An Access Control Mechanism for Geospatial Information Services

Jiayuan LIN*, Yu FANG, Bin CHEN, Yumei SUN
Institute of Remote Sensing and Geographic Information System, Peking University
Beijing, P.R.China 100871

Extended Abstract

The specifications of geospatial information services (WMS, WFS, WCS, etc) ratified by OGC provide a comprehensive framework for integration and sharing of distributed and heterogeneous geospatial information. In general, geospatial information services are software objects performing geoprocessing functions, such as map visualization, conversion of coordinate systems and geospatial analysis, which are invoked by clients through standard interfaces. Geospatial information services are significant because they represent a viable alternative to the traditional isolated, complex and often under-utilized GIS systems.

The problem, however, that has not been much explored by the GIS community is how to secure access to geospatial information. The strong demand for geospatial information security is motivated by several factors: 1) geospatial data may contain sensitive information, so that data cannot be freely disclosed; 2) users of geospatial information services, such as public administrations, urban planners, and surveyors, due to their different roles and expertise, need to be assigned different rights for operating on geospatial data; 3) controlled access to corporate and government data is also of vital importance for the development of SDIs; 4) Likewise, geospatial data providers need to license and protect the resources they publish on the Web.

Geospatial information security typically contains three aspects: confidentiality, integrity, and access control. The first two have already had satisfactory solutions in IT domain, namely cryptography and digital signature. This paper is focused on access control, for which general access control mechanisms are coarse-grained and do not take account of geometric properties of geospatial data. Access control includes authentication and authorization. Authentication ensures that login users are legal for geospatial systems, and authorization will allow legal users only to do permitted operations on intended geospatial data.

In fact, we can implement access control for geospatial information services in applications. However, this method is error-prone as applications have full privileges on the target geospatial web services, which can easily cause information leakage. On the other hand, authorization rules are difficult to share between different geospatial systems which have similar access control needs. Therefore, the desired access control mechanism should be standard and application independent. A possible solution is the ISO/GMITS standard, which provides the baseline security for geospatial information services. However, it cannot meet flexible and expressive requirements of geospatial access control. In this paper, we shall adopt GeoXACML-based security framework to realize access control functionalities for geospatial information services.

The rest of this paper is simply described as follows:

*linjiayuan@gmail.com; phone +86-10-62769285 ext.803
Project 40501052, supported by NSFC; Project 2006AA12Z201, supported by The National High Technology Research and Development Program of China

First of all, we discuss access control requirements of geospatial data. In general, we can get geospatial data in the granularity of map layer or individual objects according to their descriptive properties, geometric properties, or their combination by issuing invocations on intended geospatial information services. Therefore, access controls are classified into two categories in terms of granularities: 1) map layer access control. Features in a map layer generally have the same feature type (point, line, polygon, or composite type). Hence it is also called feature type access control. 2) feature access control. One case is that we define restriction on the set of features whose descriptive properties meet some conditions. Another case is that geometric properties of features are used to define restriction, which meet specific geospatial relation with a referring geospatial object. Certainly, restriction definition with the combination of spatial and non-spatial properties should be supported as well.

Secondly, we introduce XACML and its extension in geospatial domain, GeoXACML. XACML is a general purpose access control policy language, which provides a syntax (in XML) to define action (request) rules for subjects (users) and targets (resources). XACML describes both an access control policy language and a request/response language. The policy language is used to express access control policies (who can do what, where and when). The request/response language expresses queries about whether a particular access should be allowed (requests) and describes answers to those queries (responses). According to the extensibility points of XACML, such as DataType, FunctionId and AttributeId, GeoXACML defines different URNs to incorporate geometric attribute values, topological relation testing functions, Service-Id and Operation-Id resource attributes, and coordinate reference system (CRS) resource attribute.

Thirdly, XACML serves as a standard format for authorization information, but depends on other standards, such as SAML to specify security assertions and transport mechanisms. SAML defines the schema intended for use in requesting and responding with various types of security assertions. The SAML schema include information needed to identify and validate the contents of the assertions, such as the identity of the assertion issuer, the valid period of the assertion, and the digital signature of the assertion. The extended SAML types of queries and statements for XACML include XACMLPolicyQuery, XACMLPolicyStatement, XACMLAuthzDecisionQuery, XACMLAuthzDecisionStatement.

Finally, we present the access control framework for geospatial information services using GeoXACML and SAML. The components of the framework contains clients, Policy Enforcement Point (PEP), Policy Decision Point (PDP), Policy Administration Point (PAP), Attribute Authority, XML Key Management System (XKMS), and geospatial information services. The client firstly sends a request to SAML PEP for accessing geospatial information service. After its signature is examined by XKMS, SAML PEP will encode the access request in GeoXACML format, encapsulate it as SAML assertion, and then forward the assertion to PDP. SAML PDP obtains appropriate attribute values from AA, and evaluates the policies. Then it decides access possibility and returns the response to the SAML PEP. Finally PEP will allow or deny the client's request for accessing the geospatial information service. PAP is responsible for creating and modifying specific authorization rules for geospatial information services.