

## PROJECT PROFILE

### Advances in Trust Negotiation

#### Objective

Authenticating a subject's identity doesn't help make access control decisions if the subject is a stranger. In dynamic coalitions today, when authorization decisions are based on subject identity, administrative scalability is a serious problem. As organizations enter and leave the coalition, the rate at which coalition members must administer identity records can become unmanageably high. Even a simple staffing change at one organization requires administrative updates at each partner organization. The *Advances in Trust Negotiation* (ATN) project is studying "attribute-based access control" (ABAC), an approach to authorization that addresses this problem of administrative scalability by localizing policy changes required when organizational changes occur. Instead of using subject identity, authorization decisions are based on subject attributes that are housed in portable, verifiable attribute credentials. These attribute credentials contain potentially sensitive data, and must be protected. We call the automated exchange of protected credentials "trust negotiation". The central goal of the ATN project is to provide a clear roadmap for further work in trust negotiation and ABAC, as well as a basis for evaluating their likely future impact on access control.

#### Approach

ABAC enables trust to be established in a subject on first contact, with no prior knowledge of the subject. In a coalition, this means that organizations do not need to maintain databases that associate access rights with each subject in each coalition-member organization. Instead, attributes, such as a principal's roles within her home organization and other qualifications, are used as the basis for determining her rights in interactions with partner organizations.

The model we use gives the policy writer broad powers to delegate authority over attributes of interest. For instance, suppose a web publisher makes a student subscription rate available only to principals that possess a student ID. In this case, the authorization policy must identify recognized issuers of student ids. This is a delegation of authority over the "is a student" attribute. The policy might state, for instance, that issuers of student IDs (e.g., universities) must possess a credential from a known academic accrediting board. In that case, the student would have to present this university accreditation credential, as well as her own ID, to get the student subscription rate.

The above example illustrates one kind of decision that a policy writer may need to be able to delegate: "who is an authority on the attribute of interest?" Within a coalition, resource owners must be able to retain autonomous control of their own resources, while being able to delegate to their natural authorities issues that contribute to the authorization decision. For instance, authorization policies should be able to use the coalition as an authority on the functional assignments of member organizations. Similarly, they should be able to use partner organizations as authorities on their local task staffing assignments. Many of a principal's attributes are sensitive, and must be protected. Thus, credentials are themselves protected resources, and yet, must be disclosed to obtain access to protected resources. To address this chicken-and-egg problem, credentials can be exchanged incrementally and in both directions. Also, each subject may have a potentially large number of attributes, requiring

#### Research Focus

##### Attribute-Based Access Control

Most current access control systems base authorization decisions on subject identity. As groups of organizations increasingly wish to share computing resources, security administrators must spend an ever-growing amount of effort maintaining access rights. For instance, lots of new access rights have to be assigned when a new partnership is formed, or when there are staffing changes in a partner organization. Attribute-based access control provides an administratively scalable alternative to identity-based authorization methods.

**- William Winsborough  
Security Infrastructure  
Group**

## Approach (continued)

automated (or at least assisted) selection of which credentials to submit. Trust negotiation provides abstract protocols for automated exchange of protected credentials. Sensitive credentials are protected by enforcing credential access control policies. Mutual trust is automatically established between software agents through a sequence of credential exchanges in which an agent discloses a credential only when its access-control policy has been satisfied by credentials from the other agent. Although several trust negotiation strategies previously have been proposed, several design goals remain unsatisfied by existing techniques. The ATN project is investigating strategies to try to meet these goals.

To minimize unnecessary disclosure of credentials, some trust-negotiation strategies exchange explicit requests for credentials, thereby focusing disclosures on credentials that are relevant to establishing the quality and variety of trust required. Credential requests use the same notation as attribute-based authorization policies, and may be derived in part from the authorization policies controlling access to credentials. Part of the current effort includes the specification of an algorithm that takes as input an incoming request for locally-owned credentials and the local access policies that govern those credentials. The algorithm returns a counter request for credentials whose disclosure would unlock a set of credentials that satisfies the original input request. Prior results have shown the following property of the protocol that uses this algorithm. If each derived counter request is necessary and sufficient to unlock credentials that satisfy the original request, then the protocol ensures that no credentials are disclosed unless a successful negotiation is possible (in which case the protocol always succeeds). Note that the counter request incorporates content from policies that govern requested credentials. This raises the problem of protecting sensitive policy content. The ATN project is developing protocols that protect sensitive policy content and analyzing the impact on protocol properties. (For instance, it may no longer be possible to guarantee that no credentials will flow unless the negotiation will succeed.)

A further part of this project analyzes and makes recommendations regarding the dynamic determination of trust requirements. The level and quality of trust required for the desired transaction may depend on many factors. Prior work has focused only on server-determined trust requirements that are based on access-control policies associated with static web pages.

Through subcontracts with their academic institutions, several leaders in the new area of Trust Negotiation are engaged in the project. This interaction fosters cross-fertilization and enables the participants to plan carefully the interaction of the elements of Trust Negotiation being developed at the different institutions.

## Additional Information

For additional technical information regarding Trust Negotiation, contact William Winsborough at 443-259-2380 ([wwinsbor@nai.com](mailto:wwinsbor@nai.com)) or visit our Web page at: <http://www.pgp.com/research/nailabs/distributed/trust.asp>.

1/5/01



Who's watching your network

For more information on NAI Labs, contact your authorized NAI Sales Representative, or visit <http://www.nailabs.com>.

**CORPORATE Headquarters**

3965 Freedom Circle  
Santa Clara, CA 95054-1203  
Tel (800) 764-3337\*  
Fax (888) 203-9258

\*Call for additional Worldwide Sales Offices