

Information System Security Operation Security Policy Automation, Modeling, and Bridging

Improved Access Control in Coalition Environments

Overview

Businesses, governments, and other organizations are finding that coalition operations are increasingly necessary to their success. The Security Policy Automation, Modeling, and Bridging (AMBer) project focused on developing conceptual techniques to improve access control in coalition environments. We continue to build on this important work by creating a proof-of-concept implementation of one of the access control models developed under AMBer.

Objective

Because organizations rely on their information systems to support their operations, the ability to securely share information system resources has become critical to the tightly integrated systems and processes of business, military, and other coalitions. Secure sharing requires that organizations be able to exercise fine-grained, policy-governed control over access to shared resources. Unfortunately, current technologies do not comprehensively support such control for coalition resource sharing.

We addressed the following two problems: the lack of coalition-focused access control models; and the lack of a conceptual foundation for describing differences in authorization semantics among partner organizations. These deficiencies contribute to the complexity of designing, developing, and administering information systems within a coalition environment.

Approach

To improve access control for coalitions, We introduced the first collection of coalition-focused

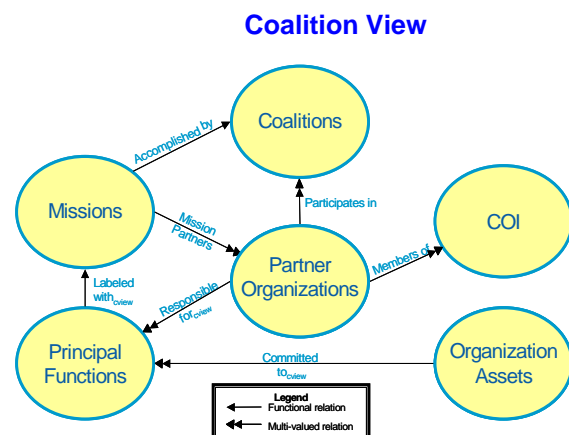
access control models and developed a conceptual framework for specifying the semantic interoperation of diverse authorization systems.

Modeling

The models developed under the AMBer project capture the entities involved in coalition resource sharing, identify the interrelationships among those entities, and define requirements for building authorizations in coalition environments. Such models are a necessary foundation for the development of coalition-focused access policies and enforcement mechanisms.

Our family of coalition-based access control (CBAC) models provides a broad spectrum of functionality, expressiveness, and flexibility in support of coalition access control policies. The basic CBAC model layers coalition access control concepts on top of a simple role-based access control (RBAC) model.

The other CBAC models incorporate elements of team-based (TMAC) and task-based (TBAC) access control. These models support the use of system context information in



This work sponsored by DARPA through SPAWAR, Contract Number N66001-00-C-8070, with McAfee Research, which is now the Security Research Division of SPARTA

decisions to activate, synchronize, and deactivate permissions. The CBAC family provides a suite of models that range in expressivity, as well as implementation complexity. The CBAC models are defined in views that reflect the different perspectives of various coalition stakeholders on coalition activities and resources.

As an example, the figure on the previous page shows the coalition-level view. In this view, coalition entities are defined at the executive level where international diplomacy or top-level corporate agreements and their associated abstractions are specified.

Semantic Bridging

To enable controlled resource sharing within a coalition, an organization must be able to correctly interpret authorizations and restrictions issued by other member organizations (e.g., one organization's "company sensitive" designation may have approximately the same meaning as another organization's "proprietary" designation). The AMBer project's semantic bridging framework allows organizations to formally define relationships between their access control models, instances of those models, and the specific authorizations in use.

The framework includes a conceptual authorization system for each member organization, as well as a commitment authorization system that formalizes the coalition agreement. The commitment authorization system serves as the "common

language" developed by the partner organizations—each organization must map common coalition authorizations into terms understandable within the local authorization system. The framework supports a scalable approach to semantic bridging, avoiding pairwise mappings between coalition participants, and allowing organizations to map only the coalition-relevant portions of their authorization systems.

By supporting a formal expression of the relationships among authorization systems within a coalition, the semantic framework helps administrators reduce the likelihood of semantic misunderstandings and enables more accurate policy specification and implementation.

Future Work

SPARTA is building on its AMBer project results by developing a prototype implementation of one of the CBAC models. Under the SPiCE project, we are designing a CBAC-based access policy expression language and building a system to automatically compile policy enforcer configurations. We expect that this system will simplify the process of implementing high-level access control policies and reduce the likelihood of erroneous or inconsistent configurations for access policy enforcement mechanisms.

