Design and Application of a Scalable Virtual Organization Privilege Management Environment

Grids enable uniform access to resources by implementing standard interfaces to resource gateways. In the Open Science Grid (OSG), privileges are granted on the basis of the user's membership to a Virtual Organization (VO). However, gateways control access privileges to resources, such as separation of common user-based job execution environments, using user's identity and attributes. Currently, access privileges are determined solely by the individual sites that own the resources based on verbal communication with VOs. While this guarantees full control on access rights to the sites, it introduces inconsistency of VO privileges throughout the Grid and hardly fits with the Grid paradigm of uniform access to resources. We have implemented the Scalable Virtual Organization Privilege Management Environment (SVOPME) to close this privilege management gap between VOs and sites. SVOPME automates the propagation of privilege policies by providing tools for VOs to codify and publish desired privileges and assist sites to provide the appropriate access policies. In this paper, we will first describe our experience in applying SVOPME to OSG VOs and sites. Next, we will review the XACML profile of SVOPME policy templates and the privilege propagating strategy and mechanism employed by SVOPME. At a site, SVOPME tools help analyze how access policies are defined for its resources for VO users. These policies are then compared with the ones published by the VO, so that sites and VOs can verify policy compliance. Upon request, SVOPME can generate directives for site administrators on how the local access policies can be amended to achieve such compliance. We will review how SVOPME tools crawl the grid site configurations and synthesize the equivalent site privilege policies that can be used to compare against those of VOs. Moreover, we will describe how to extend the site tools to support new resources and policies. Finally, we will present how SVOPME can be extended to manage other policies such as network and security.

Primary authors : WANG, Nanbor (Tech-X Corporation) ; GARZOGLIO, Gabriele (Fermi National Accelerator Laboratory)

Co-authors : ANANTHAN, Balamurali (Tech-X Corporation) ; TIMM, Steven (Fermi National Accelerator Laboratory)