An Innovative Simulation Environment for Cross-Domain Policy Enforcement

Lifeng Wang, Zhengping Wu
Department of Computer Science and Engineering
University of Bridgeport, Bridgeport, CT

Abstract

Policy-based management is necessary for cross-domain organization collaborations and system integrations. In reality different systems from different organizations or domains have very different high-level policy representations and low-level enforcement mechanisms. 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. 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.

Enforcement Hierarchy

High-level policy languages are used to define enforcement policies. Low level enforcement mechanisms allow only enforceable features to be executed. There is a semantic gap between high-level policies and low-level mechanisms, we propose an Intermediate-level processing and translation models to bridge the semantic gap and accommodate different models of high-level policies

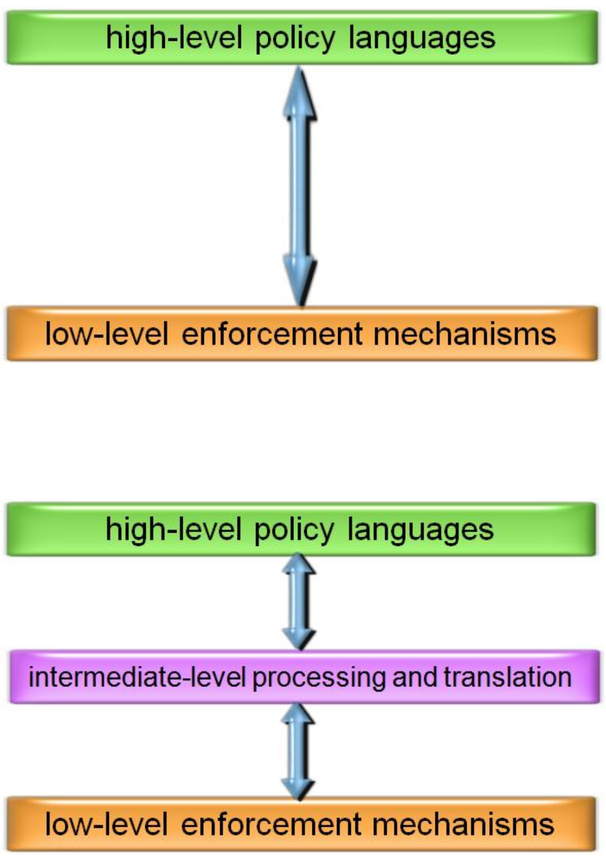

Figure 1. Policy Enforcement Hierarchy

Enforcement Architecture

Step 1:

To find a suitable high-level policy language and its representation model (as illustrated in Figure 2 and Figure 3) to match the policy rule set which is belong to the partner domain.

Step 2:

To derive a middle-level bridge model from the logical model and the representation model (as illustrated in Figure 2 and Figure 3).

Step 3:

To map the middle-level bridge model to available low-level enforcement mechanisms from partner domain using query-based construction (as illustrated in Figure 2 and Figure 3). Then this top-down mapping returns all the unsupported elements in the middle-level bridge model back to the administrator (or user).

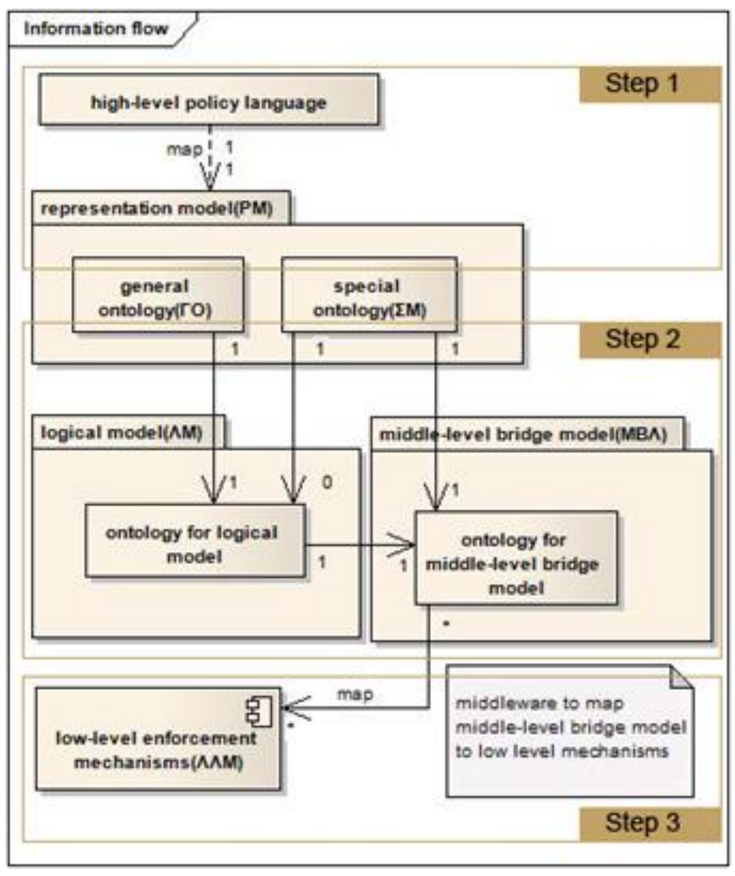

Figure 2. Example of background scene

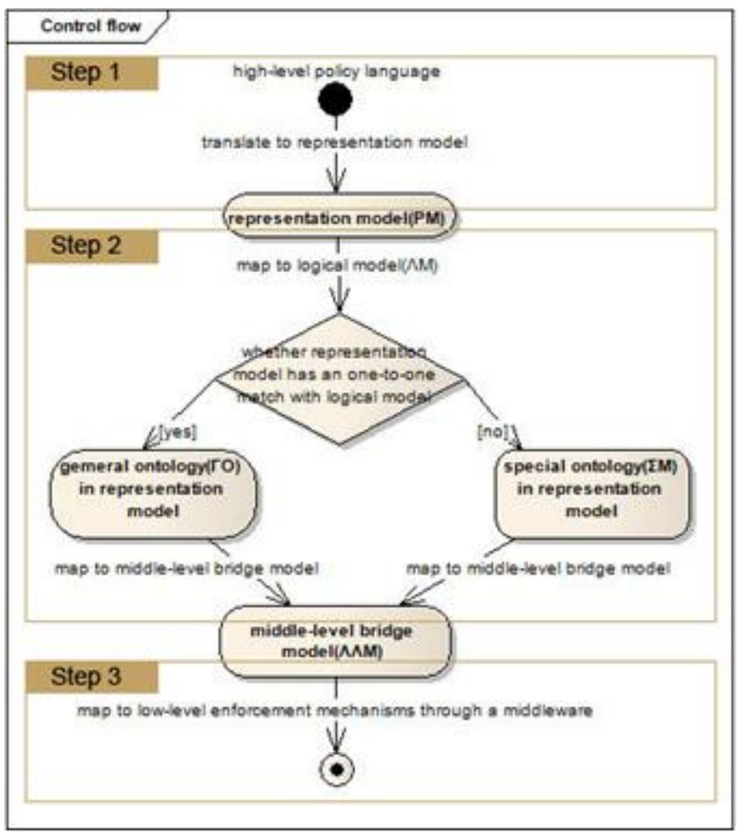

Figure 3. Control flow of the enforcement architecture

Case Study

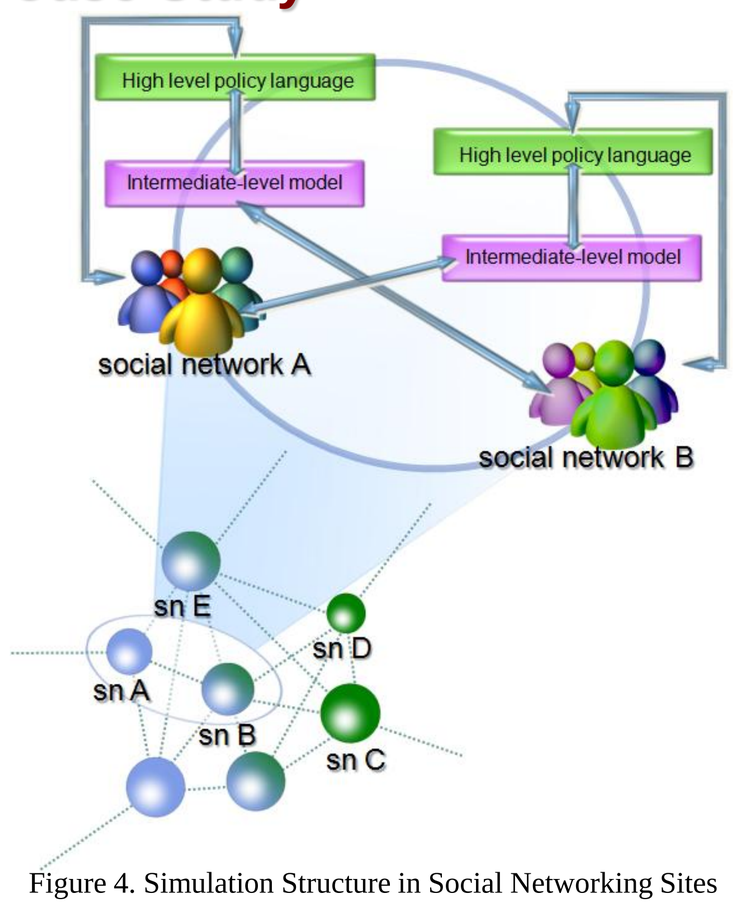

Figure 4. Simulation Structure in Social Networking Sites

We use the social networking as simulation environment. The general ontology for the simulation of privacy configuration migration includes privacy setting elements existing in both websites. The unique privacy setting elements in individual websites are represented in the special ontology. Both parts of the ontology are used by middle-level processing and translation. Finally, the middle-level bridge model of site A is mapped to low-level enforcement mechanisms in site B, and the middle-level bridge model of site B is mapped to low-level mechanisms in site A. Then, we can tell how many privacy configuration elements can be enforced easily across domain boundaries between A and B, which include all elements that can be mapped.

Conclusion

Policy-based management for multiple domain cooperation or collaboration requires system administrators to consider the possibility of integrating or interconnecting two or more domains when these domains have different policy definitions and different policy enforcement mechanisms, we have to estimate the workload for this cross-domain policy enforcement effort, as necessary. This paper introduces a simulation environment to help evaluate the possibility before software development or system rebuild. The central part of this simulation environment is a new enforcement architecture to provide a middle-level component for the mapping process and configuration recording. Once this middle-level component is created, it can be re-mapped and manually modified at any time.