Visualizing Privacy Implications of Access Control Policies in Social Network Systems

Mohd Anwar[1], Philip W.L. Fong[1], Xue-Dong Yang[2], and Howard Hamilton[2]

[1] Department of Computer Science, University of Calgary, Alberta, Canada
{manwar,pwlfong}@ucalgary.ca
[2] Department of Computer Science, University of Regina, Saskatchewan, Canada
{yang,hamilton}@cs.uregina.ca

Abstract. We hypothesize that, in a Facebook-style social network system, proper visualization of one's extended neighbourhood could help the user understand the privacy implications of her access control policies. However, an unrestricted view of one's extended neighbourhood may compromise the privacy of others. To address this dilemma, we propose a privacy-enhanced visualization tool, which approximates the extended neighbourhood of a user in such a way that policy assessment can still be conducted in a meaningful manner, while the privacy of other users is preserved.

1 Introduction

One of the main purposes of privacy preservation is impression management [1,2]. This is particularly true in the context of social network systems. 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 look at her profile from the lenses of Bob and Jill, to find out what 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. We use the term ***reflective policy assessment*** 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 changing, requiring a user to constantly perform policy assessment. As a result, reflective policy assessment is a nontrivial undertaking. Tool support is definitely desirable.

Unfortunately, a privacy dilemma is inherent in reflective policy assessment. To assess policies reflectively, a user must begin with identifying a potential accessor who is of interest to her. This, however, could lead to breaching the privacy of the potential accessor, as the latter may not want her identity to be disclosed to the user conducting the policy assessment. Suppose the running example is situated in Facebook. If Bob

J. Garcia-Alfaro et al. (Eds.): DPM 2009 and SETOP 2009, LNCS 5939, pp. 106–120, 2010.
© Springer-Verlag Berlin Heidelberg 2010

adopts a privacy setting that allows his identity to be revealed only to friends but not friends of friends, then Alice will not be able to conduct reflective policy assessment against Bob without breaching his privacy.

This privacy dilemma is not specific to just Facebook. Fong et al. proposed an access control model to delineate the design space of privacy preservation mechanisms in Facebook-style social network systems [3]. In this model, policies such as “only friends” and “friends of friends” are but examples of more general ***topology-based 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. With these policies, it would even be more important to have access to one’s extended neighbourhood in addition to her immediate friends for the purpose of policy assessment.

This dilemma is rooted in the asymmetric nature of trust. In the process of reflective policy assessment, a resource owner (e.g., Alice) conceptualizes the level of trust she is willing to invest in a potential accessor (e.g., Bob). Yet, this endeavor is possible only if the identity of the potential accessor is known to the resource owner, the feasibility of which may not always be possible because the potential accessor may not trust the resource owner.

This paper is about the design of a privacy enhanced visualization tool for Facebook-style social network systems (FSNSs) to facilitate reflective policy assessment while preserving the privacy of potential accessors. The visualization tool helps a user assess 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 a potential accessor at her extended neighbourhood. Our contributions are the following:

1. We introduce the notion of reflective policy assessment, which helps a user assess the privacy implications of her policies by positioning herself as a potential accessor. We also discover and address an inherent privacy dilemma of reflective policy assessment.
2. We translate the concept of reflective policy assessment into a concrete visualization tool for policy assessment. Since this tool would 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).
3. At the core of our visualization technique is a visual representation of a user’s extended neighbourhood. We establish graph-theoretic properties common to the social graphs of FSNSs. Based on these properties, we devise an algorithm to generate a surrogate of a user’s extended neighbourhood. This surrogate can be examined for reflective policy assessment without violating the privacy of other users.

The organization of this paper is as follows. Sect. 2 describes an access control model for FSNSs. In Sect. 3, we present the main idea of assessing policies through visualization. In Sect. 4, we present an algorithm for generating a surrogate of a user’s extended neighbourhood for policy assessment. Sect. 5 discusses subtle issues in our visualization approach. Sect. 6 presents some open questions on how to evaluate the proposed visualization technique. Sect. 7 surveys related literature, and Sect. 8 describes conclusion and future work.