one group.

Number of album policies: We compared the number of user album policies after using our approach, with previous number album policies, to analyze whether the user's sharing intentions are different than their actual policies

The album grouping statistics of our participants showed that at-least 3 of the participants' privacy settings were reused on multiple albums. Average group size was 4 showing that at-least 4 of the participant albums had the similar privacy settings.

The change in the number of policies was found out to be positive, demonstrating that the intended album policies

[1] https://apps.facebook.com/albumprivacyscanner/

[2] *Approved IRB Protocol # 11-08-01*

[3] https://www.mturk.com/

TABLE I: Comparison of Tag cloud visualizations

Freq based (Grp)	**Freq based (All)**	**Misconfig based (Grp)**	**Misconfig based (All)**	**Effect Size** r^2	**F-value**	**P-value**
Misconfigurations (before - after)						
9.16	7.07	9.30	5.37	0.04	1.45	0.23

were different than the actual album policies of the underlying participants. Dependent t tests showed that there is a significant difference between the number of policies the participants had before and after using our scheme, with a p-value of 0.004. One factor could be the participant's memory; they did not remember their actual policies and were of the opinion that the intended audience for the album is the same as its actual audience.

B. Tag Cloud Visualization Evaluation

In this section, we discuss the effectiveness of our learned data based Tag cloud visualization, in enhancing the participants' sharing intention model. We used misconfiguration change as the evaluation criteria. The misconfiguration change was calculated as: *Number of misconfigurations detected in the original policies - Number of misconfigurations detected after composing policies using Tag cloud*.

To determine the effect of Tag cloud on misconfigurations, we calculated the number of misconfigurations detected in participants' policies with and without using Tag cloud visualization. Table I shows the results for evaluation of Tag cloud visualizations with varying number of tags. Pairwise t tests on the number of misconfigurations before and after using Tag cloud showed that our scheme enabled the participants to decrease the number of misconfigurations in their policies. The difference in misconfigurations (before - after) is positive. However, One way ANOVA test to compare the misconfiguration change among the four Tag cloud visualizations revealed no significant difference between the decrease in misconfigurations according to the frequency of policy use Tag cloud with tags per album group, frequency of policy use Tag cloud with tags of all albums, misconfiguration based Tag cloud with tags per album group, misconfiguration based Tag cloud with tags of all albums.

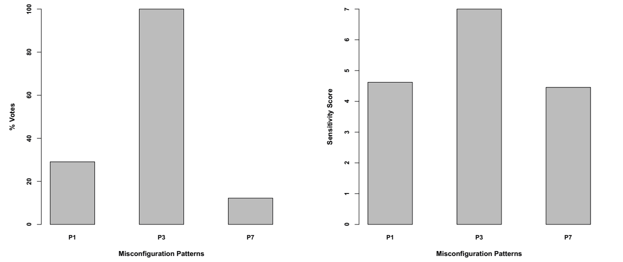
C. Participants' Perceptions

The participant perceptions of our access control misconfiguration patterns were gathered from their misconfiguration ratings, using the following criteria:

Misconfiguration Votes: The number of participants who considered a misconfiguration pattern important, out of the total number of participants who got that misconfiguration in one of their album policies.

Misconfiguration Seriousness: The participants rated the misconfiguration on a Likert scale (1-7), where 1 indicates low seriousness and 7 indicates high seriousness.

Amongst our 7 misconfiguration patterns, only 3 were detected in the participants' album policies. Figures **??** shows the participant perceptions of our misconfiguration patterns. Pattern P1(Album's visibility outside the friend network) was the most commonly detected misconfiguration pattern. Despite being the misconfiguration with highest privacy leak, only 30% of the participants considered it important, with seriousness scores of 4.5. It is possible that the participants, who did not vote for it, were aware of the audience represented by "public" setting and only gave public access to insensitive information. Pattern P3 (smart list usage) was only detected in the policies of 39% participants, and was considered important, receiving 100% votes and a high seriousness score of 7. This shows that the participants are unaware of the smart lists and their difference from the other friend lists. Pattern P7 (Empty album) was considered the least important and only received 12.22% votes with seriousness score of 4.45, demonstrating its importance to the participants who considered misconfiguration pattern P1 meaningful. Other misconfigurations involving more than one friend lists and user exceptions could not be detected, since most of our study participants did not have custom policies involving friend lists and exceptions. The average number of friend lists created per participant was 2 and the average number of smart lists per participant was 7. However, less than 10% of a participant's policies involved friend lists and user exceptions.



(a) % of votes received by misconfiguration patterns

(b) Seriousness score of misconfiguration patterns

Fig. 3: Participant Perceptions

Secondly, we performed a qualitative analysis of our misconfiguration detection application prototype, using the participant responses to our survey questions. The two usability metrics measured were, ease of use and readability, as discussed in Section IV-B. The average rating for readability and ease of use was greater than 5 on a Likert scale (1-7). This demonstrates that the participants easily understood the tasks involved in misconfiguration detection scheme and found the application's interface usable. The average time taken per participant to complete all the tasks was only 12.16 minutes.

VI. Related Work

Several efforts are being made to improve the end-user's ability to compose better access control policies on social networks. Egelman et al. [20] proposed a Venn diagram based privacy settings interface to cater for access control scenarios that lead to user errors, resulting in over-sharing of the data without user's knowledge. We leverage their scenarios related to common friends between friend lists, in our misconfiguration patterns. Recently, a general privacy wizard for social networks has been proposed to eliminate the burden of fine-grained policy specification from the users' shoulders [10]. The wizard gets user's input the policies for a small subset of their friends. A classifier is then trained on this data to specify privacy preferences for the rest of his friends. However, the wizard requires user input, so it is not possible to completely remove the policy specification task from the user.

Mazzia et al. [9] have proposed PViz, a policy visualization tool for social networks. The basis of their approach is that users conceive their networks in terms of communities and therefore want to see how a particular data item is visible to the friends in that community. While this is an interesting visualization scheme, they do not dig deeper into a Facebook item category e.g., photo albums, and treat it as a single item. Moreover, their scheme leaves it up to the user to discover misconfigurations. Our scheme detects the misconfigurations in a user's policies for Facebook items such as albums, which cannot be considered a single category. We also engage the user in the process to increase their understanding. Anwar et al. [8] have developed a reflective policy assessment tool which enables the user to view his profile impression as it appears to a particular friend. However, they use graphs in their user interface, which are difficult for an average user to understand. Lipford et al. [21] evaluate two policy presentation interfaces i.e, audience view and expandable grids and propose a combination of the two interface to get the best of the both worlds.

VII. Conclusion

In this paper, we proposed a scheme to detect and reduce the misconfigurations in access control policies on social networks, by capturing and enhancing the user's sharing intention model. The sharing intention model was collected with the help of user input in the form of album group policies. Tag cloud based policy visualization was used for policy composition—the existing policies were presented to the user together with extracted metadata, in order to guide their sharing intention model. The resulting album policies were scanned on our proposed misconfiguration patterns.

The users intended policies found out to be significantly different than their actual policies. Our scheme was able to detect the misconfiguration patterns in album policies. However, the reduction in the number of misconfigurations after using our approach was not significant. User perceptions of our misconfiguration patterns were collected in order to study the seriousness of the privacy threats they possessed. The qualitative analysis of our overall scheme demonstrated its ease of use and readability.

VIII. Acknowledgements

This research was partially supported by grants from the National Science Foundation (NSF-CNS-0831360, NSF-CNS-1117411) and a Google Research Award. We would like to thank Adharsh Desikan and Rahul Ramkumar for their help with the implementation of the user study application.

References

[1] I.-F. Lam, K.-T. Chen, and L.-J. Chen, "Involuntary information leakage in social network services," in *Proceedings of IWSEC'08*, 2008.

[2] N. Y. Times, "Facebook privacy: A bewildering tangle of options," http://www.nytimes.com/interactive/2010/05/12/business/facebook-privacy.html/, 2010.

[3] A. Acquisti and R. Gross, "Imagined communities: Awareness, information sharing, and privacy on the facebook," in *Privacy Enhancing Technologies*, 2006, pp. 36–58.

[4] L. Church, J. Anderson, J. Bonneau, and F. Stajano, "Privacy stories: confidence in privacy behaviors through end user programming," in *Proceedings of the 5th Symposium on Usable Privacy and Security*, ser. SOUPS '09, 2009, pp. 20–21.

[5] R. Gross and A. Acquisti, "Information revelation and privacy in online social networks," in *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*. ACM, 2005, pp. 71–80.

[6] H. Lipford, A. Besmer, and J. Watson, "Understanding privacy settings in facebook with an audience view," in *Proceedings of the 1st Conference on Usability, Psychology, and Security*. USENIX Association Berkeley, CA, USA, 2008, pp. 1–8.

[7] K. Strater and H. R. Lipford, "Strategies and struggles with privacy in an online social networking community," in *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction*, ser. BCS-HCI '08, 2008, pp. 111–119.

[8] M. M. Anwar and P. W. L. Fong, "A visualization tool for evaluating access control policies in facebook-style social network systems," in *Symposium On Applied Computing*, ser. SAC, 2012, pp. 1443–1450.

[9] A. Mazzia, K. LeFevre, and E. Adar, "The pviz comprehension tool for social network privacy settings," in *Symposium on Usable Privacy and Security*, ser. SOUPS, 2012, p. 13.

[10] L. Fang and K. LeFevre, "Privacy wizards for social networking sites," in *Proceedings of the 19th international conference on World Wide Web*, 2010, pp. 351–360.

[11] Y. Liu, K. Gummadi, B. Krishnamurthy, and A. Mislove, "Analyzing facebook privacy settings: User expectations vs. reality," in *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference*. ACM, 2011, pp. 61–70.

[12] "Profile watch," http://www.profilewatch.org/.

[13] "Privacy check," http://www.rabidgremlin.com/fbprivacy/.

[14] "Secure.me," https://apps.facebook.com/secure-me/.

[15] M. Madejski, M. Johnson, and S. Bellovin, "A study of privacy settings errors in an online social network," in *Pervasive Computing and Communications Workshops (PERCOM)*. IEEE, 2012, pp. 340–345.

[16] "Facebook statistics," http://newsroom.fb.com/Key-Facts.

[17] A. W. Rivadeneira, D. M. Gruen, M. J. Muller, and D. R. Millen, "Getting our head in the clouds: toward evaluation studies of tagclouds," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '07, 2007, pp. 995–998.

[18] M. A. Hearst and D. Rosner, "Tag clouds: Data analysis tool or social signaller?" in *Proceedings of the 41st Annual Hawaii International Conference on System Sciences*, ser. HICSS '08, 2008, pp. 160–.

[19] T. Eda, T. Uchiyama, T. Uchiyama, and M. Yoshikawa, "Signaling emotion in tagclouds," in *Proceedings of the 18th international conference on World wide web*, ser. WWW '09, 2009, pp. 1199–1200.

[20] S. Egelman, A. Oates, and S. Krishnamurthi, "Oops, i did it again: mitigating repeated access control errors on facebook," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI '11, 2011, pp. 2295–2304.

[21] H. R. Lipford, J. Watson, M. Whitney, K. Froiland, and R. W. Reeder, "Visual vs. compact: a comparison of privacy policy interfaces," in *CHI*, 2010.