Policy-based Privacy and Security Management for Collaborative E-education Systems

Yang, Chunsheng; Lin, F.O.; Lin, H.

National Research Council Canada
Conseil national de recherches Canada

Institute for Information Technology
Institut de technologie de l'information

NRC-CNRC

*Policy-based Privacy and Security Management for Collaborative E-education Systems. **

Chunsheng Yang, Fuhua Oscar Lin, and Hong Lin

May 2002

* published in: Proceedings of the 5th IASTED International Multi-Conference Computers and Advanced Technology in Education (CATE 2002), Cancun, Mexico. May 20-22, 2002. NRC 44906.

Canada

Policy-based Privacy and Security Management for Collaborative E-education Systems[1]

Chunsheng Yang[1] , Fuhua Oscar Lin[2], and Hong Lin[3]

[1] National Research Council, Ottawa, ON, Canada
Chunsheng.Yang@nrc.ca
[2] Athabasca University, Athabasca, AB, Canada
oscarl@athabascau.ca
[3]University of Houston-downtown, Texas, USA
LinH@uhd.edu

Abstract

This paper presents a policy-based privacy and security management scheme for collaborative e-education systems. Privacy and security management is inevitable in e-education systems. Using the Ponder [2] as policy language specification, we explore how to specify and implement four commonly used policies in e-education systems: security management policies, privacy policies, access control policies, and collaborative pollicies. Some examples from a real e-education project are given to show the potential of this scheme.

Key Words: Privacy and Security, Policy-based Management, E-learning.

1. Introduction

With the rapid development of broadband communication networks such as all-optical networks and mobile communication networks, a great deal of attention has been paid to research and develop e-education systems. E-learning or on-line learning is defined as what occurs when education and training are delivered and supported by the broadband communication networks particular by the next generation Internet. Research has shown that an effective e-education system should have the following features [1]:

(1) an expert-rich content and curriculum,
(2) flexibility and convenience,
(3) continuous assessment and real-time feedback,
(4) multimedia simulation, rich case studies and threaded discussion,
(5) cooperative and interactive learning without time or space constrains, and
(6) safe-enough privacy and security for e-delivery and collaborative education.

Existing research and development in e-education technology is still in the beginning stage. The developed e-education systems or tools, such as [7][8][9], are very slowly accepted. One of the key issues to be solved is how to facilitate the collaboration and interactions among learning communities consisting of professors, tutors, and students. Collaborative e-education systems are considered as one of the feasible solutions, because such systems allow students to interact with the educators who are simulated professors or Professors at University, or intelligent agents distributed on different locations or education institutions. Certainly such collaborative e-education systems require effective privacy and security management mechanism to protect information privacy and insure system safety. Therefore, it is critically important to provide effective mechanisms for security and privacy control and management.

In the fields of network management and distributed system management, the policy-based approach for dynamic system management is widely recognized as an effective and feasible mechanism. We believe that policy-based approach is also suitable for managing and controlling the privacy and security in collaborative e-education systems.

The main tasks in the policy-based privacy and security management for collaborative e-education systems are policy definition, policy translation, policy validation, policy negotiation, and policy management including policy distribution and policy enabling/disabling [5] as well as policy consistence control [6]. In this research, we propose to use Ponder [2][3] as an environment for policy management and implementation in collaborative e-education systems.

This paper is organized as follows. Section 2 discusses privacy and security issues in collaborative e-education systems; Section 3 gives the overview of Ponder. Section 4 discusses the specification and implementation of the policies for privacy and security management. The paper ends with a conclusion and a discussion or description of future work.

2. Security and Privacy Issues in Collaborative e-Education Systems

Collaborative e-education systems can be defined as broadband-network-based distributed multi-agent systems. Such systems provide a cooperative and interactive e-learning environment for students to interact with teachers or intelligent agents in terms of their preferences and interests from any location at any time by using mobile or private access tools [4]. Therefore, privacy and security issues are inevitable.

First of all, security issues cover all security problems related to network (esp. Internet) technology. These security problems contain denial of service for e-learning systems, gathering information from the data delivery, and unauthorized access to the private resource or information in the e-learning systems. These problems have been well protected using the existing security technologies such as PKI for authentication, secure-IP data delivery, and intrusion detection for unauthorized access or denial of service. The main issues to be solved in the collaborative e-education systems are privacy and security management for web-based applications.

Second, privacy is defined as the interest that individuals have in sustaining a 'personal space', free from interference by other people and organizations. Information Privacy in e-learning systems is the interest an education institute (agent) or student has in controlling, or at least significantly influencing, the handling of data about themselves. To protect privacy is to find appropriate balances between privacy and multiple competing interests. Recently, several techniques have been developed for providing privacy protection. Generally, they can be divided into two kinds of techniques: one is for providing pseudonym protection, another is for providing anonymity and unobservability using anonymous communication networks.

Collaborative e-education systems are fully distributed multi-agent systems built on broadband-based Internet. Therefore, to manage overall security and requires the management of system communications among agents. It is desirable that security management could allow students, teachers, or institute-proxies to choose the information (say, course-related information) that they want to share and with whom they intent to share it, and allow users to decide their personal policy for privacy protection with easy-to-use environment. To this end, we propose to use Ponder as security management environment for the collaborative e-education systems.

3. Ponder Overview

Ponder [2][3] was developed at Imperial College over the past 10 years. It is a declarative, object-oriented language for specifying security and management policy for distributed network-computing systems. Ponder policy language is flexible, expressive and extensible to cover the wide range of requirements from the current distributed systems. Ponder can provide following function support for developing policy-based management systems:

(1) Support typed policy specification. The policies can be written as parameterized types and the types can be instantiated repeatedly using different parameters for creating new policies.
(2) Support four basic policy types: authorization, obligations, refrains and delegations and three composite policy types: roles, relationships and management structures.
(3) Support the policy redundancy and inconsistencies detection for a large amount of policy systems and easily to determine the relationships between policy and target object.
(4) Support a Ponder policy compiler, which compiles a Ponder policy type into a policy class and presents it as a policy object at runtime.

Before discussing the policies, we have to introduce some definitions for the terms that are used in the Ponder. These terms are SUBJECT, TARGET, DOMAIN, ACTION, ROLE, RELATIONSHIP, and MANAGEMENT STRUCTURE.

(1) SUBJECT: students, teachers, institutes, and administrators, or system agents;
(2) TARGET: education resources or objects such as course, credits, BBS, Q/A support, library, etc
(3) DOMAIN: a group of objects which the policies can be applied;
(4) ACTION: the activities which subject can carry out. It includes load a new course, remove old course, download course, enable access, disable access, join discussion group, submit assignment, request Q/A help,

(5) ROLE: a group of policies which have the same subject, such as the students from the same department;
(6) RELATIONSHIP: a group of policies which define the right and duties of roles to wards each other, such as the relationship between student and teacher, the relationship between teacher and administrator etc;
(7) MANAGEMENT STRUCTURE: a group of roles and relationship policies, which defines policy hierarchy of organization structure. For example, university, department, and laboratory can be grouped into a management structure.

4. Policies for Pravacy and Security Management

Policies in IETF are defined as the combination of rules and services where rules define the criteria for resource access and usage. The IETF Policy Group [10] are defining a policy framework for classifying packet flows and specifying authorizations for network resource and service. In this framework, the policies are assumed to be objects stored in a directory service. A Policy Decision Point (PDP) retrieves policies from the policies repository and a Policy Execution Point (PEP) like a router requests policy decision through the Common Open Policy Service Protocol (COPS). The PEP enforces the policy for managing the system behaviors. However, this framework does not provide a language specification for specifying policies but is using the X500 Directory schema [11]. In the collaborative e-education systems, the policies are the means specifying or determining the agent behaviors for protecting information privacy and system security without cording the behaviors into the e-education systems or agents. With the policies the e-education systems are configurable for different security requirements in different educating institutes. The policy-based privacy and security management is to specify, transfer, negotiate and manage policies for users, teachers, and institutes. To this end, we must provide a policy management system for the operators to create, upgrade, and manage the policies by using policy specification language. Based on the policy syntax supported by Ponder and the requirements of the collaborative e-education systems, the policies can be classified into privacy policies, security control policies, privacy policies and collaborative policies.

Using those term definitions in Section 3, below we discuss the policies.

4.1. Security Policies

Security policies specify what actions must be involved when a security problem occurs and who must execute the actions and what the system should do. The security policies are used to protect the e-education system safety in order to avoid the attack or intrusion from unauthorized access from inside or outside. These policies are implemented using Ponder Obligation policy type. Therefore the syntax of security policies could be expressed as Figure 1.

```
TYPE OBLIG policyName {
        ON                  abnormal-behaviro-speccification;
        SUBJECT [<type>]    domain-expression;
        TARGET  [<type>]    domain-expression;
        DO
        ACTION  [<type>]    action list;
}
```

Figure 1. Security Policy Syntax

4.2. Access Control Policies

Access control policies are used to define the accessing right for subjects to perform actions on some specifying targets. They are used to protect the education resources and services in e-learning systems. We are using authorization policy type and delegation policy type to support access control policies.

Authorization policy type contains a positive authorization policy and a negative authorization policy. The former is used to specify the action that subjects are permitted to perform on target object; and the latter to specify the actions that subjects are not allowed to perform on the target object. The syntax of authorization policy type is shown in Figure 2.

```
TYPE (AUTH+ | AUTH-)  policyName {
        SUBJECT [<type>]    domain-expression;
        TARGET  [<type>]    domain-expression;
        ACTION  [<type>]    action list;
}
```

Figure 2. Authorization Policy Syntax

Delegation type policy is used to provide permission to the subjects an authorization policy to delegate all or some of their access rights to a new set of subjects. The implementation and enforcement of delegation polices are the same as authorization policies.

4.3. Privacy Policies

Privacy policies define the privacy of an operation that subjects perform and privacy of information that subjects share. They also specify the privacy for subject to create a new policy and decide the privacy of information delivery on the Internet. For example, privacy policy can be used to specify if subjects need a data protection. If they specify the data protection, the data delivered between subjects will be encrypted. We are using refrain policy type in Ponder to implement the privacy policies, because this type policy specifies the actions that subjects must refrain from performing on the target objects. It has similar syntax (as shown in Figure 1) to the authorization policy type. Refrain policies are enforced by subjects rather than access controller because subjects may not trust the target to enforce the policies. For example, when a student wants to submit his assignment to teacher or administrator office with data encryption for delivery we can use following privacy policy to specify this activity.

```
TYPE REFRAIN assignmentSubmit {
        SUBJECT  s=/student A
        TARGET   o=/administrator office or teacher
                          agent
        ACTION    disclose data-public delivery
                  WHEN       submit a assignment
}
```

4.4. Collaborative Policies

Collaborative policies are written with composite policy type which is used to group and inter-relate polices together in order to model the management structure within collaborative e-education systems. The Ponder provides three types of composite policies: roles, relationships and management structures. As mentioned at the beginning of this section, a role could be a group of privacy, security, and access control policies that have the same subjects. We use a relationship to link the roles.

Further, we can composite a management structure from the roles and relationships. For example, Figure 3 shows a collaborative management structure for a typical distance education university. In this management structure there are three roles: administrators office (role1), teachers (role 2) and students (role 3), and two relationships: supervise, report and registration. This management structure policy can be written as follows:

```
TYPE MSTRUCT VirtualUniv. {
        INST    ROLE    administrators;
                ROLE    teachers;
                ROLE    students;
        INST    REL     supervise (teachers,students);
        INST    REL     report
                        (teachers,administrators);
        INST    REL     registration
                        (students, administrators)
}
```

5. Policy Management Service

After designing the policies, based on the Ponder specification, for collaborative e-education systems, we must provide a policy management service for the agents to share the policies and PEP to enforce the policies. To this end, we need a policy service agent, which provides the policies for PEPs such as access controllers and target object agents. In order for PEP to be able to execute the policies, the policies are compiled into policy objects. The policy objects are transferred to PEPs by using COPS protocol. In this study, security policies are compiled into security policy objects (SPOs), privacy policies are complied into privacy policy objects (PPOs) and access control policies are compiled into access policy objects (APOs). These policy objects are dispatched to policy enforcement points in the collaborative e-education systems. This policy management mechanism is shown in Figure 4.

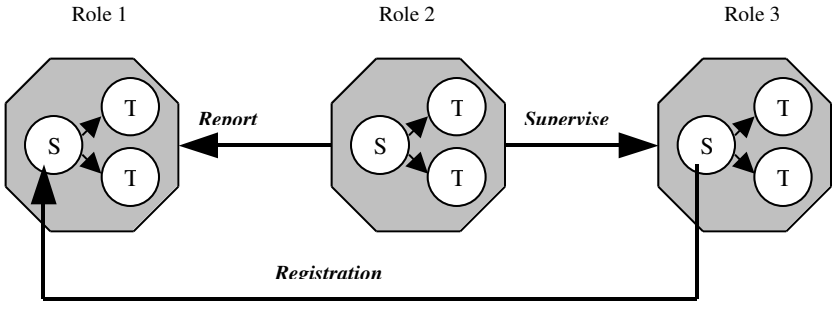

Figure 3. The example of management structure

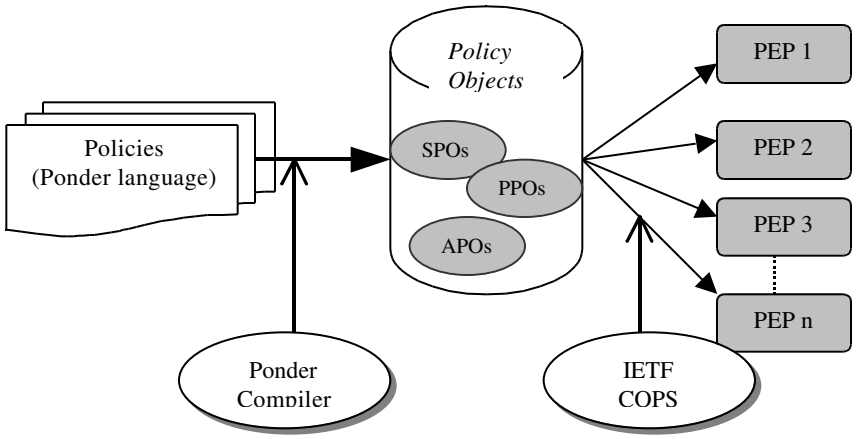

Figure 4. Policy Management Service Diagram

6. Conclusions

We have presented a scheme for privacy and security management in the collaborative e-education systems. Based on the Ponder language specification we designed the policies for managing privacy and security for e-learning systems. We also discussed the policy operation model and policy management service. Comparing Ponder to other policy specification languages such as X500, it can be pointed out that the Ponder is a very useful and flexible language for developing policy-based privacy and security management not only for e-education systems but also other distributed network systems. It can also be pointed out that policy-based approach to managing privacy and security for e-learning systems is feasible and effective. As our future work, we need to work on policy communication or policy convergence between Ponder-based policy and other policy languages. We will also work on policy-based agent coordination for effective collaboration in e-education systems.

References

1. Industry Canada, *National Broadband task Force Guiding Principles, Definitions and Recommendations*, Available from http://broadband.gc.ca/Broadband-ocument/English, 2001
2. N. Damianou, N. Dulay, E. Lupu, M Sloman, *The Ponder Specification Language, Workshop on Policies for Distributed Systems and Networks (Policy2001), HP Labs Bristol, 29-31 Jan 2001*
3. N. Dulay, E. Lupu, M Sloman, N. Damianou, *: A Policy Deployment Model for the Ponder Language* An extended version of paper in Proc. IEEE/IFIP International Symposium on Integrated Network Management (IM'2001), 2001
4. Athabasca University Annual Report 1998-1999. Available from http://www.athabascau.ca/report99/index.htm
5. H. Mahon, *Requirements for a Policy management System*, IETF Internet drat work in progress, available from http://www.ietf.org, 22 Oct. 1999
6. E.C. Lupu and M. Sloman, *Conflits in Policy-based Distributed Systems Management*, IEEE Trans. On Software Engineering, 25(6): pp852-869, Nov. 1999
7. P. Brusilovsky, J. Eklund and E. Schwarz, *Web-based Education for All: a Tool for Development Adaptive Courseware*, in the 7th international World Web Conference, 1998. Availabe from http://www7.scu.edu.au/programme/fullpapers/1893/com1893.htm
8. *Learning Space whitepaper*. Available from http://www.lotus.com/home.nsf/welcome/learnspace
9. *Balckborad Features*. Available from http://www.balckboard.com/products/infrastructure/index.cgi?SELECT=12
10. *IETF Policy Framework workgroup* http://www.ietf.org/html.chartters/policy-charter.html
11. B. Moore, J. Strassner and E. Elleson, *Policy Core Information Model*, Oct. 2000, Available from http://www.ietf/org/draft-ieft-policy-info-model-08.txt