Technical Report 2010

Improving GeoServer Security

Ing. Andrea Aime

Ing. Simone Giannecchini

GeoSolutions S.A.S.

20/12/2010

Version 01.00

Contents

GeoSolutions S.A.S

Via Poggio Alle Viti 1187
55054 Massarosa (LU) Italy
Tel: +390584962313 Fax: +390584962313
http://www.geo-solutions.it
info@geo-solutions.it

No table of figures entries found.

GeoSolutions S.A.S
Via Poggio Alle Viti 1187
55054 Massarosa (LU) Italy
Tel: +390584962313 Fax: +390584962313
http://www.geo-solutions.it
info@geo-solutions.it

Record of Changes

GeoSolutions S.A.S
Via Poggio Alle Viti 1187
55054 Massarosa (LU) Italy
Tel: +390584962313 Fax: +390584962313
http://www.geo-solutions.it
info@geo-solutions.it

Securing GeoServer

Introduction

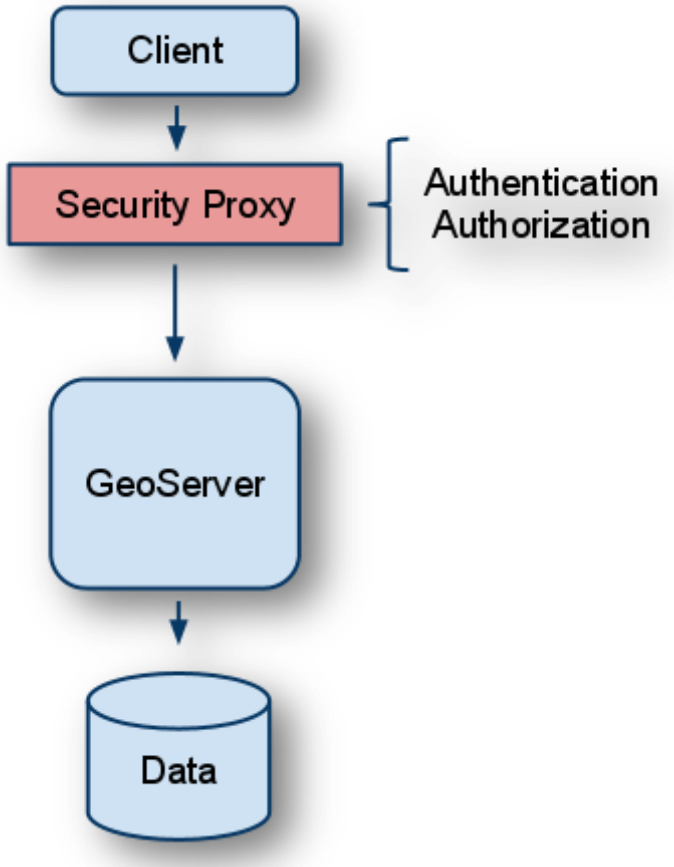
This document describes how GeoSever security can be improved to include:

- feature filters (to limit features by area or other attribute value)
- attribute selection (to hide restricted attributes)
- service limits (for example, to allow some users to request bigger/smaller images)
- mix data filters with service filters (allow some field to be visible on GetMap but not on GetFeatureInfo)

GeoSolutions S.A.S
Via Poggio Alle Viti 1187
55054 Massarosa (LU) Italy
Tel: +390584962313 Fax: +390584962313
http://www.geo-solutions.it
info@geo-solutions.it

The external proxy model

The security proxy model applies security by using a specialized HTTP proxy that received the requests, authenticates them and authorizes them.



The advantages of this model are:

- The proxy can be written in whatever language and libraries the developer feel comfortable with
- Given the same service this model can secure different implementations, provided no vendor options are needed or used
- The security is applied in a single point

GeoSolutions S.A.S
Via Poggio Alle Viti 1187
55054 Massarosa (LU) Italy
Tel: +390584962313 Fax: +390584962313
http://www.geo-solutions.it
info@geo-solutions.it

The disadvantages of this models are:

1. in order to secure the requests the proxy has to be able to parse all the requests that need to be secured, in all the syntaxes the can be expressed (often the same request can be expressed in two or more ways for a given OGC protocol and given version)
2. in order to apply data security the proxy needs to be able to add filters to the request, or to load the results and filter them in place. In some cases neither of them is viable or possible.

The disadvantages of this model are quite serious, especially if one plans to fully wrap a server as feature rich as GeoServer.

The number of protocols and protocol versions is constantly increasing. In the last few months alone we have seen the addition of WPS 1.0 and the "Simple Feature Service", and work is underway to add WMS 1.3, the next months may see the appearance of a WFS 2.0 implementation, a WCS 2.0 implementation and more REST oriented services.

An apparently simple request like WMS GetMap can be actually specified in a number of ways for what is related to styles:

- the style can be expressed as the name of a built-in style
- the style can be retrieved from a remote URL
- the style can be provided as XML along with the request both as GET or as POST

A GetMap request can also gather data dynamically from a remote WFS server (feature portrayal mode).

A WFS GetFeature request can also be expressed in four ways:

- WFS 1.0 GET request
- WFS 1.1 GET request (whose axis order in bbox is normally flipped, but in order to make sure one has to parse the 5 element bbox parameter, x1,y1,x2,y2,srs)
- WFS 1.0 POST request (using WFS 1.0 and GML 2 schemas)
- WFS 1.1 POST request (using WFS 1.1 and GML 3 schemas, and with the same axis order issues as the GET case)

GeoSolutions S.A.S
Via Poggio Alle Viti 1187
55054 Massarosa (LU) Italy
Tel: +390584962313 Fax: +390584962313
http://www.geo-solutions.it
info@geo-solutions.it

The proxy also needs to be able to perform sophisticated **filter manipulation**, again, in some cases this is simply not possible. As an example, GetMap requests do not normally support filters. In the case of GeoSever a ECQL filter can be added to the request, but at this point a vendor extension is being used, negating one of the advantages of this approach.

Even in the WFS case it's not normally possible to mix a FeatureId filter, expressed either as a KVP parameter or a OGC Filter in the GetFeature XML, with further filters.

Again, this is actually possible to do only in GeoServer using ECQL (both in this case and in the above one CQL is not capable enough for the job as it cannot encode all filters that can be expressed in the OGC syntax).

In the case of hiding GetFeatureInfo attributes the proxy is almost powerless, there is no supported way to hide attributes in such operation and the return formats, HTML and text, are pretty much opaque in terms of where the various attribute values are located.

Trying to replace the GetFeatureInfo request with a GetFeature is going to fail a functionality check, since the GetFeatureInfo is normally styling aware and knows all about the size of the symbolizers and what features are visible at each zoom level.

Another problematic topic is vendor extensions, in general the proxy has to understand them or disallow them, as some might have unforeseen effects on what data can be actually accessed.

Long story short, this model seems **unadvisable unless the following conditions are met**:

- the set of services, service versions, type of requests (GET/POST/SOAP) is known in advance and is small
- the set of vendor options needed from the server is either empty, or known and small
- all of the security required can be performed by simply altering the requests
- the development team agrees to rewrite all of the parsing code that the server already provides on its own

GeoSolutions S.A.S
Via Poggio Alle Viti 1187
55054 Massarosa (LU) Italy
Tel: +390584962313 Fax: +390584962313
http://www.geo-solutions.it
info@geo-solutions.it

The internal proxy model

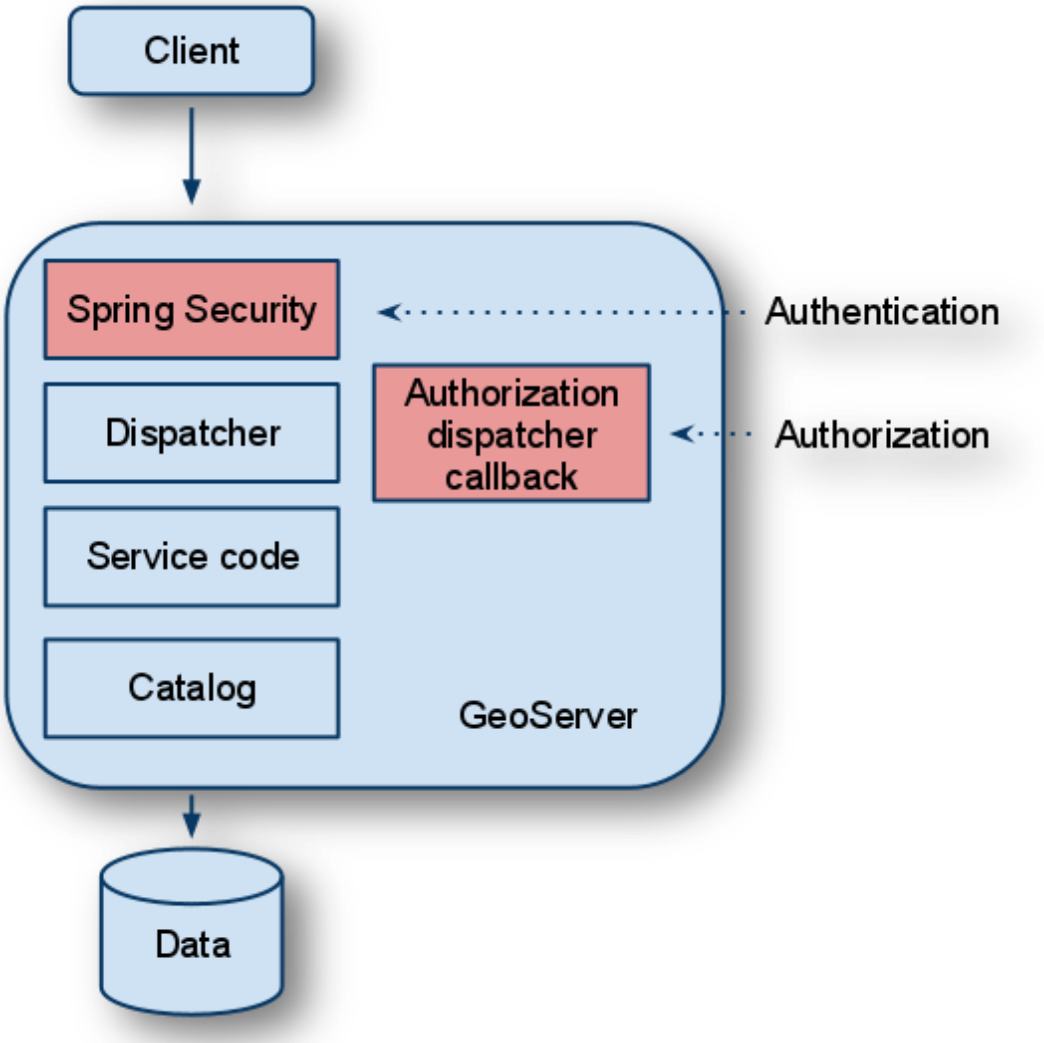
In the internal proxy model the security is handled at two levels:

- the authentication is performed by the standard Spring Security filters (be it HTTP BASIC, DIGEST, CAS, OpenID of whatever else)
- the authorization is performed by a GeoServer Dispatcher callback

A **Dispatcher callback** is a GeoServer extension point that can be registered inside the Spring context and that can listen to the evolution all the incoming requests, starting from the request arrival, parsing, execution and results construction.

The callback can thus get the request in its parsed form and can deny it or modify it as it sees fit.

GeoSolutions S.A.S
Via Poggio Alle Viti 1187
55054 Massarosa (LU) Italy
Tel: +390584962313 Fax: +390584962313
http://www.geo-solutions.it
info@geo-solutions.it



Advantages:

- it leverage the server internal parsers to avoid having to understand different syntax for the same request, only deals with the object model resulting from the parse instead
- has full access to the whole request, including vendor options
- security is delegate to Spring Security, no need to reinvent the wheel

GeoSolutions S.A.S
Via Poggio Alle Viti 1187
55054 Massarosa (LU) Italy
Tel: +390584962313 Fax: +390584962313
http://www.geo-solutions.it
info@geo-solutions.it

Disadvantages:

- it is GeoServer specific
- while it gets rid of GET/POST differences and other syntactic differences it still has to understand all of the services and all of their versions (though some versions are close enough that GeoServer uses the same object model for both).

Unlike the proxy model eventual security filters can be expressed using the GeoTools object model which can represent all possible filter combinations.

However, just like the proxy model, this approach cannot impose restrictions that cannot be expressed as a manipulation of the request or response object models.

If we consider the case of WMS GetFeatureInfo by working internally the callback can intercept the FeatureCollection that is going to be encoded and slice away certain attributes, effectively allowing to hide them.

However the same cannot be effectively done for WPS processes that take the data source name instead of using a WFS request (this is not a recommended approach, but unfortunately a possible one).

Another problematic point is filter functions, just like processes they are open ended and one can build a filter function that performs data access (for example, to overcome the lack of joins in GeoServer WFS), the security wrappers would have to recognize its presence and wrap it some way to enforce the data access security policies.

It is also to be observed that all data access manipulations are using service specific means, meaning they have to be coded separately for each service.

GeoSolutions S.A.S
Via Poggio Alle Viti 1187
55054 Massarosa (LU) Italy
Tel: +390584962313 Fax: +390584962313
http://www.geo-solutions.it
info@geo-solutions.it

Also, the Dispatcher works against OGC services only, so this approach cannot be used to secure REST services (the REST code paths have a dispatcher too, but at the time or writing, no callback extension points).

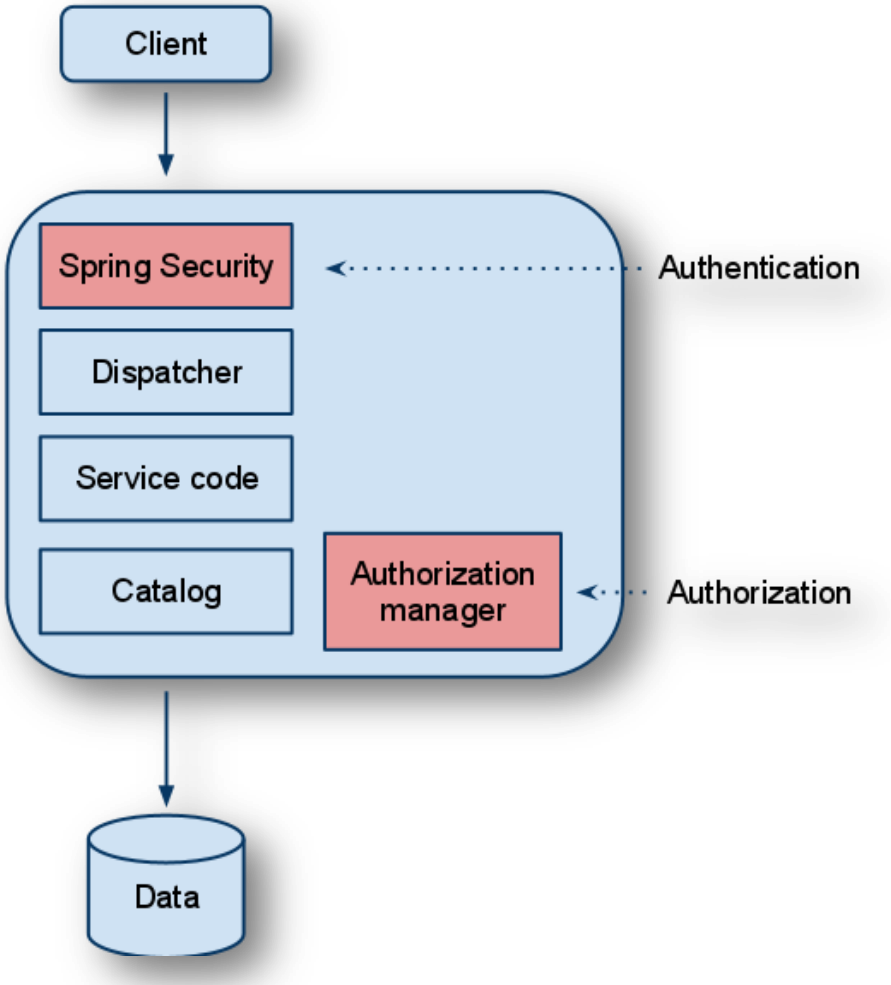
Finally, in order for mixed layer/service authorization rules to be applied the callback has to deal with each protocol different way to access data and consider the fact that many requests can access multiple data sources at the same time (GetMap is typical, GetFeature can do that as well).

GeoSolutions S.A.S
Via Poggio Alle Viti 1187
55054 Massarosa (LU) Italy
Tel: +390584962313 Fax: +390584962313
http://www.geo-solutions.it
info@geo-solutions.it

The catalog security model

In the internal proxy model the security is handled at two levels:

- the authentication is performed by the standard Spring Security filters (be it HTTP BASIC, DIGEST, CAS, OpenID of whatever else)
- the authorization is performed by the SecureCatalogImpl, which in turn calls onto the AuthenticationManager, a pluggable extension point allowing to write custom security implementations



GeoSolutions S.A.S
Via Poggio Alle Viti 1187
55054 Massarosa (LU) Italy
Tel: +390584962313 Fax: +390584962313
http://www.geo-solutions.it
info@geo-solutions.it

Advantages:

- at the catalog level the data requests are simple and uniform, just one layer at a time
- the data security can be applied no matter what service was used to reach to it, the implementation is thus time proof

Disadvantages:

- the security engages only on catalog level data access, some services, like WPS, can work by using only remote resources, and thus cannot be secured with this approach
- the current AuthorizationManager is not sophisticated enough, while the current request can be accessed via the Dispatcher.REQUEST thread local it is not possible to apply filtering and attribute selection (thus it requires core modifications to GeoServer).

While this approach is general, efficient and solid it cannot be used alone as soon as there are services that can work without accessing the catalog at all (WPS, WMS in feature portrayal mode, or just using user layers that carry the data definitions in GML).

Also some aspects of security, such as maximum request size and the like, cannot be effectively handled here: in general, any security action that requires to modify the request beyond the data access filters cannot be implemented using this model.

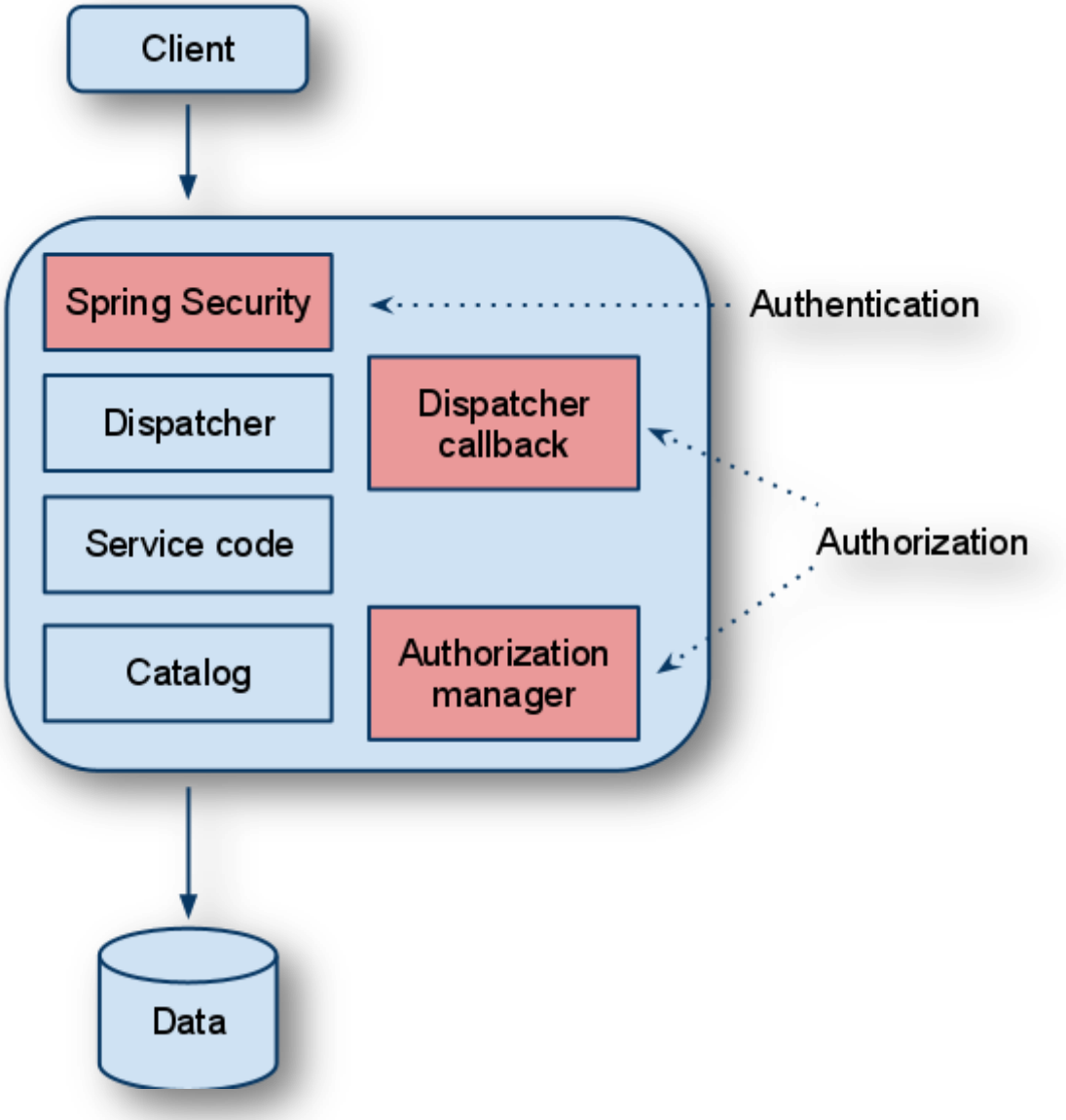
The integrated security model

The integrated model tries to address the shortcomings of the dispatcher and catalog mode by having each one of them play a role in the operations best suited to its location in the stack:

- the authentication is performed by the standard Spring Security filters (be it HTTP BASIC, DIGEST, CAS, OpenID of whatever else)
- a first level of authorization is performed at the Dispatcher callback level, in particular, at this level is performed anything that has nothing to do with data access (such as disallowing certain protocols/version) and that may require the request manipulation, throttling and the like

GeoSolutions S.A.S
Via Poggio Alle Viti 1187
55054 Massarosa (LU) Italy
Tel: +390584962313 Fax: +390584962313
http://www.geo-solutions.it
info@geo-solutions.it

- a second level of authorization is performed by the SecureCatalogImpl, which in turn calls onto the AuthenticationManager, in particular, anything that has to do with data access manipulation, either stand alone or in combination with knowledge about the specific request



GeoSolutions S.A.S
Via Poggio Alle Viti 1187
55054 Massarosa (LU) Italy
Tel: +390584962313 Fax: +390584962313
http://www.geo-solutions.it
info@geo-solutions.it

Advantages:

- uses each possible security location for what it's best suited for
- it's a natural evolution of the current "security sandwich" model, integrating the two layers and allowing for more powerful security enforcement

Disadvantages:

- GeoServer specific
- deals with security in three different place
- requires modifications to GeoServer core as noted in the "catalog security" model section

GeoSolutions S.A.S
Via Poggio Alle Viti 1187
55054 Massarosa (LU) Italy
Tel: +390584962313 Fax: +390584962313
http://www.geo-solutions.it
info@geo-solutions.it