Simulation Modelling Practice and Theory 19 (2011) 1558–1583

Contents lists available at ScienceDirect

Simulation Modelling Practice and Theory

journal homepage: www.elsevier.com/locate/simpat

An innovative simulation environment for cross-domain policy enforcement

Zhengping Wu *, Lifeng Wang

Department of Computer Science and Engineering, University of Bridgeport, 221 University Avenue, Bridgeport, CT 06604, USA

ARTICLE INFO

Article history:
Received 28 August 2010
Received in revised form 10 March 2011
Accepted 17 March 2011
Available online 23 March 2011

Keywords:
Model-driven simulation
Policy enforcement
Cross-domain collaboration
Semantic mapping and translation
Enforcement architecture

ABSTRACT

With the development of policy management systems, policy-based management has been introduced in cross-domain organization collaborations and system integrations. Theoretically, cross-domain policy enforcement is possible, but in reality different systems from different organizations or domains have very different high-level policy representations and low-level enforcement mechanisms, such as security policies and privacy configurations. To ensure the compatibility and enforceability of one policy set in another domain, a simulation environment is needed prior to actual policy deployment and enforcement code development. In most cases, we have to manually write enforcement codes for all organizations or domains involved in every collaboration activity, which is a huge task. The goal of this paper is to propose an enforcement architecture and develop a simulation framework for cross-domain policy enforcement. The entire environment is used to simulate the problem of enforcing policies across domain boundaries when permanent or temporary collaborations have to span multiple domains. The middleware derived from this simulation environment can also be used to generate policy enforcement components directly for permanent integration or temporary interaction. This middleware provides various functions to enforce policies automatically or semi-automatically across domains, such as collecting policies of each participant domain in a new collaboration, generating policy models for each domain, and mapping specific policy rules following these models to different enforcement mechanisms of participant domains.

1. Introduction

Policy-based management is an administrative approach to simplify the management of a given endeavor by establishing policies to deal with situations that are likely to occur. Policies are operating rules that can be referred to as means of maintaining order, security, consistency, or other ways of successfully furthering a goal or mission. Different communities, organizations and domains have their various standards to define policies and policy execution infrastructures to enforce their policies. These policies can be defined by various types of policy languages in their systems, such as WS-Policy [25] and XACML [7]. Low-level enforcement mechanisms can vary from system to system as well. Thus, it is difficult to enforce a policy across domain boundaries or over multiple domains. Before applying policies across domain boundaries, it is desirable to know "which policies can be supported by other domains' enforcement mechanisms," "which are partially supported," and "which are not supported?" A simulation of cross-domain policy enforcement can help system administrators decide not only the applicability of policies at foreign domains but also the workload to support policies from foreign domains. In this

* Corresponding author.
E-mail addresses: zhengpiw@bridgeport.edu (Z. Wu), lifengw@bridgeport.edu (L. Wang).

1569-190X/$ - see front matter © 2011 Elsevier B.V. All rights reserved.
doi:10.1016/j.simpat.2011.03.005

paper, we propose and implement an innovative simulation environment using semantic model mapping and translation for policy enforcement across domain boundaries. As a by-product, this proposed enforcement framework can also automatically generate partial or all enforcement code if elements in a policy model can find their correspondence in low-level enforcement mechanisms. So developers only need to perform coding for the unmapped part of a policy model to support the entire policy set from a foreign domain.

In the proposed simulation environment, the entire policy-based management architecture is divided into three levels, which can be represented by high-level policy language models, intermediate-level processing models, and low-level policy enforcement models. These three types of models are defined by a semantically-rich language – Web Ontology Language (OWL), which can be used to model both policy languages and enforcement mechanisms. So this simulation environment can accommodate different types of high-level policy languages, system administrators can easily introduce a new policy language when a new collaboration is created, and our semantic mapping and translation is flexible throughout the enforcement framework. Usability is another major issue that we try to solve. This environment can be used to simulate policy enforcement for temporary co-operations between or permanent integration of applications and systems from multiple, different domains.

For example, in a healthcare environment, the cooperation and communication between pharmacy, hospital and medical school are essential. They all have their own policy enforcement mechanisms to protect their own proprietary data and patients' records. The problem is there are more and more collaborations and communications between these domains, cross-domain policy enforcement is a necessary component of these domains' information systems. However, in most cases, these domains use different high-level policy languages to define their policies and these specific policies are executed on their own policy enforcement platforms. When a new cooperation or communication is required between two "stranger" domains, we do not know how many policy rules from the stranger domain can be enforced by current enforcement mechanisms. So in most cases, the technical departments from these two domains have to work together to evaluate whether or not it is possible to make their systems work together, and how much work is needed to establish the collaboration or communication, especially for policy enforcement. It is a complex procedure for both participant domains. The same problem also exists in social networking environment, such as how to make sure local privacy policies in one social networking site is suitable for a partner site when they intend to cooperate or communicate. Thus, a simulation environment that can help evaluate this possibility and estimate the potential workload for policy deployment and extra enforcement mechanism implementation would be very helpful. As an integral part of collaboration control or communication control, a good simulation environment can also sort out the odds in potential cross-domain policy enforcement and execution.

In this paper, Section 2 introduces the issues associated with policies from multiple domains using concrete examples. Section 3 illustrates the enforcement hierarchy proposed in this paper. Section 4 provides formal descriptions of the enforcement architecture. Section 5 goes through detailed steps in simulation procedures. Then two case studies and their analysis are discussed in Section 6. Section 7 conveys extant work on related topics, and Section 8 provides a discussion and comparison of our architecture with related architectures. We conclude the paper with a summary and future work.

2. Policies from multiple domains

Policies are operating rules that need to be enforced for the purpose of maintaining order, security, consistency and other ways to successfully further system goals or missions, especially in information systems. For example, in a web application environment, policies need to be enforced for successful web service delivery and governance, especially in the case of dynamic collaborations between services [18]. In any healthcare environment, HIPAA [29] requires certain operation policies and privacy policies to protect patient information. It defines what information is protected, who is covered by privacy protection rules, and so on. In social networking sites (one social networking site is an independent domain) [1,5], privacy protection rules can be formally expressed in policies. When people join a social networking site, they first create a profile, and then make connections with existing friends as well as new friends they meet through the site. A profile is a list of attributes associated with a person, which typically includes the person's real name (or a pseudonym), photographs, birthday, hometown, religion, ethnicity, and personal interests. This list may also contain a person's hobbies, interests and other types of information, which may be considered to be private, such as current and previous schools, employers, drinking habits, and sexual orientation [10,11]. As we know, most existing social networking sites have privacy configurations based on their own enforcement mechanisms. All targets of access control, such as profiles, photos, videos, and daily logs, can be simply called "objects" here, People who desire to visit these objects can be simply called "subjects". Below, we use the privacy configurations from three major social networking sites as examples to illustrate common points and differences in real policies from multiple domains and why policy enforcement simulation is needed for cross-domain enforcement.

For privacy protection, Facebook allows users to define access control policies to protect their "Profile", "Basic Info", "Personal Info", "Status and Links", "Photos Tagged of You", "Videos Tagged of You", "Friends", "Wall Posts", "Education Info", and "Work Info" through a privacy configuration interface. These accessible resources are objects in privacy policies. The access groups include "Everyone", "My Networks and Friends", "Friends of Friends", and "Only Friends." All these access groups are subjects in privacy policies. Fig. 1 is a screen shot of the Facebook privacy configuration interface.

Similar to Facebook, MySpace allows users to define access control policies to protect their "Online Now", "Birthday", "Profile on Mobile", "Comments", "Friends", "Photos", and "Status and Mood" items in their profiles through a privacy