GeoShield project

Managing authentication and permissions to OGC services

Presenting the new GeoServer Resource Access Manager plug-in and the Sensor Observation Service protection

Milan P. Antonovic, Institute of Earth science - SUPSI
Massimiliano Cannata, Institute of Earth science - SUPSI

12 November 2011
Presentation outline

• Introduction to the Institute of earth science – SUPSI
  – OGC implementations used
  – The need of data protection
• Presenting GeoShield
  – GeoShield’s protection strategies
  – Web administration interface
  – OGC Services covered by GeoShield
  – The Sensor Observation Service protection
  – The GeoServer Resource Access Manager plug-in
    • Access rule application process
    • Data access rule application
  – GeoServer Resource Access Manager plug-in demo
  – Next improvements
Introduction to the Institute of earth science – SUPSI

Fields of activity:
• Land Planning
• Hydrogeology
• Hydrology
• Geology
• Geomatics

Focused on:
• Government mandates
  – Geo databases maintenance
  – Web applications for decision making
    • Natural hazard
    • Water protection
    • Wells / Springs / Boreholes
    • Hydrological monitoring network
• Interregional projects (EU, World Bank)
• Training courses
• Research projects
OGC implementations used

- Geografical data serving

- Monitoring data

- Data processing service
The need of data protection

How to protect in a **centralized way** all the services??

Sensible data

Mixed data

Public data
Presenting GeoShield

• GeoShield is an Open Source solution for authentication and authorization management to OGC services

• Written in **Java**

• Relies on:
  • Apache Commons
  • GeoTools
  • EclipseLink [Persistence API]
  • PostgreSQL
  • Flexjson (JSON parser)

• Web administration interface
  • Desktop like user interface
  • Sencha - Ext JS

• OGC standards protected
  • WMS
  • WFS
  • SOS

• GeoServer plug-in:
  • Resource Access Manager
GeoShield’s protection strategy

Compatibility with:
- Web browsers
- Desktop applications
  - Udig, QGIS, ArcGIS

HTTPS

Web

GeoShield Security Proxy

Web administration interface
GeoShield’s PRE-processing protection strategy

GetFeature

The data

Loading CQL for each layer

GetFeature + OGC Filter

Forwarding the data
GeoShield’s POST-processing protection strategy

1. Parsing response
2. Adapt response according to user filter

User

GeoShield

OGC service

GetCapabilities

Capabilities document
Web graphical user interface

- **Password** protected
- User friendly (**Desktop-like** Graphical User Interface)

- **Managing authorization** for:
  - Users
  - Groups
  - Services
  - Permissions
  - Permitted requests

![Web graphical user interface](image)
OGC Services covered by GeoShield

Web Map Service 1.1.1:

*Standard protocol for serving georeferenced map images over the Internet*

- **GeoServer** (tested):
  - Filtering capability **CQL** (Common Query Language)

- **Others** (not tested)
  - INCLUDE/EXCLUDE filters only

- Requests:
  - GetCapabilities
  - GetMap
  - GetFeatureInfo
  - GetLegendGraphic

12 November 2011
OGC Services covered by GeoShield

Web Feature Service 1.1.0:

*Standard protocol allowing requests for geographical raw data over the Internet*

- Permissions definition:
  - Filtering capability **CQL** (Common Query Language)

- Requests (**Basic profile**):
  - GetCapabilities
  - DescribeFeatureType
  - GetFeature

- OutPutFormat: **GML**

12 November 2011
OGC Services covered by GeoShield

Sensor Observation Service 1.0.0:
Standard protocol allowing requests for retrieving sensor observation data

• Permissions definition:
  – Excluding / Including Offerings

• Requests (Basic profile):
  – GetCapabilities
  – GetObservation
  – DescribeSensor

• Response format:
  – text/xml; subtype='sensorML/1.0.0'

12 November 2011
The Sensor Observation Service protection

- This is the latest part of GeoShield improvement

- Handle the basic implementation (core profile)

- Permissions are based on the `sos:ObservationOffering` grouping of the `sos:Capabilities` document, GeoShield can exclude the access to:
  - Features
  - Procedures
  - ObservedProperties

- **Caching permissions in memory** for better performance
<sos:Capabilities>
  [...] 
  <sos:Contents>
    <sos:ObservationOfferingList>
      <sos:ObservationOffering gml:id="aaaa">
        <gml:name>urn:x-ist::offering:aaaa</gml:name>
        <gml:boundedBy>[
        [...]</gml:boundedBy>
        <sos:eventTime>[
        [...]</sos:eventTime>
        <sos:procedure xlink:href="B_TRE"/>
        <sos:procedure xlink:href="H_TRE"/>
        <sos:procedure xlink:href="P_TRE"/>
        <sos:procedure xlink:href="T_TRE"/>
        <sos:observedProperty xlink:href="urn:ogc:def:property:x-ist::meteo:air:humidity"/>
        <sos:observedProperty xlink:href="urn:ogc:def:property:x-ist::meteo:air:pressure"/>
        <sos:observedProperty xlink:href="urn:ogc:def:property:x-ist::meteo:air:radiation"/>
        <sos:observedProperty xlink:href="urn:ogc:def:property:x-ist::meteo:air:rainfall"/>
      </sos:ObservationOffering>
      <sos:ObservationOffering gml:id="bbbb">
        [...] 
      </sos:ObservationOffering>
    </sos:ObservationOfferingList>
  </sos:Contents>
</sos:Capabilities>
GeoShield’s Sensor Observation Service protection strategy

**ObservationOffering 1:**
- Sensor 1
- Sensor 2

**ObservationOffering 2:**
- Sensor 3
- **Sensor 4 (private)**
- Sensor 5

**ObservationOffering 3:**
- Sensor 1
- Sensor 2
- Sensor 5
- Sensor 6
GeoServer Resource Access Manager plug-in

- This year, GeoServer 2.1 version has introduced support for data filtering with an improved security framework:
  - The main feature is the availability to extend the internal Resource Access Manager with a plug-in

- Benefits:
  - **No more limited permission** (yes/no definition) for each layer
  - Extended capabilities to implement **granular data access rules**
    - Filters based on geographical functions (BBOX, INTERSECTC…)
    - Filters based on attributes
    - Include / Exclude filters
    - Workspace permissions
  - Integration with **external users database**
  - **More reliable and stronger protection** at data abstraction level

12 November 2011
Access rule application process

1. GetMap
2. Authentication
3. Authorization object
4. User is authorized?
5. Error 401 - Unauthorized
5. Caching
6. Get Access Rule
7. Rule Object
8. Apply rule / Caching rule
9. Map

User: foo.bar
Password: xxxxxxx

GeoServer
GeoShield
Benchmarking WMS GetMap

- Tests are going to be run using JMeter on my Workstation:
  - Ubuntu 10.04, Intel Core Duo 2.4 GHz E4600, 4Gb RAM
- Using a progression of 1, 2, 4, 8, 16 and 32 threads, each thread group doing 100, 200, 200, 400, 400, 800 requests respectively
- Layer: topp:tasmania_water_bodies

<table>
<thead>
<tr>
<th>threads/requests</th>
<th>1/100</th>
<th>2/200</th>
<th>4/200</th>
<th>8/400</th>
<th>16/400</th>
</tr>
</thead>
<tbody>
<tr>
<td>GeoServer*</td>
<td>79</td>
<td>71</td>
<td>79</td>
<td>102</td>
<td>316</td>
</tr>
<tr>
<td>GeoShield (PROXY)</td>
<td>291</td>
<td>315</td>
<td>653</td>
<td>3346</td>
<td>7837</td>
</tr>
<tr>
<td>GeoServer (PLUGIN)</td>
<td>134</td>
<td>151</td>
<td>190</td>
<td>332</td>
<td>1320</td>
</tr>
</tbody>
</table>

* without authentication
Installing the plug-in

When GeoServer and GeoShield are installed, adding the Resource Access Manager plug-in is quite simple:

1. Copy the `geoshield-1.0.jar` file into the GeoServer’s WEB-INF/lib directory

2. Modify the web.xml file adding a Filter definition

3. Create the `GEOSHIELD_USER`

4. Configure the permissions on GeoShield
GeoServer Resource Access Manager plug-in

Demo
Next improvements

- Extending security:
  - Web Processing Service
  - Web Applications

- Web administration interface
  - Integration with GeoServer Web Interface
  - OpenLayers integration (Real Time Permission definition and test)

- Release of the GeoShield stable version 1.0 (end of 2011)
  - Code refactoring
  - Better performance
Thank you

Institute of Earth science
http://www.ist.supsi.ch

GeoShield project
http://sites.google.com/site/geoshieldproject

Milan P. Antonovic, Institute of Earth science - SUPSI
Massimiliano Cannata, Institute of Earth science - SUPSI

12 November 2011