A Trust Model for Distributed E-Learning Service Control.
Xu, Y.; Korba, Larry

Government, Healthcare and Higher Education (E-Learn 2002),, 2002

National Research Council Canada
Institute for Information Technology

Conseil national de recherches Canada
Institut de technologie de l'information

NRC-CNRC

A Trust Model for Distributed E-Learning Service Control *

Yuefei Xu and Larry Korba

October 2002

* published in World Conference on E-Learning in Corporate, Government, Healthcare and Higher Education (E-Learn 2002) Montreal, Canada, October 14-19, 2002, (accepted - abstract only refereed). NRC 44950.

Canada

A Trust Model for Distributed E-Learning Service Control

Yuefei Xu and Larry Korba
Institute for Information Technology [1]
National Research Council of Canada
[yuefei.xu@nrc.ca | larry.korba@nrc.ca]

Abstract: As with traditional face-to-face education, "trust" is an important factor for the interactive e-learning. To deal with security and privacy concerns, this paper proposes a trust model for distributed interactive e-learning applications. The working mechanisms are based on policy-negotiation and public key cryptography. By using this model and proposed approach, fine-grained trust control of common e-learning services can be maintained. The logical model, core concepts, and typical e-learning trust interaction processes are described. An example is also provided to illustrate how the introduced model would be deployed.

Introduction

Similar to the situation in traditional face-to-face education, "trust" is an important factor in interactive e-learning. On the one hand, the e-learning provider requires some basis upon which to make trust decisions of the learner. For example, the provider must ensure that the user accessing the system, from somewhere on the Internet, is someone eligible for the service. On the other hand, the learner needs to trust that the provider and the services will protect personal information, and will release information regarding performance for instance, only to those authorized by the user.

Trust levels may also indicate the learner's levels of motivation or aspiration for learning. It is easy to imagine that students and teachers, whether young or adult, who thrive in an Internet-based e-learning environment that provides mutual trust, respect, and freedom will become a happy, safe harbor for their learning and teaching activities. Trust then will be the most crucial factor for the success of distance learning process with the maturation of e-learning.

In this work, we focus on security- and privacy-related concerns for distributed e-learning systems, where trusted interaction form the underlying requirement between clients and service providers. The concerns can be divided into two main areas. (1) Security: the concerns may include authentication, confidentiality, authorization, non-repudiation, etc. For example, users can access only those resources and services that they are entitled to access, and qualified users are not denied access to services that they legitimately expect to receive. (2) Privacy: mostly, this refers to the privacy of individuals. This includes all the individual's concerns regarding collection and use of personal information.

Trust is also an important topic in information security research. It has received a good deal of attention in recent years [Mass, Y. 2001]. However, very few focus on e-learning related issues. This is remarkable considering the boom of e-learning applications. Based on our study of proposed or applied trust-related protocols and mechanisms like X.509/PKIX (2002), PGP (2001), and KeyNote [Blaze, M. 1999], we propose a policy-based trust model for e-learning. The model supports policy negotiation between parties. The rest of this paper describes the logical model, core concepts and typical interaction processes. We then provide a sample to show how these concepts and models are used to deal with e-learning security and privacy concerns. We end with discussion and conclusions.

Proposed Trust Model

As most e-learning systems are distributed applications, and the typical application mode in e-learning is demand/supply, we consider the Client/Server (C/S) model as the basic communication model. The

[1] Bldg. M-50, Montreal Rd., Ottawa, ON, K1A0R6, Canada. NRC Paper #44950

browser/web-server model can also be thought as a particular type of C/S model. Peer-to-peer (P2P) e-learning systems have some similarities in that in this instance, each peer has both a client process and a server process. Therefore the C/S analysis is still applicable for these applications.

We propose a policy-based trust model for e-learning systems. This trust model provides fine-grained policy-based security and privacy control for e-learning services as well as provisions for policy negotiation. The logical model is shown as Figure 1.

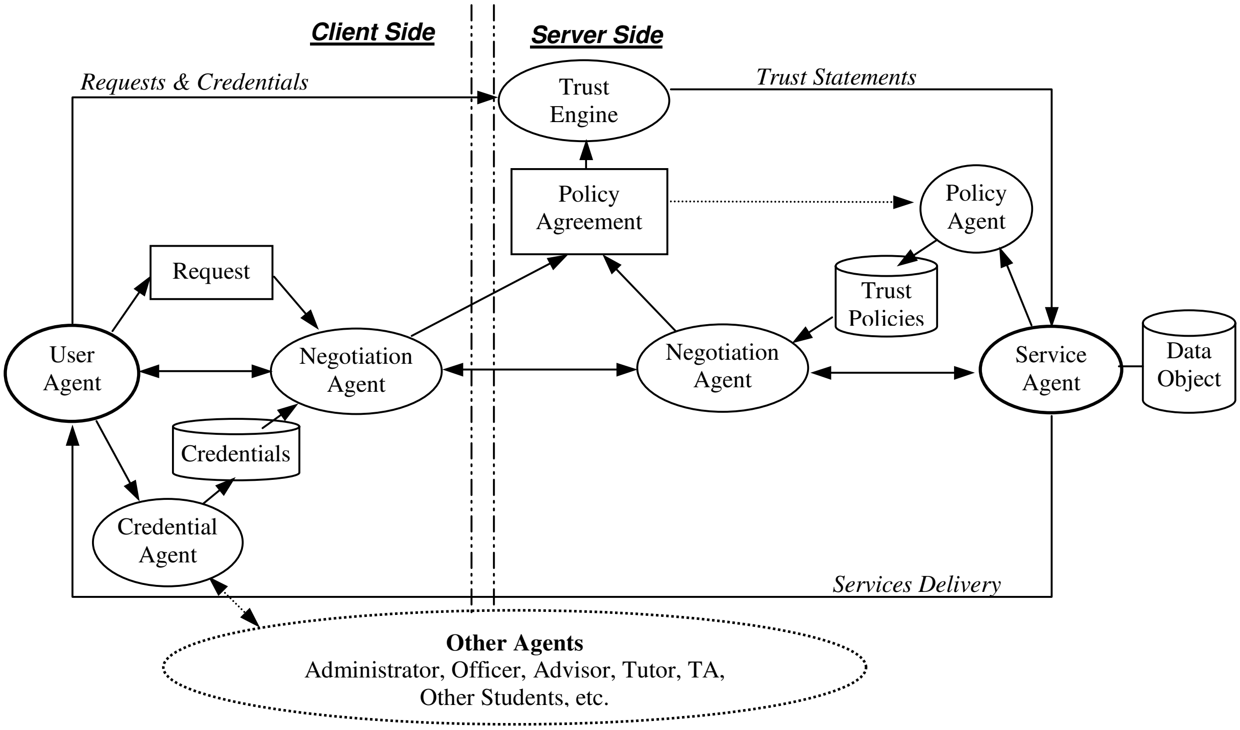

Figure 1. Policy based Trust Model for E-Learning Service Control

There are two logical sides for the model: a client side, which request services and a server side, which provides services. The active agent on the server side is the "service agent, while there is a "user agent" on the client side. In most cases, the clients and servers are geographically distributed and connected by a network (Local Area Network (LAN) or a Wide Area Network (WAN)). The network, including the Internet, may be open and unsecured.

On the server side, there are a series of provided services, such as web contents, multimedia, file management, discussion groups, course registration, and so on. Logically, these services can be seen as many computer processes and a series of data objects. For example, an HTTP server process and many html files provide static web content, and course registration service consists of a register process and some database tables or records. When a learning service receives a request from a user, a new service agent is created corresponding to this request. The service agent and related data objects then responds to the request. Each service agent also maintains a series of policies, which specify the security and privacy concerns on the data objects and services. Only requests compatible with these policies can be served.

On the client side, the user also holds one or more credentials, which certify he has some granted rights to receive some services perhaps under limited conditions. For example, before a student wants to register for a course, the student must provide proof of an approval letter (credential) signed by an advisor or supervisor.

In order to initiate a service, the two sides must first form a service agreement. The service agreement states what service is provided to the user and the conditions for that service. Then according to the request contents, the service agent may deliver some data objects to the user or execute some actions on the data objects.

Core Concepts

Role: The Role describes the operational function of an individual or group in the learning system. Examples of roles include: "tutor", and "registrar officer". This concept is used to simplify system management.

Public Key, Signature: Each individual and each role has a unified key pair: a public key and a private key. Both of these are provided by a designated authority. The public key is used as the identification of the key holder. The private is used to form a signature on the credential and request. This key is a key secret to the individual.

Request: The Request describes who wants to do what, stating the "requestor", "objects", "actions" and "signature". For example, the request of "Bob wants to edit the course score " is described as:

Requestor: Bob's public key
Object: course score
Action: edit
Signature: Bob's signature

Credential: The Credential describes what right the holder has been delegated under some conditions, as well as whether or not the rights can be delegated to third parties and the conditions of such a delegation. Credentials are issued by other agents and normally stored on the user side. For example, the follow credential describes "Scott is delegated by Bob to evaluate the student presentation of course CS302 and during school term of 2002-Fall".

Licensee: Scott's Public Key
Object: Presentation
Action: Evaluate
Condition: if (course = CS302 && term = 2002-Fall) then (approve)
Delegation: No
Signature: Bob's signature.

Trust Policy: The Trust Policy specifies who and what operations are authorized on the data objects and the conditions for those operations. The policies are bound with the service on the server side. For mobile services, the policy is mobile with the service. Service administrators initially define policy. An administrator may authorize other individuals to take on the role of defining policy. The policy has the same format as a credential. The difference is that policy is stored with the service. During the life of an e-learning process, some credentials may be accepted and stored with the service if the policy agent accepts them. In this manner, the user doesn't need to provide this credential again when he request some service. This is implied that multiple credentials may be or may not be required when user requests services depending on what policies the service has had. For example, if Scott has the credential granted by Bob to do something, but the system has no policy allowing Bob to do that, a credential on Bob's priority must be provided at the same time if Scott wants to get the service.

E-learning Trust Interaction Scenario

A typical e-learning trust interaction process is described briefly as follows:

- A user browses the service categories, which describe what services are available and simple statements on requirements for receiving the services.
- The user makes a selection requesting a service. A service provider agent is subsequently generated to deal with the request.
- Requests with the available credential types are collected and checked against the trust requirements of the service policy by the two negotiation agents.
- If the request and credential types are not compatible with the service policy, the two negotiation agents will try to solve the conflicts by coordinating actions on both sides via the following actions:
  (a) Let the provider adjust his policy; and/or
  (b) Let the user change his request; and/or
  (c) Let the user seek more compatible credentials from other agents.

- After negotiation, both sides arrive at a joint agreement. The joint agreement reflects the final service policy corresponding to this request and service. The trust engine then checks the validity of user's credentials, and calculates the final compliance value of the request against provided credentials and the joint agreement.
- The result of this compliance is sent to the provider agent as the "trust statement", which indicates the trust decision as well as additional operational requirements.
- The provider agent provides the corresponding services to the user depending on the trust statement. Some additional actions, such as logging, altering, or encryption, are also executed.

Example

In this section, we briefly illustrate how the introduced model and concepts could be deployed using the following example. In particular, the example involves protection of student personal information. Student personal information stored on the server like address, email, telephone, may be changed at any time by the owner. But some critical data, like name, birthday, or nationality may only be changed with the mutual agreement of both the register officer and the owner. The two policies bound with the service are:

Policy a

Licensee: Registrar officer
Object: Name, Birthday, Nationality of personal record
Action: Edit
Condition: if (approved by Owner) then (approve)
Delegation: Yes
Signature: Administrator's Signature

Policy b

Licensee: Owner of personal data record
Object: Name, Birthday, Nationality of the owner's record
Action: Edit
Condition: if (approved by Registrar Officer) then (approve)
Delegation: Yes
Signature: Administrator's Signature

Then a student "Alice" can delegate her rights to Registrar Officer by issue the following Credential *c*.

Credential c

Licensee: Registrar Officer
Object: Name, Birthday, Nationality of Alice's record
Action: Edit
Condition: if (notify Alice@abc.ca) then (approve)
Delegation: No
Signature: Alice's Signature

Request d

Requestor: Registrar Officer's public key
Object: Name, Birthday, Nationality of Alice's record
Action: Edit
Signature: Registrar Office's signature

If a registrar officer holds the credential c, she/he can edit Alice's record by sending the above Request *d* to the personal record management service. The final trust statement will be *(approve and notify Alice@abc.ca*),

Discussion and Conclusions

People working or learning in cyberspace need mechanisms to develop trusted relationships. Building trust is recognized as a key factor for using and developing the new interaction paradigms, particularly vital for e-learning applications. The approaches and technologies we discussed above could provide a trust decision and enforcement mechanism for interactive distance learning. This work is still at a preliminary stage. There are other important issues to be investigated. In particular, key management, credential version control, and mechanisms for adaptive negotiation among others. Approaches for dealing with these issues are currently being developed within our group. They will be reported in later publications.

Reference

Mass, Y. (2001), Distributed Trust in Open Multi-agent Systems, LNAI 2246, Springer-Verlag, 2001

X509/PKIX (2002), Public-Key Infrastructure, Jan. 2002, *http://www.ietf.org/html.charters/pkix-charter.html*

PGP (2001), An Open Specification for Pretty Good Privacy, July2001, *http://www.ietf.org/html.charters/openpgp-charter.html*

Blaze, M. (1999), The KeyNote Trust-Management System V2, IETF RFC 2704, Sept. 1999