



Information System Security Operation

Attribute-Based Access Control

Improved Decentralized Security for Coalition Environments

Problem

Today coalitions wishing to share resources often find themselves with no better alternative than to establish a virtual private network (VPN) and to make shared resources available to one another through the VPN. This means that users with access to any of the shared resources have access to all of them, which is inappropriately course-grained access control. Alternative solutions that provide appropriate granularity are based on the identity, local role, or capabilities of the resource requestor. As such, they require foreign requestors to be known to the resource-providing organization before access can be authorized, which means these systems do not scale.

Solution

The goal of the Attribute-Based Access Control (ABAC) project was to overcome these granularity and scalability problems and in so doing develop access control systems that are suitable for dynamic coalitions. Authority in coalitions is inherently distributed. ABAC provides a means for each locus of authority to determine and specify its own judgments, and for those judgments to be combined naturally to make appropriate authorization decisions. Thus, while control is decentralized, resource owners retain fine-grained control of their own resources. For scalability, they have the option to delegate authority over judgments to those better qualified. For instance, staffing decisions in foreign organizations require no local administration within the resource organization.

Approach

The approach bases authorization decisions on chains of digitally signed attribute credentials. Credential issuers assert their judgments about

the attributes of entities through the credentials. The entities include both users and organizations. Because these credentials are digitally signed, they can serve to introduce strangers to one another off-line. A key to ABAC's scalability is that the issuers of credentials can be strangers whose authority is determined based on their own attributes, as documented in further credentials.

A key issue ABAC must address is the choice of an appropriate language design. The language is at the core of an ABAC system, and, determines the kinds of judgments that can be issued in credentials. Furthermore, its semantics determines how the judgments contained in credentials issued by distributed authorities combine to decide authorization questions.

Another key issue is the data contained in credentials is often sensitive and must be protected. This is central, as it means the credentials that must be presented to obtain access are themselves subject to access control. Because the project is interested in supporting coalitions of organizations that have only limited mutual trust, we believe the requestor and the access mediator will typically be unable to agree upon a trusted third-party that might assist them in using their sensitive credentials to establish mutual trust. Instead, our approach calls for requestor and access mediator to enter into a kind of bilateral credential exchange, which we refer to as a trust negotiation. The negotiation consists of a sequence of credential exchanges that begin by disclosing non-sensitive credentials. As credentials flow, more are unlocked, enabling them also to flow. In successful negotiations, credentials eventually flow that satisfy the policy of the desired resource. Ongoing strategy design work seeks to identify and avoid the potential pitfalls associated with protecting credential content during this process.

This work sponsored by DARPA ATO through SPAWAR, Contract Number N66001-01-C-8005, with McAfee Research, which is now the Security Research Division of SPARTA.

<http://www.isso.sparta.com/research>



Attribute-Based Access Control

Improved Decentralized Security for Coalition Environment

Accomplishments

The ABAC project was a follow-on to a small start-up project, Advances in Trust Negotiation. Because the ABAC project continues the technical goals of the former, we report together the accomplishments of both. Accomplishments were in the following areas:

- **Distributed credential discovery.** We specified algorithms and a credential type system that allows some credentials to be stored with their issuer and some with their subject, while ensuring credentials can be found to answer authorization questions.
- **Policy language design.** We identified basic requirements for ABAC policy languages. We found that none of the policy languages used in existing trust negotiation strategies meet these requirements. Prominent trust management languages such as KeyNote also do not meet them. We identified Delegation Logic (DL) as a candidate language that does meet our basic requirements.
- **Design of a realistic negotiation strategy.** We analyzed existing strategies from the point of view of whether they successfully control access to credential content and information about which credentials a negotiator holds. The important ones all have high-bandwidth covert channels that enable unauthorized access to credential content. We have developed design principles and specifications that close the identified covert channels.

The focus of the base task did not include the design or construction of a full access control system; it focused on enabling technology. The

contract contains an unfunded option to build an attribute-based access control system by employing the technology developed under the base task.

Technology Transition

ABAC will have bearing on a wide variety of military and commercial coalition operations. For instance, the DARPA/Army Future Combat System requires rapid deployment and joint, international interoperability. This will require an authorization infrastructure that can be administered efficiently, such as the one being designed by the ABAC project.

Other likely military contexts for deployment of this technology include the U.S. Army Communications-Electronics Command (CECOM), where Joint Vision 2010 aims to maximize information systems integration and interoperability while increasing system/platform effectiveness. Integration of forces will require subjects, including intelligent software agents, from multiple organizations to establish trust with one another rapidly, automatically, and effectively. ABAC project technology is adaptable to contexts, beyond traditional access control, that require trust establishment.

ABAC aimed to address a fundamental problem confronting dynamic coalitions throughout the military and commercial sectors: how to make authorization decisions without requiring prior local knowledge of each subject in the coalition. More generally, this problem confronts any pair of subjects attempting to establish trust with no prior contact or knowledge of one another. The number of situations where this problem will be unavoidable is enormous, and currently there is no satisfactory alternative solution.