

Distributed Security Architectures - “Providing security services for Grids”

PI: Mary R. Thompson, LBNL

Researchers: Abdelilah Essiari, LBNL, Keith Beattie, LBNL

Summary

The overall goal of the Distributed Security Architectures project is to provide assured, policy-based access control for computer mediated resources such as data archives and instrument systems, that operate in wide area network environments; grid services such as network monitoring, file transfer and computing resources; and potentially fine-grained, object method level access control.

DOE scientific resources - instruments, data, and collaborations - that are accessed via open networks or as part of a DOE Grid must be protected against unauthorized use before any high value resources will be committed to such use.

The Distributed Security Architectures project is investigating and implementing practical solutions to the security needs of distributed systems based on the emerging *Public Key Infrastructure (PKI)* standards and implementations. An open source implementation of PKI technology was released by Netscape in 1994. Since then it has become the standard for secure Web traffic. It provides authentication, integrity and confidentiality of network communications. It has been used as the foundation of the Globus Security Infrastructure and has thus become the standard for secure Grid access as well.

PKI currently does not support authorization, although there is now the start of a *Policy Management Infrastructure (PMI)* which will address this area. Meanwhile, we have leveraged off PKI authentication to develop and distribute a modular authorization service, called Akenti, that compares a requestor’s authenticated PKI identity certificate with a set of signed policy documents describing the access policy for the requested resource. These policy documents are created and maintained by stakeholders for the resource, independent of the resource server platform. The policy is kept in signed documents which state the conditions of use for a resource,

based on attributes of the requestor and current values of system. These documents are written in XML (which provides self-descriptive tags for each item) in order to be readily understood by resource stakeholders. We provide both a command-line interface to sign an XML document and a menu driven GUI interface to create and sign them.

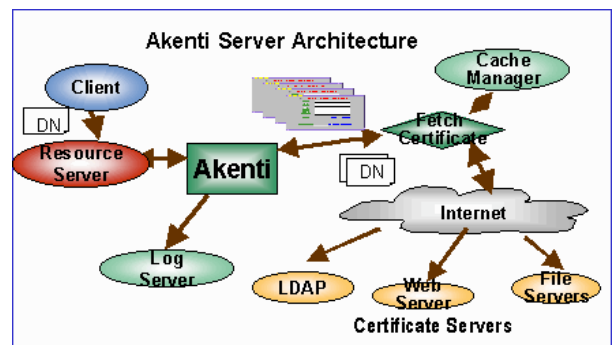


Figure 1. Akenti policy engine gathering and analyzing policy certificates to make an access decision.

The Akenti authorization server is written in C++ (with an additional C interface) and can either be linked into a resource gateway server or called as a standalone server with a simple message protocol built over TCP.

We also provide an Apache authorization module that works as part of an SSL-enabled Apache Web server and uses the Akenti engine to make authorization decisions. Thus in a collaborative or Grid environment that uses a Web server to access protected documents or to act as a Portal to community resources, Akenti can be used by both the

Web (Apache) and Grid (Globus) software to provide a uniform authorization system.

We have worked closely with the National Fusion Collaboratory to use the Akenti authorization server to protect resources on the Fusion Grid. The Fusion Grid provides remote access to fusion data repositories and to compute servers which provide access to one of the commonly used fusion analysis codes, TRANSP. Remote access to the TRANSP server has been enabled with the Globus remote job-submission tools.

We worked with Fusion Collaboratory members from Argonne National Laboratory to integrate the Globus job-manager with Akenti, in order to provide fine-grained job authorization. During a normal Globus job submission, the Globus gatekeeper process authenticates the requestor and then verifies that his Grid identity is in a local mapping file. If it is, the requestor is granted the equivalent of a user login to the machine. In practice that means that he can call the job-manager to execute any binary on the machine or to upload his own code to execute. The only constraints on his actions are those imposed by the local site administration on the local id that he is given. In practice this limits the files that can be read or written, and enforces a user privilege level, but places no real restrictions on what files can be executed.

In addition to starting new jobs, a Globus remote user can query, suspend or kill the jobs that he previously started.

The Fusion Grid required more constraints on what code was executed. In fact, they wanted to allow only the execution of the TRANSP code. On the other hand they wanted to expand the rights of some administrative users to be able to suspend or kill jobs started by people other than themselves.

We did a very early prototype integration with Akenti that only restricted the programs that could be executed. That was followed by a

second more extensive modification to the job-manager to control the choice of executables and the job resources that could be used. We are currently working on a cleaner integration that will control executables, resources and running jobs.

This next integration will be done with a carefully designed callout from the job-manager to an authorization plug-in module. We will provide a plug-in module that parses the security context information that it is handed and calls an Akenti authorization server. It is our intention that these pieces can be used by other SciDAC Grids to provide fine-grained job control. The Akenti plug-in module can be used as delivered or can act as a model to integrate other authorization schemes with the job-manager.

In the longer term, the same general model of clearly defined interfaces between access enforcement points and authorization servers will carry over to the Grid services frameworks. We are working with the Grid Services project to provide Akenti authorization as a Grid service. Included in that work is implementing some of the new security message protocols which will be used between clients and services.

We are also working with the Scalable Peer-to-peer Information Sharing project to provide Akenti authorization for file sharing. In this application authorization policy must not only control access to particular files, but authorize joining the communication groups as well. Thus, something more than traditional file access control lists is needed.

For more information contact :
Mary R. Thompson
Lawrence Berkeley National Laboratory
Phone: 510-486-7408
mrthompson@lbl.gov and visit
www.itg.lbl.gov/security/DistSecArch.html