Geophysical Research Abstracts
Vol. 13, EGU2011-7579, 2011
EGU General Assembly 2011

Building a Web Based Environment for the Intercomparison of Distributed Environmental Science Data: Challenges in Access Control and Security

Philip Kershaw (1), Jon Blower (2), Alistair Gemmell (2), Stephen Pascoe (1), and Ag Stephens (1)

(1) STFC Rutherford Appleton Laboratory, NCAS/British Atmospheric Data Centre, Didcot, United Kingdom (philip.kershaw@stfc.ac.uk), (2) Reading e-Science Centre, Environmental Systems Science Centre, University of Reading, United Kingdom

MashMyData is a NERC (Natural Environment Research Council) funded Technology Proof of Concept project whose aim is to enable environmental scientists to combine and overlay geospatial data quickly and easily in the context of a web style mash-up. Users can upload their own data and compare it with data pulled from other sources via services hosted over web based data access protocols such as OPeNDAP and the OGC (Open Geospatial Consortium) W*S standards.

However, such a model is complicated when we consider these services each with a system of authentication/authorisation in place to restrict access to the data they serve. MashMyData seeks to address this scenario within its remit and considers a use case where multiple services are invoked to perform some function on behalf of the user, thus introducing the classical problem of user delegation and how best to communicate user identity and access rights between services potentially in independent domains. The Grid provides the tried and tested solution of RFC3820 Proxy certificates but other technologies such as OAuth provide attractive alternatives.

This project leverages work carried out by the Centre for Environmental Data Archival (CEDA, the host organisation for the BADC) for the NERC DataGrid Security system and the Earth System Grid Federation, a software infrastructure developed as part of an international collaboration effort to support access to the climate model data generated for the CMIP5 (Coupled Model Intercomparison Project, Phase 5). A significant contribution for the purposes of this project has been the extension of OPeNDAP services and the NetCDF C and Java APIs to support SSL based authentication over a HTTP/HTTPS interface. The ESGF access control architecture in fact supports authentication/single sign on with OpenID and alternatively, with PKI based credentials via the credential management service MyProxy from the Globus toolkit. Attribute management and authorisation interfaces are implemented using SAML (Security Assertion Mark-up Language).

We explore alternative OAuth and Proxy certificate based solutions to the delegation question and how it is possible to extend the ESGF access control architecture to support these in a simple workflow scenario: a Portal application developed by and deployed at Reading e-Science Centre accesses data services at CEDA. It invokes a processing job using CEDA's OGC Web Processing Service implementation and an OPeNDAP service based on the Python implementation, PyDAP. The security infrastructure is provided by Python based web services and middleware, part of the NDG (NERC DataGrid) Security system which includes a SAML implementation ndg_saml and ndg_xacml, an implementation of the access control policy language XACML (eXtensible Access Control Markup Language).

We look at the challenges in matching up differing security protocols and specifications to reach a solution in what from the security perspective is a mash-up in its own right.