Open Science Grid

Security Best Practices Preview

Jim Basney
OSG Security Team
security@opensciencegrid.org

OSG All Hands Meeting – March 2009

Open Science Grid

OSG Security Team

- Mine Altunay (FNAL)
  - OSG Security Officer
- Doug Olson (LBNL)
  - OSG Deputy Security Officer
- Jim Basney (NCSA)
  - OSG Security Policy Officer
- Ron Cudzewicz (FNAL)
- Igor Sfiligoi (FNAL)
- Anand Padmanabhan (NCSA)
- Aashish Sharma (NCSA)

AHM Security Sessions

- Monday:
  - Site Admin Track III: Security Best Practices (11-12:30, 1:30-3)
- Tuesday:
  - Application Deployment Foundations Workshop: Application Security (9:35-9:55)
  - Data Management Foundations Workshop: Data Security (11:30-11:50)
  - VO Managers and Security Contacts Workshop (4-5:30)

Site Admin Track III: Security Best Practices

- This will be a hands-on session
- You will learn:
  - How to respond to a security incident
  - How to ban a user DN from your site
  - How to track down jobs submitted by a DN
  - How to locate relevant log files
  - Basic forensics steps for incident response
- Will include an open discussion on security best practices used by sites

Open Science Grid

VO Managers and Security Contacts Workshop (Tuesday 4-5:30)

- We will discuss:
  - Our Security Philosophy
  - Our Security Architecture
  - Roles and Responsibilities
  - Incident Response Procedures

Security Best Practices: Quick Overview

- Report security incidents
- Keep CRLs up-to-date
- Keep synchronized with VO membership lists
- Protect against SSH attacks
- See also: https://twiki.grid.iu.edu/bin/view/Security/BestPractices

Security Best Practices

- In case of a security incident involving OSG resources:
  - Contact your local/home organization's incident response team
  - Contact OSG security team:
    - security@opensciencegrid.org
    - https://twiki.grid.iu.edu/bin/view/Security/IncidentDiscoveryReporting

Security Best Practices

- Keep your Certificate Revocation Lists up-to-date
  - Run fetch-crl via cron every 6 hours

Critical for limiting exposure to compromised credentials

Security Best Practices

- Keep your site's VO list updated
  - Check if GUMS is contacting the VOMS server periodically and the gums-host-cron service is enabled on the CE
  - If using edg-mkgridmap ensure that the edg-mkgridmap service is enabled

Critical for limiting exposure when VO members are removed

Security Best Practices

- Protect against SSH attacks
  - Protect SSH private keys with good passphrases
  - Use firewalls to restrict SSH access so that SSH connections are allowed only from trusted hosts
  - Promptly apply security updates from software vendors, including operating system kernel updates

Thanks!