Access Control in Spatial Data Infrastructures

GSDI 12, Singapore
October 21, 2010

Jan Herrmann
herrmanj@in.tum.de
Technical University Munich
Department of Informatics
Chair for Applied Informatics / Cooperative Systems
Agenda

• introduction

• requirements for access control systems for SDIs

• appropriate concepts and technologies to build an access control system for SDIs

• administration of access control policies
Baseline: Characteristics of Spatial Data Infrastructures

- spatial data and metadata
- spatial services (usually OGC Web Services – OWS)
- many distributed users, services and data sources from different administrative domains

---

Various IT security requirements

- OWS requests / OWS responses
- WFS-T
- WMS
- WPS
- WFS
Access Control Systems for SDIs: Requirements

• definition and enforcement of access rights that refer to ...
  – individual resources of different classes. E.g.:
    • the **machine** with IP-address 123.123.123.123
    • the **service** on port 1234 of the machine with IP-address 123.1.1.1
    • the building **feature** with ID 002
    • the price **attribute** of the building feature with ID 002
Access Control Systems for SDIs: Requirements

• definition and enforcement of access rights that refer to ...
  – individual resources of different classes
  – resources with certain properties. E.g.:
    • building features who’s owner = Alice
    • building features with price < 500,000 €
    • building features with location within Germany
Access Control Systems for SDIs: Requirements

- definition and enforcement of access rights that refer to ...
  - individual resources of different classes
  - resources with certain properties
  - resources of a certain class. E.g.:
    - features of class building
    - features of class street
    - features of class POI
Access Control Systems for SDIs: Requirements

- definition and enforcement of access rights that refer to ...
  - individual resources of different classes
  - resources with certain properties
  - resources of a certain class
  - subjects with certain properties. E.g.:
    - all adult persons
    - all employees of land surveying office XYZ
    - all US citizens
    - all firemen within a disaster area
Access Control Systems for SDIs: Requirements

- definition and enforcement of access rights that refer to ...
  - individual resources of different classes
  - resources with certain properties
  - resources of a certain class
  - subjects with certain properties
  - environment states with certain properties. E.g.:
    - from Monday to Friday
    - between 8 am and 6 pm
    - during high system load
    - during a state of emergency
Access Control Systems for SDIs: Requirements

• definition and enforcement of access rights that refer to ...
  – individual resources of different classes
  – resources with certain properties
  – resources of a certain class
  – subjects with certain properties
  – environment states with certain properties
  – arbitrary actions. E.g.:
    • read/select, delete, insert, update
    • getFeature, getMap, ...
    • getObservation (from sensors)
Access Control Systems for SDIs: Requirements

• definition and enforcement of access rights that refer to ...
  – individual resources of different classes
  – resources with certain properties
  – resources of a certain class
  – subjects with certain properties
  – environment states with certain properties
  – arbitrary actions
  – the arguments of service requests. E.g.:
    • the data that shall be inserted
    • the resolution of a map
    • the version of a feature
  – ...
Access Control Systems for SDIs: Requirements

- the enforceable set of access rights shall be independent of ...
  - the clients’ software and
  - the access control capabilities of the
    - service implementations and
    - data source management systems (e.g. DBMS or file system).

→ enforce access control based on Web Service request or response only
Access Control Systems for SDIs: Requirements

- build an access control system based on standards
  - prerequisite for distributable and interoperable
    - access control policies and
    - access control system components (PEPs, PDPs etc.)
Suitable Conceptual Access Control Models

• combination of
  – rule based access control models
  – rewrite based access control models
    • handling of partially authorized OWS requests or responses
      – delete unauthorized nodes in OWS request or response
      – insert or update nodes in OWS requests
    – role based access control models

• not suitable:
  – Subject-Action-Resource access control models (e.g.: Matrix, ACL)
  – View based access control model
  – Tagging based access control model
A Suitable Logical Access Control Model

- eXtensible Access Control Markup Language (XACML) - OASIS
  - standardized languages to express access rules and access control decision requests/responses
  - XACML v3.0 core specification
  - XACML v3.0 profiles (e.g. the hierarchical resource profile, the multiple decision profile and the RBAC profile)
A Suitable Logical Access Control Model

- eXtensible Access Control Markup Language (XACML) - OASIS
  - XACML v3.0
  - XACML v3.0 profiles
    - XACML v3.0 hierarchical resource profile v1.0
    - XACML v3.0 multiple decision profile v1.0
    - XACML v3.0 RBAC profile v1.0
- GeoXACML v1.0 - OGC
  - standardized extension of XACML
  - allows to express spatial access control rules
- XACML v3.0 OGC Web Service profile - OGC
  - guidelines how to use (Geo)XACML to protect OGC Web Services
Administration of (Geo)XACML policies

• challenges
  – many users, roles, services, classes, attributes and features
  – complexity and amount of rights
  – dynamics of data, users, administrators, roles and rights
  – many interrelated administrative domains
Administration of (Geo)XACML policies

- challenges
- components needed for a sound administration

1. Policy Administration Service (PAS)
   - create, read, update and delete operations on policies
   - methods to analyze, test and optimize policies
     (e.g. consistency checks, redundancy checks)
Administration of (Geo)XACML policies

- challenges

- components needed for a sound administration
  1. Policy Administration Service (PAS)
  2. PAS-Client with an appropriate UI
     - abstract from the policy language syntax
     - provide GIS functionality to support an easy definition of (spatial) rules for spatial data
Administration of (Geo)XACML policies

• challenges
• components needed for a sound administration
  1. Policy Administration Service (PAS)
  2. PAS-Client with an appropriate GUI
  3. Layered Administration Model (LAM)
     – motivation:
       – partitioning of administrative tasks/rights. E.g.: to
         – ensure that admins can handle the administration of policies,
         – avoid the accumulation of administrative rights)
       – control the mutual influence of cooperating administrators
       – ensure interoperable policies that can be efficiently enforced and analyzed
       – ...
       – concept: layers of access control systems for the PAS
The Layered Administration Model

Layering can be continued as needed
Conclusion

• protect data and services in SDIs with (Geo)XACML based access control systems

• sound and manageable administration of policies can be achieved by using
  – a powerful Policy Administration Services and
  – following the Layered Administration Model
thank you very much for your attention

questions, comments, ...?

Jan Herrmann
herrmanj@in.tum.de
Technische Universität München