DISSERTATION: ACCESS CONTROL FOR ONLINE SOCIAL NETWORKS USING RELATIONSHIP TYPE PATTERNS

Nahim Adnan
Graduate Student
Department of Computer Science
University of Texas at San Antonio
nahimadnan@gmail.com

I. Introduction

Online social networks (OSNs) have emerged and thrived rapidly over the past several years and now have billions of users worldwide. Many existing OSNs facilitate convenient environments and various kinds of services for participating users to regularly make new connections, interact and share information with each other for a variety of purposes. The sharing and communications are based on social connections among users, namely relationships.

Since most users join OSNs to keep in touch with people they already know, they often share a large amount of sensitive or private information about themselves, including demographic information, contact information, education information, blog posts, pictures, videos, comments, and so on. Given the rising popularity of OSNs and the explosive growth of information shared on them, OSN users are exposed to potential threats to security and privacy of their data. So effective access control is needed that can protect data from unauthorized access in OSNs.

Access control in OSNs presents several unique characteristics different from traditional access control. In mandatory and role-based access control, a system-wide access control policy is typically specified by the security administrator. In discretionary access control, the resource owner is responsible for defining access control policy. However, in OSN systems, users expect to regulate access to their resources and activities related to themselves. Thus access in OSNs is subject to user-specified policies. Other than the resource owner, some related users may also expect some control on how the resource or user can be exposed. To prevent users from accessing unwanted or inappropriate content, user-specified policies that regulate how a user accesses information need to be considered in authorization as well.

Now-a-days, access control in OSNs is typically based on the relationships among users on the social graph. This type of relationship-based access control (ReBAC) has emerged as the most prevalent access control mechanism for OSNs. With ReBAC, resource owners can specify access control of their information based on their relationships with others, without knowing the user name space of the entire network or all their possible direct or indirect contacts.

One common characteristic found in most of these commercial and academic solutions is that they mainly focus on user-to-user (U2U) relationships between the accessing user and the resource owner, and at least implicitly assume ownership is the only manifestation of user-to-resource (U2R) relationships. However, this is not sufficient to capture many user activities found in todays OSN applications, where users can perform actions that create relationships between users and resources other than ownership. To enable a fully expressive relationship-based access control, it is necessary to exploit U2R and R2R relationships in addition to U2U relationships for authorization policies and decisions.

II. Research Problem

OSNs offer users various types of user interaction services, including chatting, private messaging, poking and social games. As OSN systems mature, various types of resources need to be protected, such as user sessions, relationships among user and resources, access control policies and events of users. Most of the existing OSN systems enforce a coarse-grained and limited relationship-based access control, mainly based on U2U relationships between the accessing user and the target user. Current OSNs rely on an implicit ownership relationship, between the resource and its owner, hence the authorization of such U2R access is still based on the underlying U2U relationships. There are many scenarios where related users other than the owner want to exert their control capability on the resource they share certain types of U2R relationships with. There is a huge gap between users mental model and the control offered by the systems.

As a consequence of allowing U2R relationships, users are able to specify policies for others. Furthermore, since multiple users can express access control policies for a user or a resource, it is expected that there will be several policies applicable to the same access request which will inevitably raise conflicts. This is also very critical that how the authorization policies are to be interpreted and how policy conflicts are resolved.

III. Literature Review

Literature review section of this dissertation first cited some basic OSN systems. There are some attack mechanisms on shared private data such as spam, phishing attacks, sybil attacks and malware attacks. Running third party applications in the OSN poses threat to the confidentiality of user data. There also exists some difficulties faced by the users due to the complexity of the privacy control settings. All of the mentioned problems are to provide an idea for the essence of access control mechanisms.

Author of the dissertation initially discusses some of the basic characteristics of access control systems for OSN. The relationship among users provides the basis for authorization is also included. The proposed models for relationship based access control are cited and briefly explained. Different models based on U2U relationship, level of relationships, multiple relation types, U2R relationship have been mentioned. The author presents the overall scenario of essence of the access control, different aspects of access control along with the prior research works comprehensively. Finally, the literature review section is ended with short discussion about some privacy preservation solutions on OSN.

IV. Experimental results

Two algorithms DFS and BFS have been proposed for determining if there exists a qualified path between two involved users in an access request. Two set of experiments are conducted.

In the first set experiments, there are 1000 users in the system and each user has the same number of neighbours. Effect of the number of hopcount is observed here. When hopcount increments, the average execution time required for both algorithms increases as well, but the trends tend to flatten after the hopcount reaches 4. It indicates that a qualified path can be always found between two users within 4 hops in this setting. It has been also observed that the BFS algorithm works slightly better than the DFS algorithm for large hopcount limit in sparse graphs, as DFS takes many lengthy probes before finding a qualified path while BFS does not suffer from much overhead in sparse graphs.

In the second set of experiments, the number of neighbours for each user is set in the quantities 100, 200, 500 and 1000. The effect of node degree along with variation in hopcount is observed here. As the hopcount is incremented, the time for both algorithms to find a qualified path is increased, since the search space expands accordingly. It has been found that DFS algorithm outperforms its BFS counterpart when dealing with 3 hop policies or larger. Finally, the results indicate that both node degree and hopcount limit significantly affect the performance of the two algorithms.

V. Future Works

Author presents some future research directions. ReBAC can be extended to capture some unconventional relationship such as temporal relationship, one-to-many relationship. The attribute-aware ReBAC model also needs to be adjusted accordingly to express the attributes of such new relationships. Access control problem arising due to the third party in OSN can be addressed in the future. Another potential area of research is to design user-specified conflict resolution policy.