International Journal of Research Studies in Computer Science and Engineering (IJRSCSE)
Volume 2, Issue 1, January 2015, PP 8-12
ISSN 2349-4840 (Print) & ISSN 2349-4859 (Online)
www.arcjournals.org

Policies Based Privacy Control Mechanisms for Social Networking Systems

Srikar Swamy[1], G. Suday Kiran[2]

[1]PG Scholar, CSE, BITS, Adoni AP, India
[2]Asso Professor, CSE, BITS, Adoni AP, India

Abstract: *We introduce two approaches for improving privacy policy management in online social networks. First, we introduce a mechanism using proven clustering techniques that assists users in grouping their friends for group based policy management approaches. Second, we introduce a policy management approach that leverages a user's memory and opinion of their friends to set policies for other similar friends. We refer to this new approach as Same-As Policy Management. To demonstrate the effectiveness of our policy management improvements, we implemented a prototype Face book application and conducted an extensive user study. Leveraging proven clustering techniques, we demonstrated a 23% reduction in friend grouping time. In addition, we demonstrated considerable reductions in policy authoring time using Same- As Policy Management over traditional group based policy management approaches. Finally, we presented user perceptions of both improvements, which are very encouraging.*

1. INTRODUCTION

The recent growth of social network sites such as Face book, Twitter and MySpace has created many interesting and challenging security and privacy problems. In social networks, users manage their profile, interact with other users, and self organize into different communities. Users profiles usually include information such as the user's name, birthdates, address, contact information, emails, education, interests, photos, music, videos, blogs and many other attributes. Controlling access to the information posted on user profile is a challenging task as it requires average Internet users to act as system administrators to specify and configure access control policies for their profiles. To control interactions between users, the user's world is divided into a trusted and a non-trusted set of users, typically referred to as friends and strangers respectively. Furthermore, some social networks allow users to further partition the set of friends by geographical location, social group, organization, or by how well they know them. Users are provided with group based access control mechanisms that apply rules on the different groups of friends and strangers.

Face book, one of the most popular social sites, enables users to create friend lists and to compose profile policies based on these friend lists In addition to the challenges involved with enabling fine grain access control for user profiles to control which data attributes viewable by other users, a yet unexplored problem is related to users' profile access from entities different from other social network users. With the development of Web 2.0 technologies online social networks are able to provide open platforms to enable the seamless sharing of profile data to enable public developers to interface and extend the social network services as applications (or APIs). For example, Face book allows anyone to create software plug-ins that can be added to user profiles to provide services based on profile data. Although these open platforms enable such advanced features, they also pose serious privacy risks Users' profiles in fact have a great commercial value to marketing companies, competing networking sites, and identity thieves.

Social networks platforms have focused on user-to-user fine grain access control, for example, the Face book Privacy Policy allows users to specify fine grain policies controlling which profile attributes can be accessed by their friends and friends of friends. When installing social network applications users have to grant the applications all the requested permissions in order to successfully complete the installation process. For example, the application permission request displayed by the Googleþ and Face book platforms respectively when the user attempts to install an application. Basically, the adopted application access control model is an all-or-nothing policy, where the application should be granted all the requested permissions in order to install it

successfully. In addition, API developers have access to users' data regardless of the actual applications' needs, leading to potentially serious privacy breaches. Such privacy threat is often hidden or not clear to social network users, who are often not aware of the amount of data that is actually being disclosed, since they do not really distinguish between social network users and developers outside the social network boundaries.

In November 2011, Face book's privacy practices were the subject of complaints filed with the complaints were related to the Face book's privacy practices that deceived customers and failed to keep privacy promises. One of the main complaints was related to face book's claim that third-party applications that users' installed would have access only to user information that they needed to operate, where in fact, the apps could access nearly all of users' personal data. In addition, Face book claimed that it certified the security of apps participating in its "Verified Apps" program, where in fact they did not. We believe, in order to promote healthy development of social network environments and to protect individuals' privacy rights, users should be able to take advantage of the available applications while still having a stronger control on their data. The problem is not trivial, in that it requires designing new access control models for APIs in social networks, as well as extending social network applications.

Applications should be designed and customized with the users' profile preferences, and users should have the ability to specify the data that they are willing to reveal. Additionally, users should be able to use data privacy mechanisms such as generalization to enjoy the services provided through APIs without having to disclose identifying or private information. In this paper we address this issue by deploying an access control mechanism for applications in social networks. Our goal is to provide a privacy-enabled solution that is in line with social network ethics of openness, and does not hinder users' opportunities of adding useful and entertaining applications to their profiles. Our access control mechanism is based on enabling the user to specify the data attributes to be shared with the application and at the same time be able to specify the degree of specificity of the shared attributes. Enabling such a mechanism requires applications to be developed to accommodate different user preferences. We model applications as finite state machines, and use the required user profile attributes as conditions governing the application execution.

The user is faced with the challenge of specifying the minimum set of attributes and their minimum generalization levels required to acquire specific services provided by the application. In order to address this problem we proposed the weighted application transition system and formulated the Minimal Attribute Generalization Problem. Furthermore, we propose a solution that maps the problem to the shortest path problem to find the minimum set of attribute generalization required to access the application services. We assess our solution by implementing a proof-of-concept prototype using the Drupal platform, which is an open source platform for the development of online communities and social networks.

Additionally, we conduct extensive user studies using the Face book social network. We simulate our selective installation process for different applications currently provided by Face book and assess the users' perceived benefits and ease of use. The response is encouraging and positive, in that respondents acknowledge the need for solutions of this kind to better protect their privacy and security. They also believed that our approach is appropriate to gain control of the data disclosed at the application's end.

2. BACKGROUND

Current social networking platforms offer a simple policy management approach. Security aware users are able to specify policies for their pro_le objects. For example, my work colleague is restricted from seeing my photos. But my trusted best friend from school may access all my information. Face book provides an optional mechanism that allows users to create custom lists to organize friends and set privacy restrictions. Similarly, Google+ allows users to create Circles of friends, such as family, acquaintances, etc., where the user can apply policies based on these Circles. Face book also recently announced smart lists which automatically group friends who live near by or attend the same school. However, managing access for hundreds of friends is still a very dificult and burdensome task [17]. In addition, security unaware users typically follow an open and permissive default policy.

As a result, the potential for unwanted information leakage is great [23]. We believe that current capabilities to manage access to user profile information on today's social networking platforms are inadequate.

One approach that has been taken to alleviate the burden of managing access permissions for large sets of friends is the implementation of a role based access control model (RBAC) [10, 25, 24]. Role based access control provides a level of abstraction with the introduction of a role between the subject and the object permission. A role is a container with a functional meaning, for example, a specific job within an enterprise. Permissions to objects are assigned to roles and subjects are assigned to roles. Role members are granted objective permissions associated with the role(s) in which they belong. See Figure 1. This level of abstraction alleviates the burden of managing large numbers of subject to objective permissions assignments. For the purposes of discussion, we will use the term group as to be synonymous with the term role, with the understanding that traditionally roles have subjects and objects permission assignments and groups traditionally only have subject assignments.

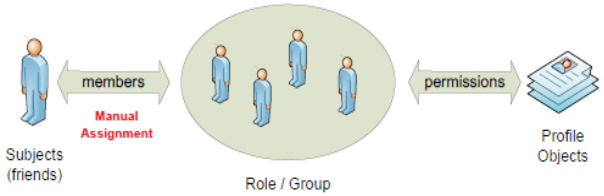


Figure 1: Role Based Access Control

Traditional RBAC can be leveraged within social networks. Often, people's relationships drive privacy decisions. People like to specify groups for their friend relationships, in which they then can set privacy policies [13, 22]. We refer to this approach as group based policy management. However, populating relationship groups can be very time consuming and burdensome to the user [14]. We introduce a group based policy management model that assists users in placing their subjects (or friends) into relationship groups. Our approach leverages proven clustering techniques to aid the user in grouping their friends more efficiently. In addition, we provide a mechanism to set friend-level exceptions within group policies. Our model is referred to as the Assisted Friend Grouping Model.

A shortcoming of the group based policy management approach is that the user's attention (mental model) is focused in multiple areas. For example, a user must _rst focus on the friend's relationship in order to group them appropriately. Next, the user must change focus to the group in order to set the group-level policy. Finally, the user must switch focus back to the friend in order to set any friend-level exceptions for each group policy. We introduce an approach that overcomes this weakness. Our model leverages users' memory and opinion of their friends to set policies for other similar friends. Studies have shown that users perform more efficiently using recognition based approaches that have minimal task interruptions [7, 12]. Using our visual policy editor, a user selects a representative friend (Same-As Example Friend), assigns appropriate object permissions to this friend and then associates other similar friends to the same policy. Our model is called Same-As Policy Management.

3. POLICY-BY-EXAMPLE

Our Policy-By-Example framework is made up of two access control models: Assisted Friend Grouping and Same- As Policy Management. We implemented both models as a prototype Face book application. The details of which are discussed in the following sections.

3.1 Assisted Friend Grouping

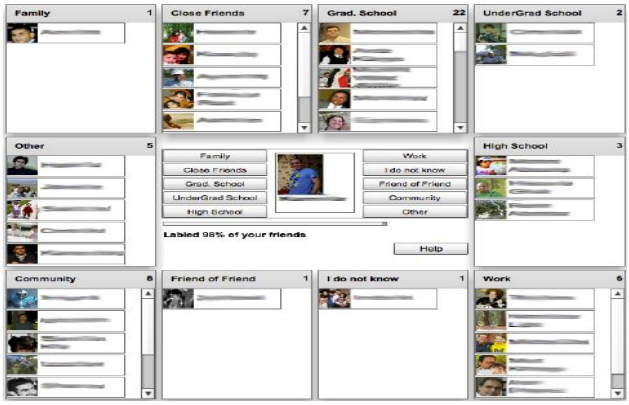
Group based policy management allows users to populate groups based on relationship and assign object permissionsto the groups, refer to Figure 1. Assisted Friend Grouping extends this model in two areas: 1) provides the user with assistance in grouping their friends, and 2) provides the user the ability to set friend-level exceptions within the group policyFor the purposes of our prototype Face book application, we predefined 10 relationship groups: Family, Close Friends, Graduate School, Under Graduate School, High School,Work, I do not know, Friends of Friend,

Community and Other. These groups where carefully selected, in part, from the work of Jones et al.[14]. They postulate that users group their friends, for controlling privacy, based on six criteria: Social Circles, Tie Strength, Temporal Episodes, Geographical Locations, Functional Roles and Organizational Boundaries.

Our friend relationship groups were selected to react these criteria.Within our prototype, each friend is presented to the user in the center of a friend grouping page, refer to Figure 3. The user is asked to select, for each friend, the group that best represents their relationship. They can either \drag" the friend to the appropriate relationship group on the page. Or, the user can click the representative relationship group name. To assist users in populating their relationship groups, we leverage the Clasuet Newman Moore (CNM) network clustering algorithm [5]. This clustering algorithm analyzes and detects community structure in networks by optimizing their modularity. Our prototype clusters the user's social network graph creating CNM clusters (or groups) of friends. During friend grouping, we present the friends to the user in CNM group order as recommendations.

For example, Bob has 50 friends and clustering his social network graph using CNM produces _ve clusters. We present to Bob, as recommendations for grouping, all the friends of one CNM group before presenting the friends of each subsequent CNM group. The premise is that CNM groups roughly align with user de_ned friend populated relationship groups. By presenting friends in the order they potentially will be grouped, the friend grouping time can be vastly reduced. The user's mental model is focused on roughly one relationship at a time, e.g., work colleagues. The user can quickly as certain that the stream of friends being presented are all work colleagues and can be placed in the Work group.

This approach reduces the number of \mental task switches" the user must perform between multiple relationship groups. After all the friends are grouped, the user sets the group policy by setting permissions that allow or deny access to the user's profile objects, e.g., email address, photos, etc. Finally, we provide the user the ability to set friend-level exceptions for each group policy. For example, a group policy may deny access to the user's email address except for group mem-



3.2 Same-As Policy Management

Social Network Systems pioneer a paradigm of access control that is distinct from traditional approaches to access control. The Gates coined the term Relationship-Based Access Control (ReBAC) to refer to this paradigm.

Relationship-Based Access Control is characterized by the explicit tracking of interpersonal relationships between users, and the expression of access control policies in terms of these relationships. This work explores what it takes to widen the applicability of Relationship-Based Access Control to application domains other than social computing. We prepare an archetypical Relationship-Based Access Control model to capture the essence of the standard, that is, authorization decisions are based on the relationship between the resource owner and the resource accessor in a social network maintained by the security system. A novelty of the model is that it captures the contextual nature of associations. We work out a policy language, based on modal logic, for composing access control policies that support delegation of trust. We use a case study in the domain of Electronic Health Records to demonstrate the utility of our model and its policy

language. This provides initial evidence to the feasibility and utility of Relationship-Based Access Control as a general-purpose paradigm of access control

3.3 Prototype Architecture

We propose a multiparty authorization framework (MAF) to model and realize multiparty access control in online social networks. We begin by examining how the lack of multiparty access control for data sharing in online social networks can undermine the security of user data. A multiparty authorization model is then formulated to capture the core features of multiparty authorization requirements which have not been accommodated so far by existing access control systems and models for online social networks. In Meanwhile, as conflicts are inevitable in multiparty authorization specification and enforcement, systematic conflict resolution mechanism is also addressed to cope with authorization and privacy conflicts in our framework. We first examine and characterize the behaviors of ICAs. Then we propose a detection framework that is focused on discovering suspicious identities and then validating them. Towards detecting suspicious identities, we propose two approaches based on attribute similarity and similarity of friend networks. The first approach addresses a simpler scenario where mutual friends in friend networks are considered; and the second one captures the scenario where similar friend identities are concerned. We also current experimental results to demonstrate flexibility and effectiveness of the proposed approaches. Finally, Some feasible solutions to validate suspicious identities

4. CONCLUSION

In this paper, we introduced two approaches to improving privacy policy management in online social networks. First, we presented an approach, leveraging proven clustering techniques, that assists users in grouping their friends for policy management purposes. Our approach demonstrated reduced grouping times and improvements in ease of use over traditional group based policy management approaches. Second, we introduced Same-As Policy Management, which leverages a user's memory and opinion of their friends to set policies for other similar friends. Our visual policy editor uses friend recognition and minimal task interruption to obtain substantial reductions in policy authoring times. In addition, Same-As Policy Management was positively perceived by users over traditional group based policy management approaches.

REFERENCES

[1] A. Acquisti and R. Gross. Imagined communities: Awareness, information sharing, and privacy on the Face book. In Privacy Enhancing Technologies, pages 36{58, 2006.

[2] A. Acquisti and J. Grossklags. Privacy and rationality in individual decision making. IEEE Security and Privacy, 3(1):26{33, 2005.

[3] A. Besmer, J. Watson, and H. R. Lipford. The impact of social navigation on privacy policy con_guration. In SOUPS, 2010.

[4] J. Bonneau and S. Preibusch. The privacy jungle: On the market for data protection in social networks. In The Eighth Workshop on the Economics of Information Security (WEIS 2009), 2009.

[5] A. Clauset, M. E. J. Newman, and C. Moore. Finding community structure in very large networks. Physical Review E, pages 1{ 6, 2004.

[6] E. Cutrell, M. Czerwinski, and E. Horvitz. Noti_cation, disruption, and memory: E_ects of messaging interruptions on memory and performance. pages 263{269. IOS Press, 2001.

[7] R. Dhamija and A. Perrig. Deja vu: A user study using images for authentication. In Proceedings of the 9th conference on USENIX Security Symposium -Volume 9, pages 4{4, Berkeley, CA, USA, 2000. USENIX Association.

[8] P. Dunphy, A. P. Heiner, and N. Asokan. A closer look at recognition-based graphical passwords on mobile devices. In Proceedings of the Sixth Symposium on Usable Privacy and Security, page 1. ACM, 2010.