A Location Aware Role and Attribute Based Access Control System *

Isabel F. Cruz Rigel Gjomemo Benjamin Lin Mirko Orsini†
ADVIS Lab - Department of Computer Science - University of Illinois at Chicago
{ifc, rgjomemo, plin3, orsinim}@cs.uic.edu

ABSTRACT

In this paper, we follow the role-based access control (RBAC) approach and extend it to provide for the dynamic association of roles with users. In our framework, privileges associated with resources are assigned depending on the attribute values of the resources, attribute values associated with users determine the association of users with privileges, and a location mapping function between physical and logical locations allows to enable/disable roles depending on the logical location of the users and thus preserve the privacy of the location. We use Semantic Web technologies and a graphical user interface based on the Google Maps API.

1. INTRODUCTION

In mobile environments, one of the most important requirements is that of the definition of location aware access control systems. Examples include emergency/disaster, healthcare, and tourism applications. In these environments, organizations can be structured as role hierarchies, such that users can access services and information at different levels. Moreover, the identity of the users may not be known in advance. Therefore, location aware access control systems should have the ability to grant a role to a visitor or to a first time client without permanently registering the user data [2]. Another consideration involves preserving the privacy of the user's location data.

Recent research approaches include the GEOgraphic Role-Based Access Control (GEO-RBAC) model [1, 4], the Extended Role Based Access Control (Ex-RBAC) model [3], and the Role and Attribute Based Access Control model [2].

We have designed and implemented a role-based access control (RBAC) approach that addresses the requirements listed above. In particular, privileges associated with resources are assigned depending on the attribute values of the resources and attribute values associated with users determine the association of users with privileges [2]. Also, we provide a location mapping function between physical and logical locations to enable/disable roles depending on the logical location of the users and thus preserve the privacy of the location [1, 4]. The *location mapping function* is implemented by extending the Google Maps API. Logical locations can be defined over the map and the user's geographic coordinates are converted into logical locations.

For our implementation, we rely on Semantic Web technologies and in particular on the modeling and inferencing capabilities supported by OWL-DL and associated reasoners. OWL-DL ontologies represent the elements of our RBAC model and the features of the application domain. We use the Pellet[1] reasoner to classify resources and roles, to determine the hierarchy of roles based on spatial constraints and user attribute constraints, and to provide consistency checking for the ontologies.

2. SECURITY FRAMEWORK

In this section, we describe the different components that make up our framework.

Access Control Model Ontology

Resource class. Objects in this class (features in the OGC terminology) are identified by names and can be associated with a location. The logical location of a resource can be of type point, line, or polygon, or recursively a collection of disjoint geometries [1]. Resources mapped to a location are defined as *spatial* resources (e.g., $ArtInstituteOfChicago$). Resources not associated to a location are *non-spatial* resources (e.g., $MuseumPass$).

Role class. Objects in this class are declared to have a set of privileges (e.g., $Student, Tourist, Child$).

Role attribute constraints. These are constraints on the values of a user attribute. Each constraint is defined as a pair $< r, c >$, where r is the role name, e.g., *Child*, and c is the constraint associated with that role, which is also a pair $< attribute, attributevalue >$, e.g., $< Age, [0, 10] >$. The role attribute constraint $< Child, Age[0, 10] >$ means that users can assume the role *Child* if they are 10 years old or younger. The constraints are modeled in an ontology as restrictions on the property values.

*Work partially supported by NSF Awards ITR IIS-0326284, IIS-0513553, and IIS-0812258.

†Primary affiliation: Dipartimento di Ingegneria dell' Informazione, Università di Modena e Reggio Emilia, Italy. Work partially supported by MUR FIRB Networked Peers for Business project (http://www.dbgroup.unimo.it/nep4b) and Confindustria Modena.

ACM GIS '08 , November 5-7, 2008. Irvine, CA, USA (c) 2008 ACM ISBN 978-1-60558-323-5/08/11...$5.00.

[1] pellet.owldl.org/

Role spatial constraints. A spatial constraint on a role is defined as a pair $< r, e >$, where r is the role name and e is the spatial extent of the role, that is, the set of locations where the role is valid. For example: $< TouristOperaPass, LyricOperaHouse >$ is a role spatial constraint. The Role $TouristOperaPass$ will be enabled if the user is in the location $LyricOperaHouse$. A hierarchy is defined over the set of spatial constraints to represent a *partial order* or *lattice* $\preceq$ on the roles [4]. Given two spatial constraints $< r_i, e_i >$ and $< r_j, e_j >$, if $< r_i, e_i > \preceq < r_j, e_j >$ then a user assigned to r_j is also assigned to r_i and e_j is spatially contained in e_i. Thus, if the role r_j is enabled, the role r_i is also enabled.
Action class. This class represents the actions that can be performed by users on the resources (e.g., $FreeEnter$).
Privilege class. Objects of this class represent pairs $< Action, Resource >$, where the one-to-one association is imposed by a cardinality constraint [2].
Privilege attribute constraints. These are constraints on the values of a resource attribute. The constraints are defined as pairs $< p, c >$, where p is the privilege name (e.g., $AllowCamera$) and c is the constraint associated with that privilege, which is a also a pair $< attribute, attributevalue >$ (e.g., $< AllowedObjects, camera >$).
Session. A user is assigned a session upon entering the system (e.g., $John\_680481$). A session is owned by a single user and has a set of roles associated with it.

Modeling and Description Logics Reasoning

The first step in our approach is to develop (or reuse) ontologies to model the domain. The second step consists of providing an RBAC classification for all the classes of the domain ontologies. The Description Logics reasoner propagates that classification to all the domain ontology elements using both axioms (e.g., defining a resource) and any valid inference, such as inheritance (e.g., subclasses of *Student* will be classified as *role* and share the same privileges). Other functions of the reasoner include grouping resources according to their security policies (e.g., museums and churches) and defining the role hierarchy based on the spatial constraints.

Access Model

Constraints can be defined on the attribute values of resources or users. When a constraint is defined on a resource attribute value, a privilege is associated with the resource only if the resource value satisfies the constraint. The constraints defined on user attribute values allow to dynamically assign roles to a user. A role is assigned to a user and enabled if the role attribute constraints are satisfied by the user's attribute values. In addition, a role is dynamically enabled depending on the user's logical location.

3. DEMONSTRATION

To demonstrate our access control model, we developed a client-server application supporting a graphical user interface based on the Google Maps API (see Figure 1) and considered a tourism demonstration scenario. During the demonstration, we will show a map of the city of Chicago with several attractions (e.g., museums, monuments, parks), which are modeled as spatial resources in the ontology and visualized with different colored elements (points, lines, polygons) on the map.

Multiple user sessions, each identified by a session ID and represented by an icon on the map, can be created. When

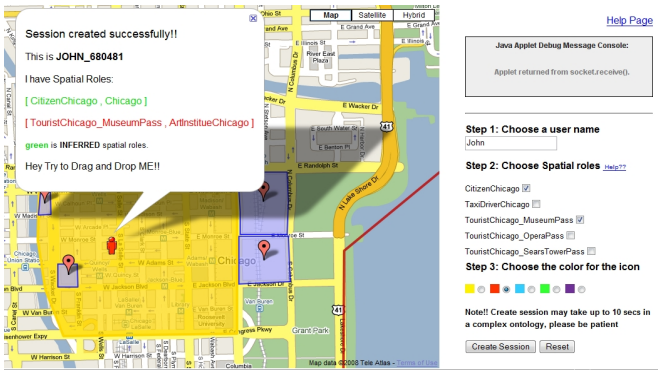

Figure 1: Graphical user interface.

a session is created, the set of available roles for the user is shown. Also, multiple clients can interact with the system concurrently. The demonstration will show the dynamic capabilities of our system in three different ways:

(1) Depending on the attribute values of a resource. For instance, we define the privilege *AllowCamera*, which allows visitors to take their cameras inside a museum. If the privilege constraint $< AllowedObjects, camera >$ is verified for a particular museum, e.g., *ArtInstituteChicago*, then visitors can take their cameras into *ArtInstituteChicago*.

(2) Depending on the attribute values of a user. For example, when a session starts, the user age is checked and if smaller than 10, the role constraint $< Child, Age[0, 10] >$ is dynamically associated with the user and the role *Child* is enabled. The privilege $< FreeEnter, MuseumsChicago >$ associated with the role *Child* allows the user to enter museums in Chicago for free.

(3) Depending on the location of a user. Our user interface allows for dragging and dropping icons that represent user sessions on the map, and placing them inside areas of interest, for example, the *LyricOperaHouse*. Then the spatial constraint $< TouristOperaPass, LyricOperaHouse >$ is verified and the role *TouristOperaPass* enabled. If the icon is placed outside the location *LyricOperaHouse* (but still spatially contained in *ChicagoLoop*), then $< Tourist, ChicagoLoop >$, which is the inferred role spatial constraint, is verified. The role *Tourist* will be enabled and the role *TouristOperaPass* disabled.

4. REFERENCES

[1] E. Bertino, B. Catania, M. L. Damiani, and P. Perlasca. GEO-RBAC: A Spatially Aware RBAC. In *ACM Symposium on Access Control Models and Technologies (SACMAT)*, pages 29–37, 2005.

[2] L. Cirio, I. F. Cruz, and R. Tamassia. A Role and Attribute Based Access Control System Using Semantic Web Technologies. In *Int. IFIP Workshop on Semantic Web and Web Semantics*, volume 4806 of *Lecture Notes in Computer Science*, pages 1256–1266. Springer, 2007.

[3] X. Cui, Y. Chen, and J. Gu. Ex-RBAC: An Extended Role Based Access Control Model for Location-aware Mobile Collaboration System. In *Int. Conf. on Internet Monitoring and Protection (ICIMP)*, pages 36–42, 2007.

[4] M. L. Damiani and E. Bertino. Access Control and Privacy in Location-Aware Services for Mobile Organizations. In *Int. Conf. on Mobile Data Management (MDM)*, pages 11–20, 2006.