

Spatial Data Infrastructures and Security

- Brad Spencer, CubeWerx Australia

Background

Providing controlled and highly secure access to web deployed geospatial data has been a priority since before September 11, 2001, but even more so today. This is because geographically depicting data adds another dimension of intelligence and context making it richer and more valuable. Add to this the rapid uptake of publishing of data on the Internet and it becomes clear that data holdings are in jeopardy of misuse. Consequently, controlling access to data content on local and remote data servers has now become a critical need for government agencies, businesses and military services worldwide.

The Service Oriented Architecture (SOA) emerging from the work of the Open Geospatial Consortium (OGC®) is strongly influencing the deployment of Spatial Data Infrastructures (SDI) being implemented around the world. These projects have matured to a point that their broader acceptance or even very existence is now dependent on their capacity to secure these data resources. So, many organisations active in the development of SDIs are now reviewing how they can put in place a common security framework that can control access to these resources. This trend is equally if not more relevant to commercial data providers who wish to deploy their services with all the benefits of a Service Oriented Architecture.

CubeWerx, in partnership with other innovative organizations, have invested and contributed to providing solutions directed at resolving this important security challenge. Offering solutions in this area implies deploying mechanisms for identity/authentication, access control including managing roles of participants in such a way that each jurisdiction/data publisher maintains complete autonomy of its published web-enabled data resource. As a result of these initiatives CubeWerx has developed an innovative SCOTS product called CubeWerx Identity Management Server (IMS).

CubeWerx Identity Management Server

CubeWerx® Identity Management Server (IMS) provides a mechanism for data administrators to centrally control user access through a 'policy' server that grants authorization rights to each web resource. IMS is designed for deployment in a distributed federation of jurisdictions providing security for all resources within that federation. Implemented as a web server extension, this product offers a distributed access control framework that facilitates secure sharing of web resources inside and outside each

CubeWerx®

jurisdiction. This includes any static or computational resources available through a web server using HTTPS.

A web resource can be:

- web page,
- document,
- CGI/ ASP program,
- servlet,
- portlet,
- OGC® web service,
- database query,
- file upload/download,
- generated image,
- etc.

Built on simple identity concepts, this product innovates by allowing jurisdictions to establish a single web-enabled, collaborative, security framework for sharing all their secure and non-secure web resources with users inside and outside their organizations. This product enhances standard web server products by implementing a secure distributed framework for supporting the following functions

- Authentication
- Single Sign-on
- Access Control

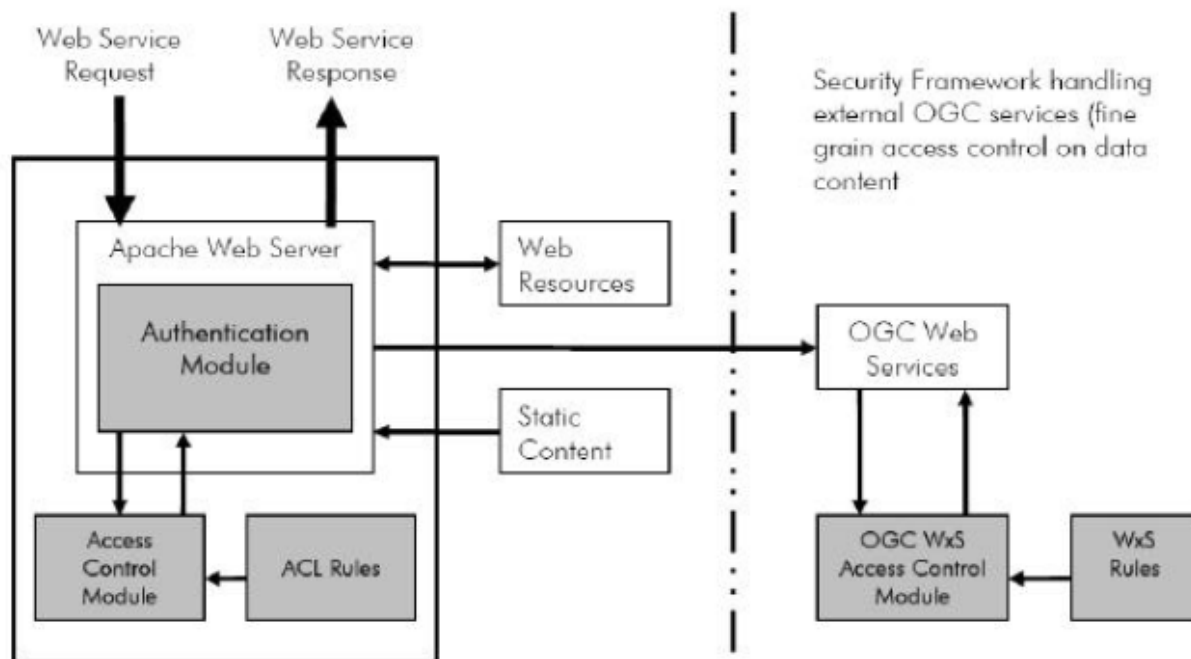
CubeWerx IMS is essentially a framework that manages identities and enforces role-based access control rules on web resources. Rather than dictating policies, its goal is to support policy rules already available in most organizations and provide secure, flexible, extensible, and highly available components for supporting Access Control Rules (ACL). These components are themselves invoked as web services allowing each trusted organization in a federation to determine its own authentication and access control policies.

CubeWerx IMS supports access control at the web server level through a standard Secure Socket layer (SSL) operated web server (HTTPS). Fine grain access control to data content is also available for OGC® web services allowing controls over OGC® operations, data layers and geographic areas or specified extents. CubeWerx WMS/WFS products have also been extended to facilitate this rule-based fine grain access control capability. In addition, with CubeSERV® Cascading WMS, the CubeWerx IMS product can be used to control access to WMS data content from other remote or distributed WMS services (OGC compliant).

CubeWerx IMS Architecture

IMS is based on the widely used, open source Apache web server. Apache supports the extension of its own functionality through the use of pluggable modules. IMS is implemented as an Apache module with an accompanying suite of CGI programs and GUI tools. Very much like it is configured for Apache's standard authentication module, Apache may be configured to 'IMS wrap' specified regions of the server's URL space.

IMS is implicitly invoked when a service request arrives at the web server - whether a computational service is requested or static content is requested. These protected resources and other IMS configuration information is specified in the web server's configuration file. Apache recognizes requests for URLs covered by these access controls as IMS-controlled service requests and directs them to IMS for handling.



Authentication

The IMS authentication service provides a framework for authenticating users within jurisdictions and validating that authentication when a user makes subsequent service requests. A user needs to go through the authentication procedure only once before being able to access services at any jurisdiction, subject to individual/group access controls.

To authenticate a user at a jurisdiction, IMS calls on web services that are most likely already in place and provided by that jurisdiction. For example, if LDAP is being used at a jurisdiction for authentication it can continue to be used within an IMS environment. IMS simply defines the protocols by which jurisdictions are asked to authenticate their own users on behalf of IMS. But IMS authentication can also be used if no other authentication mechanism exists.

IMS currently supports three styles of authentication:

- Simple authentication - This style is characterized by providing all of the information-necessary to authenticate a user in a single operation with a fixed set of arguments. This corresponds to the common username and password form of authentication.
- Certificate-based authentication - This style is characterized by the user providing an X.509 certificate through an SSL connection.
- Prompted authentication - This style is characterized by conversational prompting, where the prompts are determined at authentication time. Authentication using Plug-gable Authentication Modules (PAM) fits into this category.

Elements of these three styles may be combined; e.g., both a valid certificate and a user-name and password might be required for authentication. IMS is typically used in a web-oriented context using HTTP and other web-based communication protocols. Every jurisdiction within the federation runs an IMS application that extend the capability of their web server. Each and every web service request is first re-directed to the IMS at the jurisdiction providing the authentication service.

After successful authentication, a user is provided with a cryptographically-protected credential. Encrypted credentials are difficult to forge or tamper with and will accompany any subsequent service request to any jurisdiction of a Federation. Any IMS server within the federation that receives a request is able to decipher and validate any accompanying credential and proceed to examine the access control for the request. Thus providing a single-sign on capability within the federation for authenticated users.

Credentials must be kept private to IMS and its trusted components and agents since the credentials confer the federation-wide identity of the user making a service request. Therefore, all communication takes place over a secure SSL connection, making it difficult for credentials to be captured and replayed by an attacker. In the typical case where a web browser is the user agent, the credentials are returned to the user's browser within an HTTP cookie.

If IMS grants access, the web server will carry out the service request (services to the right in Fig 1) as it would any request. If IMS denies access, the outcome will be authoritative and Apache will refuse to perform the request, returning a standard 403 status code.

Service Level Access Control

One of the main functions of IMS is to manage access control for web resources. Access control for a jurisdiction is handled by Access Control Lists, or ACLs, stored on the web server. When IMS receives a request for a web resource under its control, it consults a subsystem called the Access Control Service (ACS). The Access Control Service consults a set of rules to determine whether the request will be permitted. These rules are expressed in an XML syntax, and securely stored and managed on the web server. Any request routed through IMS is accompanied by a set of credentials which allow ACS to determine the identity of the requestor, and make the appropriate decision according to the ACL rule set.

An ACL rule consists of three basic components:

- **What:** the what of a rule refers to a Service. There may be more than one service on URL contained in each rule.
- **Who:** the who corresponds to a User List, which may contain a set of users, an IMS-group, a role, or a combination of these.
- **How:** the how, is defined by additional options, such as constraints on CGI parameters, whether to pass credentials to cascaded web services, etc.

IMS supports Access Control definitions at a Role or Group level. Groups are convenient shorthand for a jurisdiction's administrator to use when specifying access control rules for types of users or members of a group. Rather than explicitly listing the set of users who have certain access rights to a service, an administrator can reference a group name that



represents all the membership in a set. The set's membership is built dynamically and consists of any combination of users and other group names. A group's membership is determined solely by the administrator of the jurisdiction that defines it, unless membership is delegated to other jurisdictions.

Fine Grain Access Control

If the user is using IMS in conjunction with the CubeWerx OGC compatible map server, CubeSERV WMS/WFS, they may create more complex, application specific access control rules with the CubeSERV Access Control Rules editor. CubeSERV WMS/WFS products have been extended to support fine-grain access control (see Fig 1) to OGC® resources as can any other WMS/WFS server.

Fine-grain access control may include limiting or allowing access to user defined:

- Specific geographic regions or AOIs – the user can specify the vertices of any number of included or excluded polygonal areas in any supported Coordinate Reference System(CRS).
- Map layers – the user can specify any included or excluded data layers.
- Execution of specific OGC operations – the user can include or exclude any of the supported OGC operations such as GetMap, PutStyles, etc.
- Any combination of these.

It is proposed that in the near future fine grain access control will also support attribute filters and SLD usage. This means even greater levels of management granularity such as limiting access to specified feature types and/or controls over the portrayal rules that control the symbology and scale rules for geographic features.

Standards & Interoperability

CubeWerx follows the OGC Services Framework methodology (Service Oriented Architecture) for the development of the IMS software product using services and content protocol concepts that have been developed and tested in previous OGC test beds and specification initiatives. These services and content protocols play a supporting role to CubeWerx' ability to deliver OGC-based technologies that will dramatically extend the outreach of the SDIs.

CubeWerx mandate is to develop geospatial warehousing and web service products based on open specifications in support of an emerging SDI market. CubeWerx has an existing track record in participating in many service interoperability initiatives including CGDI and OGC®. CubeWerx has participated into the development of CGDI architecture specifications under the GeoConnections Technical Advisory Panel (TAP) working group and has participated in almost all OGC® test beds and pilot projects since 1998.

CubeWerx is contributing to current consensus building activities on security framework while developing a commercial product. In addition to OGC® activities, CubeWerx will participate in other open and interoperable Web security standardization efforts such as Liberty Alliance (<http://projectliberty.org>) and OASIS SAML (<http://www.oasisopen.org/specs/index.php#samlv1.1>).



Conclusion

It is clear that many organisations around the world are very focused on the issue of securing geo services for reasons that vary from the need to limit malicious use through to the protection of commercial Intellectual Property (IP). CubeWerx participated in several initiatives in this regard and has proven that a pragmatic lightweight approach to developing a product (CubeWerx IMS) that can be deployed as a common security framework which SDI custodians can easily implement is entirely feasible.

With CubeWerx® IMS product installed at each jurisdiction within a federated community, any member of that federation can be authenticated once and collaborate with all nodes making computer to computer cascading secure, transparent and operationally practical. In addition, fine grain access controls provide an even greater level of security allowing jurisdictions to define how authenticated users or groups of users can use their data resources. A user or group of user's access can be limited to specific layers and even areas within these layers thus enabling the data editor to provide data on a need-to-know basis.

The benefits of such technology will vary according to each organisation's circumstances, the nature of the data/services, the need to protect IP and many more. However, it is clear that by using CubeWerx IMS organisations can now publish data in an open SDI environment with a high degree of security. This advancement should have profound impact in the further development of regional and national SDIs and ultimately the Global SDI.



CubeWerx

CubeWerx®

15 Rue Gamelin, Suite 506
Gatineau, Quebec J8Y 6N5
Canada

North American sales
sales@cubewerx.com
Telephone: (819) 771-8303
Facsimile: (819) 771-8388

Australia and New Zealand sales
CubeWerx Australia Pty Ltd
Brad Spencer, General Manager
ABN: 37 115 163 285
Mob: +61 (0)404 841 131
Tel/Fax: +61 (0)2 9481 7024
brad.spencer@cubewerx.com.au
www.cubewerx.com.au