Chapter 16
A Survey on Access Control Techniques for Social Networks

Yousra Asim
COMSATS Institute of Information Technology, Pakistan

Ahmad Kamran Malik
COMSATS Institute of Information Technology, Pakistan

ABSTRACT

Online Social Networks (OSN) are getting popular day by day. Users share their information in OSN with others users. Access control is required to prevent unauthorized access to this information. Several studies have been conducted for access control in social networks. This chapter is a survey of available access control models/techniques based on social networks. Available access control models can be categorized as relationship-based, attributes-based, community structure-based and user activity centric model. A number of techniques have been proposed by several authors for access control in social networks. Most of the approaches use Social Network Analysis (SNA) techniques, others use user related information, for example, attributes or activities, the rest use a combination of approaches.

INTRODUCTION

"Man is a social animal" is a well-known quote by a renowned Greek philosopher, Aristotle (n.d.). Historically, human beings invented many ways to communicate with each other. The communication journey started from letter writing and kept on moving through telegraph, radio, TV, Computer, Internet, messenger up to the social network. Users of every age keep themselves connected with their friends and relatives via social networks e.g. Facebook, Twitter etc. Online Social Network (OSN) provides value and immediacy to its users. Users of this platform like to share their interests, activities, personal information and enjoy to increase their friendship circles but they also don't like to let their private information distorted. Proper and efficient access control strategies can fulfill their dreams in this regard.

DOI: 10.4018/978-1-7998-0417-8.ch016

Access control process basically involves authentication and authorization. It may also include identification and access approval. Authentication addresses the question: Who are you? It can uniquely identify a user. Authorization addresses the question: What can you do? It is the process which manages the resources that authenticated client is permitted to do. Normally access control is used to perform the following functions: granting access right, limiting access rights, preventing access rights and revoking access rights. Access control administration can be centralized or decentralized. In centralized approach of administration, central authority is responsible for granting or denying access to user. It is more restricted approach in which all decisions are depending upon a central authority. If central authority fails due to some technical problem, no access to resources will be granted by anybody. Moreover, if a single authority fails to satisfy all the requests then it will disappoint users. In decentralized approach of administration, users are responsible for their resource policies, this approach has no single point of failure but user's privacy is at risk. It is very difficult to maintain security of resources at each node of the social network.

Access control models and techniques prior to social network are described in this paragraph. These models and techniques are not the subject of this chapter yet they are the basis of most access control implementations and also used in combination with social network techniques. Access policies are defined to map different access rights. Historically, researchers used different access control structures like access control matrix (Graham & Denning, 1972), access control lists (Sandhu & Samarati, 1994) and many other access control models to implement access policies. The use of these techniques depends upon the scenario and feasibility of proposed approach. Access control can be categorized into different types from the administration point of view. For example, MAC and DAC (US Department of Defense standard, 1985). Mandatory Access Control (MAC) is the strategy in which rules are strictly controlled and enforced by system administrator. Access to resource is granted according to that rules. Discretionary Access Control (DAC) is the strategy in which access is granted to resources depending upon the policy specified by its owner. The NIST standard Role-based Access Control (RBAC) model (Ferraiolo, Sandhu, Gavrila, Kuhn & Chandramouli, 2001) is the strategy in which access is granted to resources depending upon the roles of users. Rule-based access control, for example (Carminati, Ferrari & Perego, 2006) is the strategy in which access is granted to resources depending upon rules specified for access. Attribute-based Access Control (ABAC) model, for example (Hu, Kuhn & Ferraiolo, 2015) is the strategy in which access is granted depending upon different properties of subject, object and other related data.

Recent access control techniques, mainly for social networks, are based on community structure and relationship patterns. They apply different techniques, for example, Social Network Analysis (SNA) techniques to find out social network structure like clique, k-core etc. In this case, access can be granted by applying rules to a cluster found after the application of above described techniques. Social network requires proper access control techniques to manage the resources of it users. Researchers have proposed different access control techniques/models for online social networks, different architectures for these models, access rules and policy specification languages. This study is all about them. Social network based access control techniques available in literature can be classified into the following categories according to their characteristics; Relationship-based access control model, Attribute-based access control models, Community centric and User activity centric techniques.

The remainder of this chapter is organized as follows. Relationship-based access control models/techniques for OSN is further organized into sub sections according to access control models for OSN. Attribute-based, Community centric and User activity centric access control models/techniques are described in the following sections. Discussion of the access control techniques for OSN is described before the conclusion section.