Public Abstract
First Name:Ionut
Middle Name:Ovidiu
Last Name:Ciordas
Adviser's First Name:Gordon
Adviser's Last Name:Springer
Co-Adviser's First Name:
Co-Adviser's Last Name:
Graduation Term:SS 2007
Department:Computer Science
Degree:MS
Title:Fine-grained authorization in the Great Plains Network virtual organization

The last few years have experienced a steady growth in research institutions showing interest in developing research projects that involve more than one institution's computing resources forming so called virtual organizations. The goal of any virtual organization is to provide member institutions with a safe and robust collaborative research environment.

Shibboleth was one of the choices of infrastructure to be used to create a collaborative inter-institutional research environment In the standard Shibboleth architecture, the identity provider (the user's home institution) is in charge of authenticating the user and also of storing all the entitlements that the service provider (the shared resource) is basing their access control decisions. Business and user privacy policies make it difficult to deal with the storage and management of all the entitlements in the identity provider. One problem pertains to the security risks involved in allowing external entities to manage entitlements in the identity management system of an institution. Another problem emerges from the identity providers' usage of the eduPerson object class to store the entitlements that belong to a user. The eduPerson object class does not support significant modifications in its format to allow for virtual organization entitlements to be stored in its structure.

This thesis addresses some of the issues that have slowed the adoption of Shibboleth in deploying fully collaborative research environments. In order to allow for fine-grained authorization at the virtual organization level, there is a need to define, manage and use virtual organization entitlements independently of any institution or participating company. Virtual organization entitlements encompass the idea of a shared resource that needs to be made available to any entitled entity from any member organization. The virtual organization entitlements are maintained separately from the identity provider in the new entitlements repository. The identity provider is in charge of authenticating the users, the service provider is in charge of the authorization decisions, and the entitlements repository is in charge of defining, managing and providing access for queries and updates to be run by the stored entitlements service. The identity provider, the service provider and the entitlements service jointly provide for creating a secure and robust collaboration environment for use by virtual organizations.