

Motivation and Overview

U.S. CMS and U.S. ATLAS Privilege Project

<http://computing.fnal.gov/docs/products/voprivilege/>

Date: 2004-12-03, Last Updated 2005-01-14

Author: Markus Lorch, Anne Heavey

Contact Email: mlorch at vt dot edu

1. Introduction

US CMS and US ATLAS, based at Fermilab and Brookhaven National Lab respectively, are sponsoring the VO Privilege Project to develop and implement finer-grained authorization for access to grid-enabled resources and services in order to improve user account assignment and management at grid sites, and reduce the associated administrative overhead.

The project will increase overall authorization flexibility and usability by implementing a role-based access control mechanism in which a VO's authority defines which VOs a subject (user) may join and which roles a subject may assume. The subject must be given the power to select an appropriate VO-membership and role combination for a given service request to grid resources. The sites and resources will have adequate information to identify users and stop their activities as needed, without affecting other users.

The enforcement mechanisms developed will leverage existing security semantics of the underlying operating systems and the system will present itself as an incremental improvement over the widespread use of shared user accounts which offer little or no restrictions and protection. A primary goal is to overcome the limitations presented by static mapping of grid-subjects (users) to (possibly shared) local accounts.

2. Motivation

In existing grid security infrastructures, such as deployed in Grid03, grid resource access rights are granted on a very coarse level through UNIX operating system file access rights. VO group and role policies are not communicated to the grid resources. Sites therefore have no basis for differentiating between users from a given VO. Up until now, all users from a given VO have been mapped to a single, shared user account to reduce the administrative overhead of manually maintaining individual user accounts and simplify the sharing of (data) resources among members of a single VO. It follows that every access is granted with the full set of access privileges that the VO as a whole is authorized to assume, and user activities are not well insulated from each other. This many-to-one mapping provides limited support for the implementation and management

of fine-grained authorization policies and affords a relatively low degree of overall system security.

As more users, applications, resources, and services come on board, this level of security would become more and more hazard-prone with respect to resource security, data and job security, accountability, and efficiency. Finer-grained authorization is required. To achieve and maintain good service with the enhanced security, it's important to incorporate the policies of both the VO and the individual site when defining the details of the finer-grained system.

We want to empower the VOs to set varying policies for different user groups and roles in order to limit which tasks the users can perform and with what priorities, on an access-by-access basis. We want to empower users to choose an appropriate group/role combination according to the activity they plan to perform. We want to empower sites' computing and storage resources to intelligently enforce priorities and data access rights set at the VO level and to identify users and stop their activities as needed, while adhering to their site-specific security requirements.

3. Requirements

The US CMS and US ATLAS collaborations have identified the following requirements for the grid security infrastructure:

- Resource providers (sites) define fine-grained authorization policy based on VO groups and roles, and have mechanisms that can enforce these policies consistently over all the resources in their domain.
- Enforcement mechanisms must support existing applications and use cases.
- The access rights with which a specific access is granted are reduced and ideally represent a fair approximation of the least amount of privileges required for this access.
- Users can drive/customize the allocation of a subset of their access rights to a specific access (e.g. through the selection of their current "role").
- Users may be a member of multiple collaborations (VOs) and the system should support the separation-of-duties principle for these users.
- Users are to be separated from each other and an individual user's files must be protected against accidental or malicious modification by other users (including other members of the same collaboration).

3. System Implementation Overview

The VO Privilege Project software, depending on its implementation, relies on, interfaces to and further develops at least some of the following independent pieces of VO-implemented and site-implemented authorization software: [VOMS](#), [VOMRS](#), [Grid-map callout interface](#), [GUMS](#), and [SAZ](#). The project schema requires a number of

enhancements to and previously unused functionality of these products, for example that VOMS dynamically add attributes to a user's proxy certificate specifying the role under which the user is making a request to access grid resources, and that GUMS act as an identity mapping service to map users to local accounts. The Globus gatekeeper Grid-map callout interface allows for the replacement of the built-in Grid-map file mechanism with a component (called PRIMA module) that can extract and process presented role attributes and privilege assertions and query the GUMS identity mapping service. The interface between the PRIMA module and the GUMS identity mapping service is based on the OGSA SAML Authorization Interface, which is in the process of being standardized in the [OGSA-Authorization working group](#) of the [GGF](#).

3.1 Stage I

The first stage of VO Privilege development seeks to integrate VOMS, the Grid-map callout interface, and GUMS, and to develop the PRIMA software module to parse the Gridmap callouts and communicate with the GUMS identity mapping service. On or at a given grid resource, the integration of these elements is intended to:

- obviate the need to replicate static grid-map files.
- provide for the mapping of users to local user and group IDs based not only on their authenticated identity (distinguished name) but also on VO-membership and role attributes as presented to the grid service.
- provide dynamic assignment of local accounts to qualified users (based on their credentials) who have not yet been assigned their own account.

Stage one also includes integrating the doors into the dCache storage system to also utilize the identity mapping service.

3.2 Stage II

Stage two will implement finer-grained access control in which a given role is assumed to grant the user a set of rights, and the user is charged with selecting from this set, enabling only those rights he or she will need, following the least privilege access principle. Least privilege access is intended to prevent accidental overusage and limit the damage a malicious entity can cause when a user's credentials are compromised. Stage two will also implement dynamic execution environments, designed to enforce access rules via file system access control lists, network firewall rules, system quotas, and so on.

3.3 Functional Overview and System Architecture

Figure 1 below depicts a high-level overview of the privilege components. The authorization process using the privilege components is explained in the following paragraphs.

Authorization Architecture

FNAL Privilege Project

Version 3 - 2004-08-05
mlorch@fnal.gov

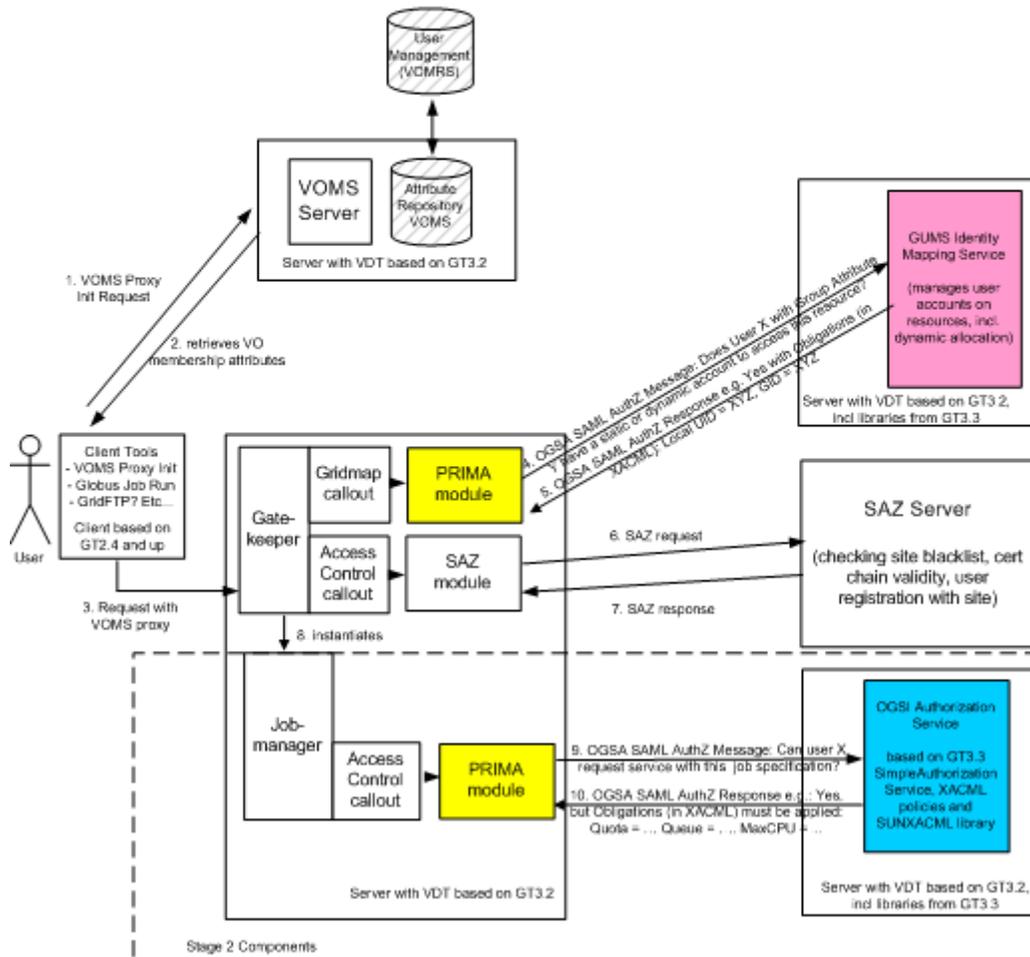


Figure 1 – Architectural Overview of the Privilege Components

Before a user can access a grid resource a short-lived credential (proxy) has to be created. When the privilege components are used one step is added to the generation of such a proxy credential: The user is asked to provide desired VO (and optionally role-related) information when requesting a proxy certificate. The used tool, voms-proxy-init, will contact a VOMS server to request a trusted attribute statement from VOMS that proofs to a relying party (e.g. the gatekeeper) that this user is entitled to be treated as a member of the requested VO and (optionally) may hold the requested roles. This information is then embedded in the proxy credential. If a user wishes to change roles, he or she must request a new proxy certificate using the appropriate arguments. The use of standard proxy

certificates without VOMS attributes will still be permitted but result in a default VO/role mapping.

The proxy certificate with the VOMS issued attributes embedded in the form of X.509 Attribute Certificates will be automatically supplied to the gatekeeper when the user requests a grid service. On the gatekeeper the Grid-map callout invokes the PRIMA module. PRIMA extracts the VOMS attribute certificates containing the VO and role information from the user's proxy certificate and checks these attribute certificates for validity. To be able to verify the validity of the attribute certificates the PRIMA module must be configured with the service certificates (public-key certificates) of all trusted VOMS servers. PRIMA then queries the site's identity mapping service (GUMS) authoritative for this resource. This query is realized via a https secured channel with a SOAP message containing a SAML Authorization Decision Query for an authorization decision. The GUMS service will respond with a SAML Authorization Decision Statement that, if appropriate, will permit the requested access and provide authorization obligations. The obligations will instruct the PRIMA module to grant the requested access with a specific local user id (and optional local group and supplemental group ids).

As a final step to user authorization site's may require the gatekeeper to also contact the Site Authorization Service (SAZ) which enforces the site-specific access control rules/policies such as specifying prohibited users, checking for revoked certificates, and validating the user's certificate path. The SAZ service developed at FNAL is currently relying on a proprietary protocol for communication. It is planned that future versions will implement the same SOAP/SAML protocol and authorization interface used in the PRIMA-GUMS communication.

4. Summary

The VO Privilege Project is developing and implementing finer-grained authorization for access to grid-enabled resources and services based on identity mapping, role-based access control and finer grained access control policies. Both the VO as well as the resource site are recognized as role and access control policy authorities. Stage I of the project encompasses centralized and role-based mapping of grid users identities to site-local user and group IDs as well as providing mechanisms for the management and dynamic assignment of local accounts. Stage II will implement finer-grained access control policies and leverage the existing security semantics of the underlying resource operating systems to a farther extend in an effort to further reduce the amount of unnecessary access rights a request is served toward the goal of least privilege access.