Chapter 15
Trust-Based Usage Control in Collaborative Environment

Li Yang
University of Tennessee at Chattanooga, USA

Chang Phuong
University of Tennessee at Chattanooga, USA

Andy Novobilski
University of Tennessee at Chattanooga, USA

Raimund K. Ege
North Illinois University, USA

ABSTRACT

Most access control models have formal access control rules to govern the authorization of a request from a principal. In pervasive and collaborative environments, the behaviors of a principal are uncertain due to partial information. Moreover, the attributes of a principal, requested objects, and contexts of a request are mutable during the collaboration. A variety of such uncertainty and mutability pose challenges when resources sharing must happen in the collaborative environment. In order to address the above challenges, we propose a framework to integrate trust management into a usage control model in order to support decision making in an ever-changing collaborative environment. First, a trust value of a principal is evaluated based on both observed behaviors and peer recommendations. Second, the usage-based access control rules are checked to make decisions on resource exchanges. Our framework handles uncertainty and mutability by dynamically disenrolling untrusted principals and revoking granted on-going access if access control rules are no longer met. We have applied our trust-based usage control framework to an application of file sharing.

INTRODUCTION

Conventionally registered parties behind firewalls collaborate in well controlled environments. With new virtual communities emerging, parties communicate directly with one another to exchange information or execute transaction in a peer-to-peer (P2P) fashion. The dynamism of the P2P communities means that the principal that offers services will meet requests from unrelated or unknown principals. Peers need to collaborate and obtain services within environments that are unfamiliar or even hostile. Therefore, peers have to manage the risks involved in the collaboration when prior experience and knowledge about each other are incomplete. One way to address this uncertainty is to develop and establish trust among peers. Trust can be built by either a trusted third party (Atif, 2002) or by community-based feedback from past experiences (Resnick, Kuwabara, Zeckhauser, & Friedman, 2000) in a self-regulating system. Trust leads naturally to a decentralized approach to security management that can tolerate partial information.

In such a complex and collaborative world, a peer can protect and benefit itself only if it can respond to new peers and enforce access control by assigning proper privileges to new peers. Access control models (Bertino, 2001a; Jajodia, Samarati, Sapino, & Subrahmanian, 2001) determine authorization based on principals' permission on target objects. Usage of a digital object is temporal and transient in a virtual community, such as online reading, which is beyond an instantaneous access. The usage control (UCON) model (Park & Sandhu, 2004) is proposed to handle continuity of access decisions and mutability of subject and object attributes. Authorization decisions are made before an access and repeatedly checked during the access. The on-going access may be revoked if the security policies are not satisfied due to changes of the subject, object, or system attributes.

The general goal of our work is therefore to investigate the design of a novel approach to addressing both uncertain information and mutable attributes. If successful, this approach will offer significant benefits in emerging applications such as P2P. It will also benefit collaboration over the existing Internet when the identities and intentions of parties are uncertain. We integrate trust evaluation with usage control to handle uncertainty of entities and mutability of attributes. Underlying our framework is a formal computational model of trust and access control that will provide a formal basis to interface authentication with authorization.

Related Works

Most recent research on access control includes task-based authorization controls (Thomas & Sandhu, 1998), team-based access control (Georgiadis, Mavridis, Pangalos, & Thomas, 2001), role-based access control (Gerraiolo, 2001), temporal role-based access control (Bertino, 2001b), and X-GTRBAC (Bhatti, Ghafoor, Bertino, & Joshi, 2005). Recently, UCON (Park & Sandhu, 2004) handles the attribute mutability of a principal or an object when the system makes decision for a request. All of them assume that a principal or an object is defined and represented by its attributes. This means that the identity, role, or group of the subject can be identified through certain authentication mechanisms and that information about behaviors of a principal is certain. However, in a pervasive and collaborative environment, identity may not be identified. Moreover, identity itself can not convey priori information about the likely behavior of a principal. Behaviors of a principal may change between friendly and malicious when privileges are executed. A principal can not make access control decision only based on identity information because identity itself can not ensure friendly behaviors.

Life Cycle Pattern Study of Malicious Codes
June Wei, Randall C. Reidand Hongmei Zhang (2008). *International Journal of Information Security and Privacy (pp. 26-41).*
www.irma-international.org/article/life-cycle-pattern-study-malicious/2474