LCG/GDB Security

(Report from the LCG Security Group)

RAL, 8 July 2003

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

Overview

Topics for agreement today

- Rules for Use of LCG-1 Paper #36
- Audit Requirements Paper #37
- Incident Response Paper #38
- User Registration/VO Management Paper #39

Security Group meeting

– *19th June (phone)*

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

Rules for Use of LCG-1 #36

- To be agreed to by *all* users (signed via private key in browser) when they register with LCG-1
- Deliberately based on current EDG Usage Rules
  - Does not override sites rules and policies
  - Only allows professional use
- Once discussions start on changes
  - Chance we never converge!
- We know that they are far from perfect
- Are there major objections today?
  - One comment says we should define the list of user data fields (as agreed at the last GDB)
- Use now and work on better version for Jan 2004
  - Consult lawyers?

Audit Requirements #37

- UI None
- RB None – look at later
  - For origin of job submission
- CE gatekeeper maps DN to local account
  - Keep gatekeeper and jobmanager logs
- SE/GridFTP
  - Keep input and output data transfer logs
- Batch system
  - jobmanager logs (or batch system logs)
  - Need to trace process activity – pacct logs
    - This is large
- Central storage of all logfiles? Rather than on the WN
- To be kept for at least 90 days by **all** sites

Incident Response #38

- Procedures for LCG-1 start (before GOC)
  - Incidents, communications, enforcement, escalation etc
- Party discovering incident responsible for
    - Taking local action
    - Informing all other security contacts
- Difficult to be precise at this stage – we have to learn!
- We have created an ops security list (before GOC)
  - Default site entry is the Contact person but an operational list would be better
- LCG-1 sites need to refine and improve
- All sites must buy-in to the procedures

User Registration & VO Management #39

- User registers once with LCG-1
  - Accepts User Rules
  - Gives the agreed set of personal data (last GDB)
  - Requests to join one VO/Experiment
- We need robust VO Registration Authorities to check
  - The user actually made the request
  - User is valid member of the experiment
  - User is at the listed institution
  - That all user data looks reasonable
    - E.g. mail address
- The web form will warn that these checks will be made
- User data is distributed to all LCG-1 sites

User Registration aims

- To provide LCG-1 with accurate information about users for
  - Pre-registration of accounts (where needed)
  - Auditing (legal requirements)
- To ensure VO managers do appropriate checks
  - To allow LCG-1 sites to open resources to VO

- BUT… the current procedures have limited resources
  - To some extent has to be “best efforts”
    - E.g. do we need backup VO managers?

VO Registration (2)

- Today's VO managers
  - ALICE Daniele Mura INFN
  - ATLAS Alessandro De Salvo INFN
  - CMS Andrea Sciaba INFN
  - LHCb Joel Closier CERN
  - DTEAM Ian Neilson CERN
- Plan to continue to use the existing VO servers and services (run by NIKHEF) and the current VO managers (all agree to continue)
  - DTEAM run at CERN

VO/Experiment RA

- For LCG-1 start
- VO manager checks request via one of
  - Direct personal knowledge or contact (not e-mail)
  - Check in official CERN or experiment database
  - With official experiment contact person at employing institute
    - Signed e-mail? (not done today)
- Identity and employing institute are the critical ones
- VO managers/LCG registrar to maintain a list of institutes and contact persons
- Work needed on more robust procedures for 2004
  - That can scale
    - With distributed RA's?