# Access Control in a Port – A GeoRBAC Approach

Eneko Olivares[1], Benjamín Molina[1], Carlos E. Palau[1], Manuel Esteve[1], Miguel A. Portugués[2], Alejandro García-Serrano[2]

[1]Universitat Politècnica de València
{enolgor, benmomo, cpalau, mesteve}@upvnet.upv.es
[2]InfoPort Valencia (IPV)
{maportugues,agserrano}@infoportvalencia.es

**Abstract:** Access Control mechanisms are nowadays mandatory to guarantee a minimum level of security in physical or logical environments. Different attributes can be used to grant access to users. In critical infrastructures individual position of users and devices is a clear alternative or complement. GeoRBAC is an extension of the Role Based Access Control (RBAC) mechanism that considers the position as another condition when performing access control decisions. In this paper we propose a real implementation and deployment of a GeoRBAC system integrated in the ICT infrastructure of a port, using OGC Sensor Web Enablement (SWE) set of standards to allow geolocation information interoperability.

**Keywords:** Access Control Mechanisms, Location-Based Services, Security, Transport and Logistics

## 1 Introduction

One of the key security aspects of any critical infrastructure (either logical or physical) to preserve security is access control, because it concerns how users can access resources in those infrastructures. It is understood as the protection of the resources of an infrastructure through a process that decides their access rights, regulated by a security policy. Different access control mechanisms have been proposed in the literature related to CIs (Critical Infrastructures) protection; however access control mechanisms considering geolocation improve security, because a user's location is correlated to the access rights he is entitled to [3].

The proposed access control system is based on the GeoRBAC model, and has been tested in the premises of a CI (i.e. the Port of Valencia).

This paper is structured as follows: Section II presents an outline of the system work. Section III describes the system and its main functionality. The chapter ends with the conclusions and further work.

## 2 Outline of the System

The system was originally designed to fit in a specific port environment, which currently uses a Port Community System (PCS) to exchange and manage all data of the different organizations working in the port. Our system integrates with the PCS to retrieve all required data (users, roles, operations and permission sets) and store it on a separate database. The core of the system is a Complex Event Processor (CEP) that performs all different access control decisions, generating the corresponding messages and alerts of the different access control events, sending them to the management interface.

In order to retrieve real-time information about the position of the tracked users, a SOS (Sensor Observation Service) server was used as intermediary to collect and store every location device positions. The SOS is part of the Sensor Web Enablement standards and defines the web interface of a service that provides methods to perform CRUD (Create, Read, Update and Delete) actions of sensors and data provided by them [1] [2].

In the port environment the SOS collects all data regarding location of vehicles, people and tracked containers. Some of this location data comes from the PCS and some is collected directly from tracking devices.

## 3 Design and Development

The system has been mainly designed for outdoor environments, although it could be easily adapted for indoor cases with proper indoor positioning. The main features of GeoRBAC have been implemented (role-schemas, spatial-roles, fully OGC compliant) whereas others are missing for simplicity reasons (role hierarchies, user assignments, activation between roles and granularity) [4]. Furthermore, some features not defined as part of the GeoRBAC model were added in order to create a globally functional system (policy administration and policy integration).

### 3.1 Description of the GeoRBAC implementation

The design of the system is modular, where different components can be attached to the core through adapters. In core includes the Complex Event Processor that is in charge of making access control decisions based on defined rules.

In order to determine if a particular user is inside or outside a zone the CEP uses geo-fencing algorithms. As every boundary can be modelled as a polygon, the Point In Polygon (PIP) algorithm is used, since it is independent of the units used.

Rules, users, roles, bounded areas and registered devices are fed into the core by a database. The database engine (preferably relational) is totally independent of the system, and different adapters are provided to unify the output format of the data in a common interface accessible from a Data Access Object (DAO).

The location data is received from a collector where it is possible to define different position sources (depending on the device that retrieves positioning data). The collector receives data in the same units as the defined zone boundaries for all the different

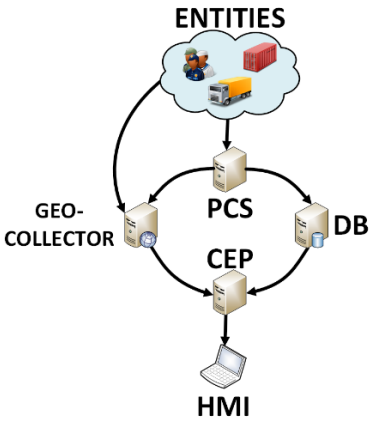
sources, so an intermediate layer of conversion has to be defined if the position source feeds location data in a different unit.

There is a distinction between the user and the device that provides the position of the user (so every device can be easily replaced or reused). To achieve this, every device should have a unique identifier and be associated to a user.

The last core component is in charge of receiving and forwarding access control decisions, logging data and positioning data. Different receptors can be registered to receive all or specific types of messages so whenever any component triggers an action that generates a new message this will be forwarded to the corresponding receptor.

Every component that has to establish an outside communication (e.g. database server connector or all the position sources that are not simulated) is completely free to choose its own security layer, if any. In this way, simple components that don't need a security layer (e.g. behind a proxy inside a trusted network that handles security issues) are easier to implement and components that require specific configurations will handle its own security layer (e.g. specific SSL trusted chains).

In the following images the GeoRBAC mechanism are illustrated in the use case environment (Figure 1), with the different building components (Figure 2).



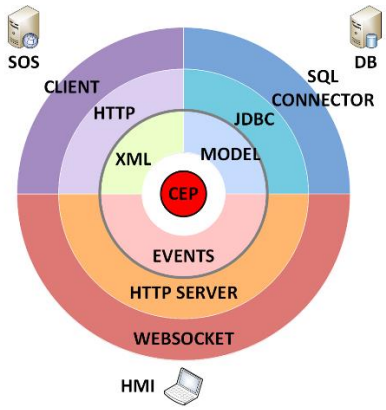




**Fig. 1.** General overview of the system **Fig. 2.** Detailed GeoRBAC implementation

## 4 Conclusions and Future Work

The presented GeoRBAC proposal has been successfully implemented in the Valencian port system for a pilot. Although there were some features not initially implemented, in subsequent iterations this was resolved.

Some features of the Prox-RBAC model [5] were also added, such as the transmission of permissions, but only under certain circumstances.

In order to increase the interoperability with other systems, everything that had to be geometrically described such as positions (points) or zone boundaries (polygons) was

defined under the OGC standards. The SWE also normalizes the interfaces for accessing sensor information and hence increases interoperability.

The system has been thoroughly tested aiming for a ready-to-use and functional service in a production environment such as a port. For this purpose, a lot of effort went into increasing the usability of the system; making a simple and clear interface to configure the server reduces the possibility of human error that could potentially lead to a security hole.

As for future work and extension points of the system, the main features that the system lacks and will be covered in future iterations are role hierarchies, multiple operations and different granularity levels.

## Acknowledgment

The work in this paper has been partially funded by CELTIC ACIO: Access Control In Organizations, co-funded by the Ministry of Industry (AEESD - TSI-100201-2013-50); and H2020 DORA: Door to Door Information for Airports and Airlines (H2020-MG 635885).

## References

1. Sensor Observation Service (SOS), Open Geospatial Consortium (OGC), available at http://www.opengeospatial.org/standards/sos, last visited May 2013.
2. Giménez P., Molina B., Palau C. E., Esteve M.: Sensor Web Simulation and Testing for the IoT, IEEE International conference on Systems, Man, and Cybernetics (IEEE SMC 2013), Manchester, October 2013
3. David F. Ferraiolo and D. Richard Kuhn. Role-based access controls. 15th National Computer Security Conference, pages 554–563, 1992.
4. Maria Luisa Damiani, Elisa Bertino, Barbara Catania, and Paolo Perlasca. 2007. GeoRBAC: A spatially aware RBAC. ACM Trans. Inf. Syst. Secur. 10, 1, Article 2 (February 2007).
5. Michael S. Kirkpatrick, Maria Luisa Damiani, and Elisa Bertino. Prox-RBAC: A proximity-based spatially aware rbac. In Proceedings of the 19th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems, GIS '11, pages 339–348, New York, NY, USA, 2011. ACM.