Authorization Based on Evidence and Trust*

Bharat Bhargava and Yuhui Zhong

Center for Education and Research in Information Assurance and Security (CERIAS), and Department of Computer Sciences
Purdue University, West Lafayette, IN 47906-1398, USA {bb, zhong}@cs.purdue.edu

Abstract. Developing authorization mechanisms for secure information access by a large community of users in an open environment is challenging. Current research efforts grant privilege to a user based on her objective properties that are demonstrated by digital credentials (evidences). However, holding credentials is not sufficient to certify that a user is trustworthy. Therefore, we propose using the notion of trust to characterize the probability that a user will not harm an information system. We present a trust-enhanced role-mapping server, which cooperates with RBAC (Role-Based Access Control) mechanisms to together implement authorization based on evidence and trust. A prerequisite for this is our proposed formalization of trust and evidence.

1 Introduction

Research is needed to develop authorization mechanisms for a large and open community of users. In such an environment, prior knowledge about a new user normally does not exist [20]. For authorization, the permission set for each user must be determined. Current research efforts grant privilege to a user based on her objective properties that are demonstrated by digital credentials (evidences) issued by third parties [4],[9]. Credentials are not sufficient to certify that a user is trustworthy. Therefore, a formalized notion of trust is used by us to characterize the probability that a user or an issuer of credentials will not carry out harmful actions [6]. Next, the impact of users' behavior on system's trust towards them needs to be quantified. Furthermore, the reliability of evidence or credentials from different issuers might be different. Authorization based on evidence as well as trust makes access control adaptable to users' or issuers' behavior. The research requires: (1) an appropriate representations of the evidence and trust, so that their manipulation can be automated, (2) a suitable authorization architecture that can incorporate the evidence and trust, and (3) integration of this scheme with existing access control mechanisms. We investigate these issues and propose a trust-enhanced role-mapping (TERM) server architecture, which can cooperate with RBAC (Role-Based Access Control) mechanisms for authorization based on evidence and trust.

* This research is supported by CERIAS and NSF grants CCR-9901712 and CCR-0001788.

Y. Kambayashi, W. Winiwarter, M. Arikawa (Eds.): DaWaK 2002, LNCS 2454, pp. 94–103, 2002.

This paper is organized as follows. Section 2 introduces related research. Section 3 presents the fundamental concepts in our system, and their formal definitions. The architecture of a TERM server is described in section 4. The algorithms and implementation are in section 5. We focus on the role-assignment policy language and the algorithms that evaluate the reliability of evidence and role-assignment policies. Conclusions are in section 6.

2 Related Work

Authorization in an open environment: This is an active area of research. One direction is *trust management* [4],[5]. A trust management system provides a language allowing system administrators to define authorization policies based on credentials, and an engine to enforce the authorization polices. These systems design their own access control mechanisms instead of taking advantage of the existing ones such as RBAC [9].

Another direction of research divides the authorization problem into two subproblems: (1) determine the permission set of a user (2) enforce access control by using existing mechanisms like RBAC. These approaches have the advantage of easy integration with existing systems. Our research effort is in this direction. Others determine users' permission set only according to evidence/credentials. Our work is distinguished by using evidence and trust.

Trust Models: Several researchers have proposed algorithms to summarize trust opinions from third parties. The summarization includes evaluating an opinion from an issuer, or combining opinions from different issuers [1],[11],[14]. Little research has been done to quantify trust based on direct experience. Because personal experience plays an important role when forming trust opinion in real life, we consider this first-hand information in our framework.

RBAC: RBAC has emerged as a promising technology for efficiently managing and enforcing security in large organizations [2],[17]. A role is an entity with some semantics regarding the authority and responsibility. The authorization process is divided into two parts: role-permission mapping and user-role mapping. Role-permission mapping associates roles with permission sets. User-role mapping assigns roles to users.

3 Concepts and Formal Definitions

The following concepts, definitions and representations are used in our research.

3.1 Concepts

Evidence: Evidences (also called credentials) are statements about certain properties of an entity (called subject). An evidence can come from internal or external sources. Evidence can be information stored in a local database (e.g, user name and password) or public key certificate (e.g, X.509 V3) [8],[10], digitally signed document (e.g, PICS rating) [18], etc.