
# Application Security

Jim Basney
OSG Security Team
security@opensciencegrid.org

OSG All Hands Meeting
Application Deployment Foundations Workshop
March 2009

# Virtual Organizations (VOs)

- A VO is a collection of people with a common research focus/goal (e.g., CMS physics analysis)
  - OSG sites provide resources to VOs
  - VOs are responsible for authenticating and authorizing their members
- Two options for computing on OSG:
  - Join an existing VO
  - Form a new VO

# Join an Existing VO

- Get a certificate
  - Your certificate identifies you to VOs and Sites
  - DOEGrids CA provides certificates to OSG members
    - I can help you get your certificate today
- Agree to the OSG and VO Acceptable Use Policies (AUPs)
- Register your certificate with the VO
  - Your VO membership grants you access to VO resources

# Form a New VO

- Write a Charter describing the purpose of your VO
- Write your VO Acceptable Use Policy
- Agree to the OSG Service Agreement
- Register a Support Center for handing trouble tickets
- Deploy a VO Membership Service (VOMS)
  - You will be responsible for managing VO membership
- Register your VO with OSG

Open Science Grid

# Certificates

- User certificate
  - Identifies a person
  - Obtained from a Certificate Authority
  - Typically valid for one year (and renewable)
  - Private key encrypted by a passphrase
- Proxy certificate
  - Short lived certificate created from a User certificate
  - Enables single sign-on and delegation
- VOMS certificate
  - A proxy certificate containing VO membership information from voms-proxy-init
- Service or Host certificate
  - Identifies a service or host
  - Obtained from a Certificate Authority
  - Typically valid for one year (and renewable)

# User Responsibilities

- Protect your private key (userkey.pem)
  - Do not share it
  - Choose a strong encryption passphrase
  - Do not make unnecessary copies
  - Store it only on local disks, accessible only by you
  - Protect any copies in web browsers with a “master password”
  - If compromised, immediately revoke your certificate
- Abide by OSG and VO policies
- Report known or suspected security breaches to security@opensciencegrid.org

# VO Rights Management

- VO members may be organized hierarchically into *groups*
- VO members may be assigned different *roles* (“admin”, “software”, “production”)
- VO groups and roles are indicated by *attributes* in VOMS proxies
- Use ‘voms-proxy-init –voms’ to select among authorized groups and roles
- GUMS (Grid User Management Service) maps VO members to local accounts

Open Science Grid

# Certificate Lifetimes

- Certificates will not be accepted past their validity times
- Renew your User/Server/Host certificates before they expire
- Choose proxy certificate lifetimes carefully
  - Proxy is often needed for duration of job's lifetime (including any queue wait time)
  - Proxy renewal services are available (Condor-G, MyProxy, …)

Open Science Grid

# Pilot Jobs

- A *pilot job* is a type of application that runs at a site and coordinates work submitted by multiple VO users
- A pilot job framework should:
  - Verify that work comes from authorized VO users
  - Integrate with site accounting and authorization mechanisms
  - Isolate user jobs from one another
- The *glexec* system provides identity switching for pilot jobs to meet these requirements

Open Science Grid

# Discussion

- What questions do you have about application security in OSG?
- Will you be joining an existing VO or forming a new VO?
- Will you be using a pilot job framework?
- Any other questions/comments?

Thanks!