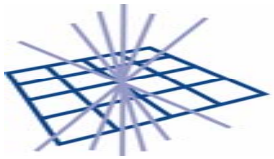

GridPP
UK Computing for Particle Physics

Update on LCG/EGEE Security Policy and Procedures

David Kelsey, CCLRC/RAL, UK
d.p.kelsey@rl.ac.uk

LCG GDB Meeting,
CERN, 22 June 2005

Information Society

Overview

Work of the Joint (LCG/EGEE) Security Policy Group

- **In collaboration with US Open Science Grid (OSG)**
- **JSPG meeting – CERN – 13/14 June 2005**

- User Acceptable Use Policy
  - Not yet in EDMS
- VO Security Policy (and AUP)
  - https://edms.cern.ch/document/ 573348/
- Incident Handling and Response Guide
  - https://edms.cern.ch/document/428035/

User AUP (Version: *The Taipei Accord 29 April 2005*)

USER AGREEMENT (accepted during registration with a VO)

1) **You may only perform work, or transmit or store data consistent with the activities and policies of the Virtual Organizations of which you are a member, and only on resources authorized for use by those Virtual Organizations.**

2) **You will not attempt to circumvent administrative or security controls on the use of resources. If you are informed that some aspect of your grid usage is creating a problem, you will adjust your usage and investigate ways to resolve the complaint.**

User AUP (2)

3) You will immediately report any suspected compromise of your grid credentials or suspected misuse of grid resources to incident reporting locations specified by the Virtual Organization(s) affected and credential issuing authorities as specified in their agreements and policy statements.
4) You are aware that resource providers have the right to regulate access as they deem necessary for either operational or security-related reasons and that your use of the Grid is also bound by the rules and policies of the organizations through which you obtain access, e. g. your home institute, your national network and/or your internet service provider(s).

User AUP – Discussion since 18 May

- **Sent to GDB and ROC Managers for comment**
- **Approved by OSG Council on 31 May 2005**
- **Comments received (mainly on bullet 4)**
  - What about resource provider policy?
  - What about Grid/Infrastructure policy?
  - Do we have the right to cut-off users?
    - Legal status of “Service” providers?
  - What about Data Protection laws?
  - Style: *I am/will* versus *You are/will*
- **Discussed issues at JSPG meeting 14 June**
  - Decided to consult some legal experts
  - Feedback received from one site and one network
  - Expecting another site feedback soon

AUP feedback to date

- **Site legal advice**
  - Current draft text not sufficient
  - Rules not binding unless users aware of them
    - Must be pointers to all rules
    - Doesn't matter if too long to read
      - *As long as they have the opportunity*
  - Bullet 4 does not give us the right to control access
  - Data protection needs to be addressed if personal info shared
  - Must state that users register every 12 months
- **NREN response**
  - Looks good approach
  - Similar to work on location independent networking project
  - Perhaps move towards single AUP for common "visiting user" policy?
  - Bound by home site and home network rules
    - Must respect others and cease activity when requested
  - Need to make clear what is allowed and what not
    - Then can control access
    - Access can be limited to one application (tested in law)

AUP conclusion

- **Not yet ready for GDB approval**
  - BUT further comments very welcome
- **Awaiting feedback from another site lawyer**
- **JSPG needs to discuss the way forward**
  - Remembering that OSG has already approved
- **Will come back to GDB and ROC managers asap**

VO Security Policy

- **Draft document – presented at last GDB**
  - Author: Ian Neilson
- **https://edms.cern.ch/document/ 573348/**
- **No comments received**
  - Except for internal JSPG discussion
- **Made clear that security contact point must be a single e-mail address**
- **Recent discussion (not concluded) on VO AUP text**
  - Binding users to Grid/Infrastructure Policy or not?
  - What do users need to read, be able to read, be aware of?
- **Depends on final decision on User AUP**
- **So again, not ready for approval yet**
- **BUT… comments welcome!**

New Incident Response

- **Based on work by Open Science Grid**
- **We use the OSG document "as is"**
  - But with a covering document explaining differences
- **https://edms.cern.ch/document/428035**
- **Presented to GDB for first time today**
  - Then period of discussion
  - Ask for feedback from ROC Managers and OSCT
- **Aim for approval at next GDB**

OSG Document

- **Describes policy and procedures**
- **Sites MUST report security incidents**
  - In addition to normal reporting to CERT, CSIRT
- **Handling of sensitive data**
  - Public disclosure via PR offices
  - National/International coordination done by law enforcement
- **Security Contacts must be registered for each site**
  - Maintained by GOC
- **Mail list is also group of experts to provide advice**
- **Mail lists: Report and Discuss**
- **Defines the Incident Reporting process**
  - Discovery, Analysis, Classification, Containment, Notification, Escalation, Response, Post-incident analysis
- **Volunteer response team created if needed**

LCG/EGEE covering document

- **Intended audience**
  - Site Security Contacts and System Administrators
- **Defines mail lists for LCG/EGEE**
- **Warns that Incident Response info may be shared with other Grids (where agreements exist)**
- **Team leader to coordinate response**
  - Initially organised by site reporting and its local ROC security contact
  - ROC contact responsible to make sure that process happens

Sharing of Incident Info

- **In many cases it will be important to share Incident information between Grids**
- **May happen informally via sites which belong to more than one Grid**
- **Formal agreements will be needed**
  - Where Grids follow the same/similar policy and procedures
  - But only where reciprocal agreement
- **JSPG keen to arrange reciprocal agreement with OSG**
- **Also need to consider national Grids**
  - ROC responsibility so job here for OSCT?

Summary

- **More work needed on AUP and VO Security Policy**
  - Will come back to GDB when ready
- **Inviting discussion on Incident Response document**
  - Approval at next GDB?

Useful Links

- **Meetings - Agenda, presentations, minutes etc**

http://agenda.cern.ch/displayLevel.php?fid=68

- **JSPG Web site**

http://proj-lcg-security.web.cern.ch/

- **Policy documents at**

http://cern.ch/proj-lcg-security/documents.html