A Visualization Tool for Evaluating Access Control Policies in Facebook-style Social Network Systems

Mohd Anwar
School of Information Sciences
University of Pittsburgh
Pittsburgh, Pennsylvania, USA
manwar@pitt.edu

Philip W. L. Fong
Department Computer Science
University of Calgary
Calgary, Alberta, Canada
pwlfong@ucalgary.ca

ABSTRACT

Understanding the privacy implication of adopting a certain privacy setting is a complex task for the users of social network systems. Users need tool support to articulate potential access scenarios and perform policy analysis. Such a need is particularly acute for Facebook-style Social Network Systems (FSNSs), in which semantically rich topology-based policies are used for access control. In this work, we develop a prototypical tool for Reflective Policy Assessment (RPA) — a process in which a user examines her profile from the viewpoint of another user in her extended neighbourhood in the social graph. We verify the utility and usability of our tool in a within-subject user study.

Categories and Subject Descriptors

H.1.2 [**Models and Principles**]: User / Machine Systems—*Human Factor*; D.4.6 [**Operating Systems**]: Security and Protection—*Access Control*; K.4.1 [**Computers and Society**]: Public Policy Issues—*Privacy*

General Terms

Security, Human Factors

Keywords

Access control, Reflective policy assessment, Visualization, Usability

1. INTRODUCTION

Impression management [12, 22] is one of the reasons why privacy is considered so important. This is particularly true in the context of social network systems [5]. A profile owner selectively grants a profile viewer access to her profile items in accordance with the impression she wants to convey. For example, say Jill is a friend of Alice, and Bob is a friend of Jill. For proper impression management, Alice may grant Jill, but not Bob, access to her sorority photo album. To check whether her policy allows her to convey the desired impression, Alice may want to find out what items of her profile Bob as well as Jill can see. In our everyday life, we look into a mirror to get a sense of what others see when they look at us. The term *Reflective Policy Assessment (RPA)* [1] is used to refer to this process of assuming the position of a potential accessor for the sake of assessing the privacy implications of access control policies.

Authorization in a social network system is primarily based on the topology of the social graph, which is co-constructed by all the users of the system. It is therefore difficult for a user to mentally keep track of the topology of her constantly changing social network. Furthermore, one's needs for privacy is constantly evolving, requiring a user to constantly perform policy assessment. As a result, RPA is a complex task. Tool support is definitely desirable.

This need for RPA is particularly acute in *Facebook-style Social Network Systems (FSNSs)* [9, 2, 7]. Such systems support *topology-based* access control policies, whereby accessibility is determined by the present topology of the social graph. For example, Alice may adopt the policy that grants access to her sorority photo album only if the accessor shares three common friends with her. Because topology-based policies can be used for expressing complex trust delegation, the need for RPA becomes even more important.

This paper is about the development and evaluation of a policy analysis tool for FSNSs to facilitate RPA. The visualization tool helps a user analyze her access control policies by: (a) visually depicting the extended neighbourhood of her social graph and (b) allowing her to inspect her profile from the view point of another user (a potential accessor) at her extended neighbourhood. Our contributions are the following:

- We develop a prototypical visualization tool for supporting RPA in FSNSs. Since this tool does not require the knowledge of access control policies of all the users of the system, it can be implemented on the client side (e.g., as a third-party Facebook application).
- We design a simulated environment for evaluating this tool in a user study in such way that the study is generalizable, and the privacy of participants are preserved.
- We conduct a within-subject user study to verify the utility and usability of our tool.

The organization of this paper is as follows. Section 2 describes FSNSs and RPA. In Section 3, we present the implementation of the prototype and experiment design. In

SAC'12. March 25–29, 2012, Riva del Garda, Italy

Policy	*When is access allowed*
distance$_k$	distance between owner and accessor is no more than k
clique$_k$	owner and accessor belong to the same k-clique (i.e., they belong to the same close-knit group)
common-friends$_k$	owner and accessor share k common friends (i.e., accessor is a known quantity)

Figure 1: A sample of topology-based policies

Section 4, we present methodology and results of the user study. Section 5 surveys related literature, and section 6 concludes the paper.

2. REFLECTIVE POLICY ASSESSMENT FOR FSNSs

2.1 Facebook-Style Social Network Systems

Facebook-style Social Network Systems (FSNSs) [9, 2, 7] are generalizations of the access control mechanism found in Facebook. One characteristic of Facebook is that access control policies are *topology-based* [9, 2, 7]. Specifically, rather than explicitly identifying the identities of users who are allowed access to a resource, the owner of that resource specifies a desired relationship between herself and a legitimate accessor. For example, by adopting a policy of friends-of-friends, the owner of a photo album requires that only those users within a distance of two from her in the social graph are allowed access to that album. Facebook provides a standard vocabulary of policies (i.e., no-one, only-me, friends, friends-of-friends, everyone) from which resource owners may choose from.

An FSNS is an information-sharing platform that adopts an access control mechanism similar to that of Facebook, with the exception that the policy vocabulary may contain topology-based policies that are not yet provided by Facebook. Specifically, an FSNS tracks a social graph of the users. Every resource has an owner, who can impose on the resource an access control policy chosen from the policy vocabulary of that FSNS. The policies in the policy vocabulary are topology-based. When a user requests access to a resource, the reference monitor will check that the resource owner and the resource accessor are related in a way prescribed by the access control policy of that resource.

2.2 Topology-based Policies

A topology-based policy [9, 2, 7] is essentially a predicate that, when given a social graph, an owner vertex and an accessor vertex, returns a boolean authorization decision. In addition, such a predicate does not base its authorization decision on the identities of the owner and the accessor, but instead relies only on the topology of the social graph. The standard vocabulary of access control policies offered by Facebook are clearly topology-based. There are, however, other useful topology-based policies that are not yet supported by Facebook, but nevertheless capture important social concepts. Figure 1 gives a sample of topology-based policies that have been studied in previous work [9, 2, 7].

Armed with topology-based policies, FSNSs support the expression of access control policies with rich social significance. Specifically, topology-based policies allows resource owners to express delegation of trust in a natural manner. For example, by adopting the policy friends-of-friends as the access control policy of one's photo album, one is effectively delegating to her friends to decide who may access the album. Yet, with an ever-evolving social graph, and the rich semantics of topology-based policies, it is cognitively challenging for an FSNS user to understand the privacy implications of adopting a certain topology-based policy. "Exactly who are the people who can access this photo album?" "What does my profile look like to people in different regions of the social graph?"

2.3 Reflective Policy Assessment

To create a desired impression, we repeatedly look into the mirror and adjust our getup until we are satisfied. A mirror allows us to see what others see when they look at us. The process of formulating access control policies is similar to what it takes to create a desired look. With an ever-changing social graph and ever-changing privacy requirements, a user needs to repeatedly assess and adjust her policies. One way to achieve this is to examine the appearance of her profile from the perspective of various kinds of potential accessors, in order to check if the access control policies of her various profile items are formulated properly, so that she conveys the right impressions to the right kinds of potential accessors (e.g., a fun-looking profiles to her buddies, but a more sensible look to those not familiar to her). In previous work [1], we use the term *Reflective Policy Assessment (RPA)* to refer to this kind of policy analysis that are achieved through the metaphor of "mirror-looking".

To support RPA, a visualization technique has been proposed [1]. The proposed tool provides a visual representation of an extended neighbourhood (e.g., all users within a distance m, for some small m) of a profile owner in the social graph. The profile owner may specify the size of her extended neighbourhood. The profile owner may then point to any user in the extended neighbourhood as a potential accessor of her profile. This action signals to the tool that the profile owner intends to position herself as the selected user and examine her profile from the viewpoint of that user. The tool displays a succinct representation of the profile, as accessible by the potential accessor. This tool allows a user to conduct the following kinds of policy analysis:

What-if Analysis: It allows a profile owner to perform "what-if" analysis on her access policies. More specifically, it allows her to assess the adequacy of her access policies in concrete access scenarios, and to evaluate the effect of adopting these policies when her extended neighbourhood possesses a certain topological structure.

Targeted Effort: By displaying how other users are topologically related to a profile owner, the tool helps her identify topologically interesting nodes in the extended neighbourhood, thereby allowing her to properly target her policy assessment effort.

2.4 Privacy-preserving RPA

An unrestricted view of the extended neighbourhood of a user can breach the privacy of other users. Suppose Alice is in the extended neighbourhood of Bob. Suppose further that the friends (or their friends, etc) of Alice have set up the access control policies of their friend lists in such a way that these friend lists are not accessible by Bob. Then Alice is not reachable by Bob by traversing the social graph, and thus the existence of Alice is a private information that is

not supposed to be known by Bob. An RPA tool that indiscriminately depicts the extended neighbourhood of Bob will compromise the privacy of Alice.

An accurate rendering of the extended neighbourhood, however, is not necessary for RPA. Rather, an approximate rendering of the extended neighbourhood should suffice so long as the approximation exhibits the typical topology of social networks. Therefore our proposed tool renders the reachable region of the profile owner's extended neighbourhood as is, but approximates the unreachable region of the extended neighbourhood by randomly generating synthetic nodes and edges in a way that preserves such properties of social networks as power law vertex degree distribution [6] and small-world characteristic [21]. (This is achieved in part by adapting the R-MAT graph generation algorithm [4].) Since our generated graph preserves the properties of online social networks, the approximated neighbourhood would cover topologically interesting access scenarios needed by the profile owner for conducting RPA against unreachable nodes. Details of the extended neighbourhood generation algorithm can be found in [1].

2.5 Research Problem

The goal of this paper is to find out whether the proposed RPA visualization tool is effective in assisting profile owners in comprehending the privacy consequence of adopting certain topology-based access control policies.

3. PROTOTYPE & EXPERIMENT

3.1 Prototype Implementation

To measure in what extent RPA helps users understand privacy implications of their topology-based access control policies, we developed a prototype system with following components: (i) an interface to create profiles, including profile items and friend list (Figure 2 (A) and (B)), (ii) a tutorial on topology-based policies (Figure 2 (C)), (iii) an interface to author topology-based policies for each profile item (Figure 2 (D)), (iv) a tool to perform reflective policy assessment (RPA) (Figure 2 (F)), and (v) an environment to test users' understandings of the implications of their policies and to survey users' attitudes towards our tool.

The prototype system is built as a Desktop Application on Mac OS X with Adobe Flex SDK 3.2 and Adobe AIR runtime environment. The development of the tool for RPA (component (iv) of the system) involves three distinct tasks: (1) to generate a graph of the extended neighbourhood of a user, (2) to visualize the graph (generated at task (1)) to the user, and (3) to allow the user interact with the graph to perform RPA at any node of the graph. For task (1), we have implemented the algorithm in [1], within which synthetic edges are generated using R-MAT [4] algorithm. For task (2), we have used Kap Lab's Visualizer[1] to render the graph. For task (3), we have used profile information and authored policy (input received from component (i) & (iii) of the system respectively) of the user and topological information of the generated graph to compute what profile items are accessible from different nodes of the graph. Based on the user's mouse over selection of a node, we display a configuration of her profile accordingly.

[1]http://lab.kapit.fr/display/kaplabhome/Home

3.2 Experiment Design

The aim of this experiment is to address the following research question: To what extent does our visualization technique facilitate the assessment of access control policies in FSNSs? If the tool is effective in supporting policy analysis, we should observe that users perform more accurate policy analysis with the tool than without tool. An empirical user study will help us test if this is indeed the case. Such a user study shall compare the policy analysis by the user in two configurations: (i) no tool is available; (ii) tool is available.

With performing the user study, we face two challenges.

Testbed. How do we build a testbed to run the proposed user study? A deployed FSNS, such as Facebook, would have been a convenient environment to conduct the proposed user study. There are, however, two problems with this approach. First, not all topology-based policies are supported in Facebook. As a result, the effectiveness of reflective policy assessment against advanced topology-based policies cannot be gauged. Second, such a study will harvest information of users located in the extended neighbourhood of a participant. This setup thus requires consent from a population much larger than the participating group. Even if the institutional research ethics committee approves this aggressive experimental design, successfully obtaining consent from such a large population is not likely. To resolve this problem, we design a simulated environment that addresses these privacy challenges.

Ecological validity. Another challenge in this experimental design is to realistically simulate experiences that users have in the articulation of privacy issues and authoring of privacy policies in social network systems. In other words, in order to make a true effort to understand the implication of their privacy policies, subjects need to be able to express their privacy desires in their policies. Besides, policy authoring process should not be complex or unfamiliar to them so that they can easily author realistic policies according to their desire for privacy. To address this ecological validity challenge, we have made following design decisions in our experimental apparatus (Figure 2) including the prototypical policy visualization tool:

1. The experimental apparatus presents a set of privacy sensitive profile items under 8 categories. The categories are following: basic information, likes or interests, contact information, affiliation, education or work, photos, and videos. The subjects pick the most privacy sensitive profile item under each category. The apparatus allows subjects to provide two privacy-sensitive profile items besides the ones suggested to them. By allowing each subject to choose a set of privacy sensitive profile items, we help them express their privacy desires in their policies.

2. For the immediate neighbourhood (i.e., friend list), subjects are asked to provide a list of friends. These friends include school friends, work friends, family members, and others. The tool chooses the extended neighbourhood. By populating the immediate neighbourhood of a subject with her provided list of friends, we help them perceive privacy risks similar to their operational social network.

3. Due to the novelty of the three topology-based policies, namely clique_k, $\mathsf{distance}_k$ and $\mathsf{common\text{-}friends}_k$, a tutorial

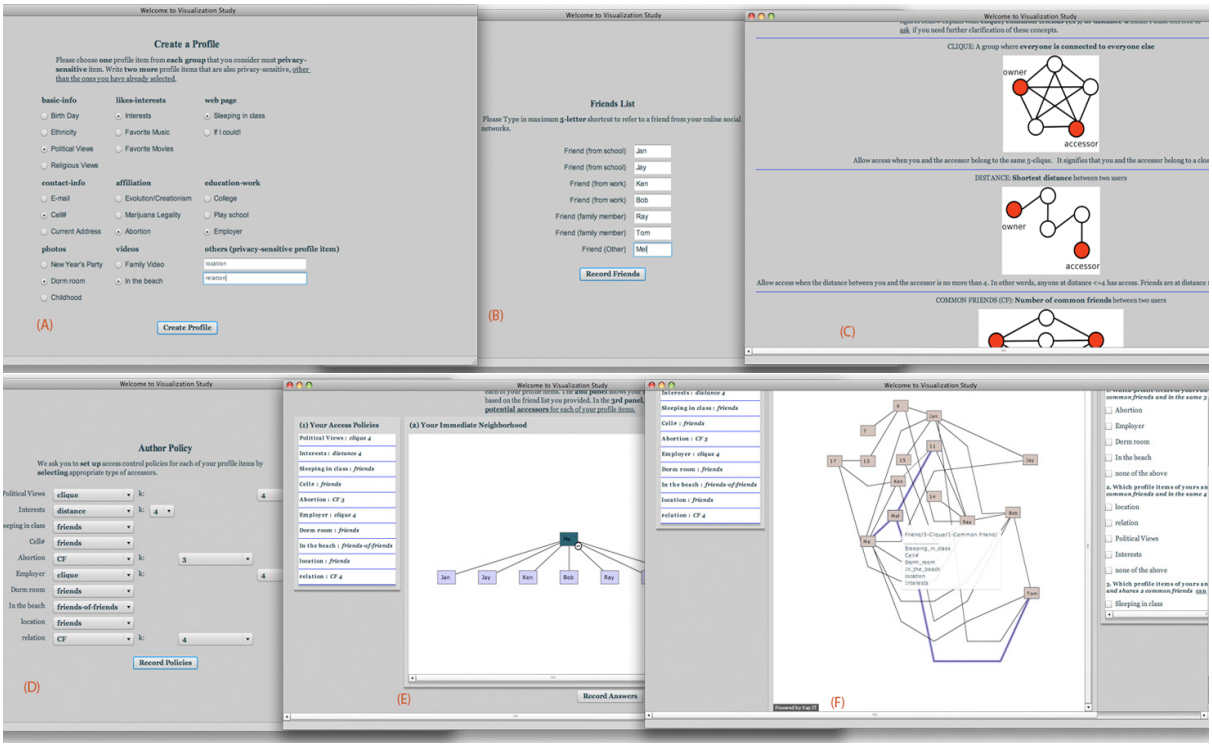

Figure 2: Experiment and Prototype Interface: (A) Interface to create profile, (B) Interface to provide friend-list, (C) Tutorial on topology-based policies, (D) Interface to author policies, (E) Interface for policy analysis without tool, (F) Interface for policy analysis with tool.

is provided. Furthermore, subjects are told during the study to ask any question they may have regarding these policies.

4. To ensure that policy authoring itself is not a cumbersome task, the policy authoring facility is provided by means to easy drop-down privacy settings (similar to privacy settings of Facebook).

4. USER STUDY

4.1 Methodology

Observational approach. When a user formulates access policies using privacy settings of an FSNS, they articulate on access scenarios in terms of few predefined policy vocabularies such as "friends". Understanding privacy implications of access control policies boils down to identifying which profile items are accessible to accessor at different access scenarios. A subject may think that she knows exactly who have access to her profile items when she may not know or vice versa. Therefore, a subject's knowledge needs to be tested on "what profile items are accessible to certain accessors". To test the effect of our visualization tool, we have conducted a within-subject experiment with two conditions: (a) subjects perform policy analysis without our tool. (b) subjects perform policy analysis with our tool. Observational approach is complemented with post-use survey and brief informal interview questionnaire.

Attitudinal approach. We conducted a post-use survey to know the subjects' attitudes towards our visualization tool. We also inquired their attitude towards privacy settings in FSNS in general, and whether a visualization tool like ours would help in access control policy analysis. Informal Short Interview. We further conducted short interview to augment the post-use survey to collect rich detailed data that is not possible to gather from the survey. We observed that only a couple of subjects attempted the open ended survey question on "general comments", whereas they provided anecdotal account of their use experience and make constructive suggestions for improving our tool during short interview.

Study setup. The conjoint faculties research ethics board at the University of Calgary approved the study and all participants provided written informed consent prior to their participation. This study was approved as a minimal risk study by the ethics board. Subjects received a financial compensation of $30 CDN for their participation. The order of treatments (policy analysis test without the tool and policy analysis test with the tool) were randomly assigned to subjects. All subjects reported to be regular user of at least one social network system. We piloted the system before the actual test. The study was set up as a within-subject design with policy analysis tool as the single factor. An advantage of within-subjects designs is that individual differences in subjects' overall levels of performance are controlled by comparing the scores of a subject in one condition to the scores of the same subject in other conditions.

4.2 Demographics

Figure 3 illustrates the demographics of our study population. Out of thirty six subjects, 69.44% were male and 30.56% were female. 80.56% of our subjects were students,

Gender:	Male: 25; Female: 11
Age:	Range: 18..40 years
Occupation:	Students: 29; Professionals: 7
Education:	Undergrad students: 18; With Bachelor: 6; Master students: 5; PhD students: 4; With Master: 2; ESL students: 1

Figure 3: Demographic information of subjects

while 19.44% of them were professionals.

4.3 Policy Analysis with Tool

In a simulated environment, each subject is assigned with policy analysis task twice - once with the tool and once without the tool in a random order. We group our study subjects into two treatments:

Treatment 1: subjects perform policy analysis without the tool first and then with the tool; and

Treatment 2: subjects perform policy analysis with the tool first and then without the tool.

In the policy analysis task, each subject is asked to answer multiple-choice questionnaire based on their chosen policy for their profile items. These questions are generated to test whether a subject can tell which of her profile items are available in different access scenarios. Each of these questions has following form: *Which profile items of yours an accessor who is X can access?, where X = a privileged user identified through topology-based policy vocabularies.* A sample question could be the following: *Which profile items of yours an accessor who shares 2 common-friends with you and in the same 3-clique can access?*

When the task is performed without the tool, a subject needs to mentally evaluate their policies against the access scenario. If policy analysis is done with tool support, the subject is presented with a graph representing her extended neighbourhood. To identify a specific access scenario, all that the subject needs to do is to hover over the various vertices of the graph, in search of the access scenario presented in the question. On mouse over, each node of the graph shows the access scenario that it represents. On selection, each node also shows the configuration of the subject's profile as seen from the perspective of that node. In summary, for policy analysis with the tool, a subject just needs to find the node in her extended neighbourhood (graph) that represents the access scenario of her interest. Finding the node of interest is as simple as hovering the graph.

Figure 4 shows the comparison of policy analysis test scores with and without the tool support of a subject in **Treatment 1** (i.e., without tool first, then with tool). Figure 5 shows the comparison of policy analysis test scores with and without the tool support of a subject in **Treatment 2** (i.e., with tool first, then without tool). The policy analysis test score is calculated as percentage of correct answers. With these two figures (**Treatment 1** and **2**) combined, we see that all but one subjects scored higher with tool support, while one subject's score remained the same. Interestingly, the subjects in **Treatment 2** scored higher than the subjects in **Treatment 1**. The descriptive statistics on test scores in Figure 6 shows that all mean, median, mode, minimum, and maximum scores are higher with tool support.

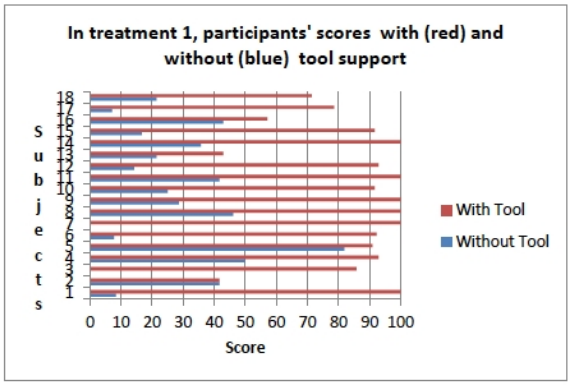

Figure 4: A within-subject comparison of test scores in Treatment 1

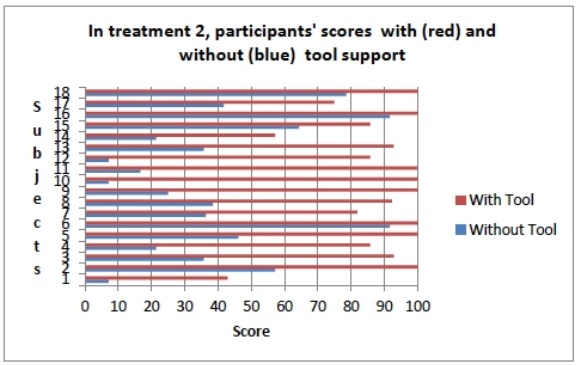

Figure 5: A within-subject comparison of test scores in Treatment 2

Using t-test, subjects' test scores without the tool support were compared to their test scores with the tool support. As shown in Figure 7, the policy analysis test scores were significantly higher with the tool support (Mean = 86.71) than without tool support (Mean = 33.72) as indicated by a significant t-test, $t(35) = 11.62$ and $p < 0.01$. This finding indicates that the visualization tool significantly helps subjects understand who can or cannot access their profile items.

4.4 Survey Questions

Upon completion of the policy analysis task, we asked the subjects to take a post-use survey. In the survey, we asked 11 questions on following topics: subjects' social network use, subjects' familiarity with privacy settings, subjects' experience on policy analysis, and subjects' attitudes towards our

	W/o Tool	With Tool
Mean	33.72	86.71
Standard Error	4.14	2.93
Median	32.14	92.58
Mode	21.43	100.00
Standard Deviation	24.83	17.60
Minimum	0.00	41.67
Maximum	91.67	100.00
Count	36	36

Figure 6: Descriptive statistics on test scores

	W/o Tool	With Tool
Mean	33.72	86.71
Variance	616.45	309.76
Observations	36	36
Pearson Correlation	0.20	
Hypothesized Mean Difference	0	
df	35	
t Stat	-11.62	
p-value	< 0.01	

Figure 7: Paired t-test statistics

visualization tool. The survey responses indicate that the subjects of our study extensively use social network systems (SNSs): majority of them are Facebook users and many of them use multiple SNSs. A 41.67% of them have more than 150 friends. Our subjects have experience of using privacy settings, while majority of them feel that privacy settings are sometimes inadequate or just inadequate to their privacy desires. A 44.44% of the subjects think that policy analysis is hard while 33.33% of the subjects has never tried or unsure of policy analysis. A 77.78% think that the visualization tool can help in policy authoring by providing feedback on who can access what profile items. A 63.89% think that they would obviously enjoy policy authoring with our tool while 27.78% think that they would probably enjoy policy authoring with tool. More details on the survey responses are presented in Figure 8.

4.5 Short Interview

In the short interview, we sought open ended comments and attitudes of the subjects on two items: visualization tool and topology-based policies. Thirty-four of thirty-six subjects provided us some comments on the tool or policies or both. In these comments, subjects expressed the perceived values from the tool and topology-based policies and provided us suggestions to improve the tool. One important comment on the perceived value of the tool is about awareness: "after using the tool, I understand that lot of people can access my profile than what I thought."

Visualization tool. Thirty-four subjects commented on our tool. Based on the perceived value from the tool, we grouped these comments into 3 categories: (i) very useful (9 comments), (ii) useful (18 comments), (iii) somewhat useful (7 comments). For example, comments in the category (i) include, "The tool is very helpful, provides more control, and without (the tool) it is impossible to understand who has access to what profile item." Three of the subjects provide us suggestions to improve the tool. Suggestions include comments like, "The tool would have been more useful if the nodes were color coded based on access scenarios."

Topology-based policies. Nineteen subjects commented on the topology-based policies for which our tool is used. Based on the perceived value from topology-based policies, we grouped these comments into 3 categories: (i) very useful (4 comments), (ii) useful (10 comments), (iii) somewhat useful (5 comments). Out of three topology-based policies (that our tool supports but not available in any social network system), 6 of the subjects liked the $\mathsf{common\text{-}friends}_k$ policy, 3 of the subjects liked the $\mathsf{distance}_k$ policy, and 1 subject liked both the $\mathsf{common\text{-}friends}_k$ and $\mathsf{distance}_k$ policies. Interestingly, these subjects identified the rationale behind the policies of their likings. For example, one subject comments: *"Distance policy helps to think about strangers."*

Social Networks (2 questions)
1. *What SNS do you use?* Facebook: 32; MySpace: 7; LinkedIn: 3 Twitter: 6; Others: 15
2. *How many SNS friends do you have?* ≤ 50: 9; 51-100: 8; 101-150: 4; > 150: 15
Privacy Settings / Access Policy (3 questions)
1. *How often do you check it?* Whenever adding contents: 18; Once/month: 9 Never: 8; Many times/month: 1; No response: 1
2. *When do you consider changing it?* Befriending: 13; Whenever adding contents: 11 Sending/receiving invitation: 8 De-friending: 6; Never: 3; Writing journal: 1 Notice my info on others wall: 1
3. *How adequate is it to your privacy desire?* Sometimes inadequate: 16; Not sure: 9 Adequate: 6; Inadequate: 5
Policy Analysis (1 question)
1. *How easy is the task?* Hard: 18; Not sure/never tried: 12 Too easy: 5; Easy: 2; Too hard: 1
Visualization Tool (5 questions)
1. *Does tool help in policy authoring/privacy setting?* Agree: 22; Strongly agree: 6; Not sure: 5 Disagree: 2; No response: 1
2. *Does tool help in analysis of topology-based policy?* Agree: 21; Strongly agree: 8; Not sure: 4 Disagree: 2; No response: 1
3. *If such tool available, would you review/change privacy settings more?* Probably: 17; Obviously: 15; Not sure: 3 No response: 1
4. *Would you enjoy policy analysis more with the tool than w/o?* Obviously: 23; Probably: 10; Not sure: 3
5. *With the tool, would be more confident about privacy settings?* Obviously: 20; Probably: 14; Not sure: 1 No response: 1

Figure 8: Survey questions & answer summary

5. RELATED WORK

This work is an extension of our previous work [1], in which we first articulated the idea of Reflective Policy Assessment (RPA), the privacy challenge arises from this kind of policy analysis, and a privacy-preserving procedure for approximating the extended neighbourhood of the profile owner. The present work extends the previous work in two major ways. First, we report a prototype implementation of a visualization tool for supporting RPA. Second, we conduct a within-subject user study to verify the utility of RPA and the usability of our visualization tool.

Assessing the security implications of access control policies traditionally lies in the domain of safety analysis [14, 20], or, more recently, security analysis [19, 18]. When the projection of security implications becomes a challenging computational problem, safety or security analyses are indispensable. While appreciating the scope and analytical rigor of such approaches, this work seeks to address the cognitive challenges of users in the projection of the privacy implications of their access control policies.

It is difficult for users to understand the overall effect and consequences of their access control policies. As a result,

the research community has started developing tool support for policy analysis. In [17], Kolovski *et al.* developed policy assessment tool to detect redundant policies. Gofman *et al.* developed RBAC-PAT for analyzing RBAC and ARBAC policies [13]. Yee used data flow charts for visualizing the flow of privacy-sensitive data [27].

A visualization tool can reduce the cognitive load of users in policy analysis, in particular, in RPA [1]. It is also a better fit with the requirements of impression management. Visualization techniques have long been used in social network analysis [11]. With the soaring popularity of online social networks, visualization techniques are widely used to empower users of such networks. For example, Heer and boyd employed visualization techniques for exploration and navigation of large-scale online social networks [15]. Facebook offers a profile owner to see how a friend sees her profile[2] .

As a basis for usable security, some visualization solutions for access-control and file-sharing policies are presented in [24]. Vaniea *et al.* developed visualization tool for security professionals that visualizes the output of policy analysis and shows the effect of the policy changes [26]. Heitzmann *et al.* developed treemap-based visualization of access control for the NTFS file system that can help a non-expert user understand and manipulate file system permissions in a simple and effective way [16]. Ueno *et al.* developed an access control interface, namely Soramame [25], that extracts and visualizes the data-flows of access control policies and uses animation to help users better understand the policies.

Reeder *et al.* proposed a visualization technique to support authoring of security policies [23], whereby the access control matrix is rendered as an expandable grid representation. Reeder *et al.*'s works and ours share a common underpinning of visualizing authorization decisions under the assumption of some security policies. In our work, when a profile is displayed from the viewpoint of a potential accessor, we are essentially rendering a segment of a row in access control matrix corresponding to that accessor. Our work is distinct from their work on two counts: (i) our work is tailored for the assessment of topology-based policies in FSNSs, and (ii) we address the additional concern of preserving the privacy of potential accessors.

To the best of our knowledge, we are the first to propose **a visualization tool for supporting the assessment of access control policies in social network systems**. Our proposed visualization technique supports impression management for a family of FSNSs. This family was defined in [9, 2], which formally specify an access control model that delineates the design space of FSNSs. A distinctive feature of FSNSs is that no global name space is available for identifying users, and thus access control policies are specified in terms of the topology of the social graph. This element of distributed access control causes policy assessment to be a nontrivial undertaking, thereby necessitating our visualization technique.

A number of recent proposals attempt to advance beyond the access control mechanisms found in commercial social network systems. An example is that of Carminati *et al.*, in which a decentralized social network system with relationship types, trust metrics and degree-of-separation policies is developed [3]. Another example is Relationship-Based Access Control (ReBAC) [8, 10], in which the relationship between a resource owner and a resource accessor in a poly-relational social network is used as the basis of authorization decisions. An interesting research direction is to extend RPA for these next-generation access control systems.

[2]http://www.facebook.com/privacy/?view=profile

6. CONCLUSION

We developed a visualization tool to help a profile owner in a Facebook-style Social Network System analyze her access control policies by displaying how potential accessors at her extended neighbourhood are topologically related to her, and allowing her to visually analyze her policies via a mirror-like facility from the view point of a potential accessor of her interest. We conducted a within-subject user study with two conditions: policy analysis without our visualization tool and policy analysis with our visualization tool. Results of the study show that subjects were able to perform (statistically significantly) more accurate policy analysis with the tool than without the tool.

7. ACKNOWLEDGMENTS

This work is funded in part by an NSERC Strategic Project Grant, and has benefited from the in-kind support of Security Resource Group Inc.

8. REFERENCES

[1] Mohd Anwar, Philip W. L. Fong, Xue-Dong Yang, and Howard Hamilton. Visualizing privacy implications of access control policies in social network systems. In *Proceedings of the 4th International Workshop on Data Privacy Management (DPM'09)*, volume 5939 of *LNCS*, pages 106–120, Saint Malo, France, September 2010.

[2] Mohd Anwar, Zhen Zhao, and Philip W. L. Fong. An access control model for Facebook-style social network systems. Technical Report 2010-959-08, Department of Computer Science, University of Calgary, Canada, 2010. Submitted for review.

[3] Barbara Carminati, Elena Ferrari, and Andrea Perego. Enforcing access control in web-based social networks. *ACM Transactions on Information and System Security*, 13(1), October 2009.

[4] D. Chakrabarti, C. Faloutsos, and Y. Zhan. Visualization of large networks with min-cut plots, A-plots and R-MAT. *International Journal of Human-Computer Studies*, 65(5):434–445, 2007.

[5] C. Dwyer, S. R. Hiltz, M. S. Poole, J. Gussner, F. Hennig, Osswald Sebastian, Sandrea Schliebelerger, and B. Warth. Developing reliable measures of privacy management within social networking sites. In *Proceedings of the 43rd Hawaii International Conference on System Sciences (HICSS)*, pages 1–10. IEEE Computer Society, 2010.

[6] M. Faloutsos, P. Faloutsos, and C. Faloutsos. On power-law relationships of the internet topology. *ACM SIGCOMM Computer Communication Review*, 29(4):251–262, 1999.

[7] Philip W. L. Fong. Preventing Sybil attacks by privilege attenuation : A design principle for social network systems. In *Proceedings of the 2011 IEEE Symposium on Security and Privacy (S&P'11)*, pages 263–278, Oakland, California, USA, May 2011.

[8] Philip W. L. Fong. Relationship-based access control: Protection model and policy language. In *Proceedings of the First ACM Conference on Data and Application Security and Privacy (CODASPY'11)*, pages 191–202, San Antonio, TX, USA, February 2011.

[9] Philip W. L. Fong, Mohd Anwar, and Zhen Zhao. A privacy preservation model for Facebook-style social network systems. In *Proceedings of the 14th European Symposium on Research In Computer Security (ESORICS'09)*, volume 5789 of *LNCS*, pages 303–320, Saint Malo, France, September 2009.

[10] Philip W. L. Fong and Ida Siahaan. Relationship-based access control policies and their policy languages. In *Proceedings of the 16th ACM Symposium on Access Control Models and Technologies (SACMAT'11)*, pages 51–60, Innsbruck, Austria, June 2011.

[11] Linton C Freeman. Visualizing social networks. *Journal of Social Structure*, 1(1):151–161, 2000.

[12] E. Goffman. *The Presentation of Self in Everyday Life*. Anchor, New York, NY, USA, 1959.

[13] Mikhail I. Gofman, Ruiqi Luo, Ayla C. Solomon, Yingbin Zhang, Ping Yang, and Scott D. Stoller. Rbac-pat: A policy analysis tool for role based access control. In *TACAS '09: Proceedings of the 15th International Conference on Tools and Algorithms for the Construction and Analysis of Systems*, pages 46–49. Springer-Verlag, 2009.

[14] Michael A. Harrison, Walter L. Ruzzo, and Jeffrey D. Ullman. Protection in operating systems. *Communications of the ACM*, 19(8):461–471, 1976.

[15] J. Heer and D. Boyd. Vizster: visualizing online social networks. In *IEEE Symposium on Information Visualization 2005 (INFOVIS 2005)*, pages 33–40. IEEE, 2005.

[16] Alexander Heitzmann, Bernardo Palazzi, Charalampos Papamanthou, and Roberto Tamassia. Effective visualization of file system access-control. In *Proceedings of International Workshop on Visualization for Cyber Security (VizSec)*, pages 18–25. Springer, 2008.

[17] Vladimir Kolovski, James Hendler, and Bijan Parsia. Analyzing web access control policies. In *Proceedings of the 16th international conference on World Wide Web - WWW '07*, pages 677–686. ACM Press, 2007.

[18] Ninghui Li and Mahesh V. Tripunitara. Security analysis in role-based access control. *ACM Transactions on Information and System Security*, 9(4):391–420, 2006.

[19] Ninghui Li, William H. Winsborough, and John C. Mitchell. Beyond proof-of-compliance: Safety and availability analysis in trust management. In *Proceedings of IEEE Symposium on Security and Privacy*, pages 123–139. IEEE Computer Society Press, 2003.

[20] R. J. Lipton and L. Snyder. A linear time algorithm for deciding subject security. *Journal of the ACM*, 24(3):455–464, 1977.

[21] Stanley Milgram. The small world problem. *Psychology Today*, 2(1):60–67, 1967.

[22] S. Patil and A. Kobsa. Privacy as impression management. Technical Report UCI-ISR-03-13, Institute for Software Research, University of California - Irvine, Irvine, CA, USA, 2003.

[23] Robert W. Reeder, Lujo Bauer, Lorrie Faith Cranor, Michael K. Reiter, Kelli Bacon, Keisha How, and Heather Strong. Expandable grids for visualizing and authoring computer security policies. In *Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems (CHI '08)*, pages 1473–1482, New York, NY, USA, 2008. ACM.

[24] Jennifer Rode, Carolina Johansson, Paul Digioia, Roberto Silva Filho, Kari Nies, David H Nguyen, Jie Ren, Paul Dourish, and David Redmiles. Seeing further : Extending visualization as a basis for usable security. In *SOUPS '06*, pages 145–155. ACM Press, 2006.

[25] Nachi Ueno, Ryota Hashimoto, Michio Shimomura, and Kenji Takahashi. Soramame: what you see is what you control access control user interface. In *Computer Human Interaction for the Management of Information Technology (CHIMIT '09)*, 2009.

[26] Kami Vaniea, Qun Ni, Lorrie Cranor, and Elisa Bertino. Access control policy analysis and visualization tools for security professionals. In *In USM'08: Workshop on Usable IT Security Management*, 2008.

[27] George Yee. Visualization for privacy compliance. In *VizSEC 06: Proceedings of the 3rd international workshop on Visualization for computer security*, pages 117–122. ACM, 2006.