A General Design towards Secure Ad-hoc Collaboration

Masayuki Nakae
NEC Corporation
Kawasaki, Kanagawa, Japan
m-nakae@bp.jp.nec.com

Xinwen Zhang
George Mason University
Fairfax, Virginia, USA
xzhang6@gmu.edu

Ravi Sandhu
George Mason University
and TriCipher Inc., USA
sandhu@gmu.edu

ABSTRACT

We propose a general design for secure collaboration systems, which is underpinned with an access control policy model, an administrative scheme, and an enforcement scheme, based on the Typed Usage Control (TUCON) model. TUCON is a generalized form of the usage control model (UCON) proposed recently. By utilizing mutable object attributes, UCON can reflect the dynamic nature of ad-hoc collaborations such as temporal and/or spatial usages. In TUCON, every object has an object type as a persistent attribute, which works as a name space that indicates an organization to which the object belongs. With object types, TUCON policies can distinctly control intra-organization and inter-organization information flows. This approach achieves the autonomy of collaborative teams as well as the mutual confidentiality of collaborating organizations.

Categories and Subject Descriptors

D.4.6 [**Operating Systems**]: Security and Protection—*Access controls*; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection—*Unauthorized access*

General Terms

Security

Keywords

Access Control, Information flow, Usage Control, Collaboration.

In order to increase the productivity and efficiency of intellectual activities such as scientific or engineering research, the importance of collaborative work among concerned organizations is well understood. To date, distributed computing technologies such as virtual private networking, peer-to-peer file sharing, Web services, and Grid, are expected to encourage inter-organizational collaboration in academic and commercial sectors.

For secure collaboration, a primary concern is how to balance the competing goals of *autonomy* and *confidentiality* with respect to intra- and inter-organization information flows. Several approaches have been proposed in literatures. However, it is still a research issue to capture the dynamic nature of ad-hoc collaborations such as temporal and/or spatial usages.

We propose a general design for secure ad-hoc collaborations, which allows the dynamic changes of object attributes such as user locations as well as the autonomy and confidentiality of collaborative work, in a model-based approach as follows.

First, we show an access control policy scheme for inter-organizational collaboration, based on the *Typed Usage Control* (TUCON). TUCON is a generalized form of the usage control model (UCON), which can capture the dynamic features of collaborative work with attributes that represent transient states of an object such as task progress. TUCON introduces an *object type* as a persistent attribute that is assigned to an object in its creation time. A typed pair of a subject and an object distinguishes internal activities in a single organization from external activities spanning different organizations. With a unique type assigned to a collaborative team (i.e., a virtual organization), our TUCON-based policy scheme allows fine-grained information flow control beyond organizational boundaries, and the autonomy of individual collaborative teams.

Second, we propose a *joint administrative model* (JAS), which enables collaborating organizations to administrate their TUCON policies as an agreement with confidentiality requirements (e.g., a non-disclosure agreement). Since a TUCON policy involves exactly two organizations, it can prevent a collaborating organization from leaking sensitive data without the opponent's agreement. Furthermore, by allowing collaborating organizations to update their agreement, our scheme can flexibly support diverse relationships of collaborating organizations.

For TUCON policy enforcement, we develop an enforcement scheme with *attribute monitors* in a distributed environment. In order to solve the problem that a platform in a distributed system may host several entities of different organizations as a result of user activities in collaborative work, we deploy attribute monitors on distributed platforms, which recognize user activities over remote platforms from process execution sequences, and appropriately update object attributes. Working with the attribute monitors, the policy enforcement point (PEP) on a platform can correctly enforce a TUCON policy throughout a distributed system.

Finally, we present a distributed architecture for secure collaboration, which consists of policy administration point (PAP), user platforms, and attribute repositories. PAP allows the representatives (or administrators) of collaborating organizations to make an agreement on a TUCON policy based on the JAS. User platforms perform collaborative services under the attribute-based enforcement scheme with attribute monitors. An attribute repository securely forwards object attributes over collaborating organizations. We have implemented a prototype system based on this architecture and have been studying the effectiveness of our proposed scheme and the performance with some example applications. We are further optimizing the implementation, and applying it to practical information sharing solutions.

ASIACCS'06, March 21–24, 2006, Taipei, Taiwan.