LCG/GDB
Security Issues and Tasks

or Report from the Security Group

CERN, 10 Apr 2003

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

Aims

- Report on the first meeting of the new LCG Security Group (met yesterday at CERN)
- Present the issues we identified
  - And initial plans to work on these
    - But this is NOT a detailed plan yet
- Concentrate on what needs to be done by July 2003
  - (we also considered plans for the rest of the year)
- Invite comments, suggestions, feedback from the GDB

Draft Mandate

- To advise and make recommendations to the Grid Deployment Manager and the GDB on all matters related to LCG-1 Security
- To continue work on the mandate of GDB WG3
  - Policies and procedures on Registration, Authentication, Authorization and Security
- To produce and maintain
  - Implementation Plan (first 3 months, then for 12 months)
  - Acceptable Use Policy/Usage Guidelines
  - LCG-1 Security Policy
- Where necessary recommend the creation of focussed task-forces made-up of appropriate experts
  - *the Security Tier1 Contacts group already working*
    - *Dane Skow, FNAL*

Membership

- Experiment representatives/VO managers
  - *Important to create the balance between functionality and security*
- Site Security Officers
- Site/Resource Managers
- Security middleware experts/developers
- LCG management and the CERN LCG team
- Non-LHC experiments/Grids
  - Many sites also involved in other projects

- Missing today: Resource managers, middleware, geographical spread (Asia/Pacific) – nominations welcome
- Do we need reps from all 4 experiments? And who?
- Group should remain small (to allow real progress)

First Meeting
9 Apr 03 CERN

- Agenda: *http://agenda.cern.ch/age?a03877*
  - Morning: Introductions, Aims and WG3 report
  - Afternoon: Site survey, Issues and Plans
- Attended
  - Alberto Masoni, ALICE
  - Gilbert Poulard, ATLAS
  - David Stickland, CMS
    - Replaced by Greg Graham and Nick Sinanis for afternoon
  - Joel Closier, LHCb
  - Dane Skow, FNAL Security (by phone)
  - Bob Cowles, SLAC Security – non-LHC (by phone)
  - Denise Heagerty, CERN Security
  - Ian Bird, GDA manager
  - Markus Schulz, LCG CERN team
  - Dave Kelsey, RAL, Chair

Final WG3 report

- Final report (V2) now available following comments from Feb GDB and individuals
- A snapshot
  - Lots of work still to do
  - Starting point for work of the Security Group
- Needs to go on GDB web
  - Already on yesterday's agenda page

Tier-1 Site Survey

- Dane Skow reported
- *http://home.fnal.gov/~dane/LCG-1/*
- Questionnaire – see appendix B of WG3 report
- Have security contacts for all Tier1 sites
- Most have responded to questionnaire and most have provided link to their AUP (summary on web)
- Common agreement
  - Incident handling, AUP, 3rd party registration, no shared authentication, audit logs (3 mnths), communications channel
- Areas of diversity: Firewalls and Service restrictions

Issues and Implementation planning for July 2003

(responsibles in red where defined)

User Registration

- A Registration web (CERN team)
  - following existing EDG procedures
  - Instructions to the user
    - Where to obtain certificate etc
  - LCG-1 Usage Guidelines (see later)
    - "Signed" by certificate from trusted CA
  - Web form asking for the agreed info
    - Start from EDG form
    - Personal data required by sites (Sec Contacts)
- An LCG-1 Guidelines VO server and database (LDAP?) (CERN team)
  - But need to deal with privacy issues

User Registration (2)

- Once user has registered, the accounts need to be created at each of the LCG-1 sites
  - Some will allow pool accounts (e.g. atlas027)
    - still not shared
  - Others need named accounts
  - Do we need a policy on pool vs named? (general feeling No)
- Some sites require pre-registration of users
  - Big concern of scaling problems
    - EDG today has 450 registered users (many registered already)
  - Or registration by trusted 3rd party
    - Aim for "trusted" LCG-1 (and expt VO) registration
- More work required here (who?)
  - Aim for automation, but may have to start with manual procedures

VO Management

- The model
  - One LCG-1 Guidelines VO and 4 experiment VO's
  - For Authz, user needs to belong to LCG-1 *and* at least one experiment VO
  - Registration databases will contain personal information (privacy issues) and therefore require careful distribution and restricted access
  - The Authz VOMS database needs to be widely available and hence will contain limited info

VO management (2)

- Dane Skow told us about the USCMS VO Management Service Extension project (VOX) (FNAL)
  - Draft proposal (still to be considered)
  - *http://www.uscms.org/s&c/VO/design/proposal.doc*
- Builds on (collaboration forming)
  - VOMS (EDG, INFN)
  - LCAS/LCMAPS (EDG, NIKHEF)
  - VO-CMS (FNAL)
  - GUMS (BNL)
- Assumes a distributed VO database (is this appropriate?)
- Group will read proposal and comment (esp expts)
- For July 2003, concentrate on US CMS – learn from this
  - Later see if can scale to the whole project
- Encouragement for this group to continue
  - With appropriate membership
- Scope of fuller project still to be discussed

VO management (3)

- Jul03: use the existing experiment VO's
  - In EDG run today by NIKHEF
  - and existing VO Authz technology
- But, aim to improve Registration Authority (RA) procedures
  - With existing VO managers
- Written VO RA procedure(s) are required (who?)
  - Ideally one, but could be VO-specific
- Registration should contain an expiry/renewal date

Incident Response

- Existing procedures work well for site-specific problems
- New Grid aspect: need global view of behaviour
  - Clear role for Operations centres
  - Problems to be reported here
    - In addition to existing local reporting requirements
- Jul03: The CERN team will act as the incident clearing house
- Need informal communication
  - Via existing LCG Security Contacts list
    - Recent (non-Grid) Linux attacks are a good example!
- More formal procedure to be written down (Sec Contacts)
  - What are the responsibilities?
    - E.g. site discovering problem must initiate process

Incident Response (2)

- Operations Centre will need access to audit logs
  - Or agreed access to info contained within?
    - Is direct access to audit logs allowed?
- Need to agree which audit logs, their format and develop tools
  - CERN team
- If centre belongs to multiple Grids, will need to report incidents to them all.
- Legal and/or disciplinary action: Still between site and user
- Operations Centre will need to coordinate urgent removal of user from Authz.
  - Must also coordinate the re-instatement
- We recommend hierarchical Tier structure
  - Communication with Tier 2's via Tier 1

AUP/Usage Guidelines

- We need a first version for Jul03 (Sec Group)
- Start from EDG Usage Guidelines
  - Modify to LCG-1
  - Perhaps add something on privacy/use of personal data? (or perhaps later)
- To get through one lab's lawyers takes a long time
  - Impossible if all LCG lawyers involved?
  - Need a well defined process for review
- Two statements hopefully help
  - The Guidelines in no way prejudice the site rules
    - Need links to those available (English translations?)
  - LCG-1 is NOT to be used for "personal" use

LCG Security Policy

- We need one!
  - To state security aims of project and responsibilities of sites (and users)
  - Related to AUP
- But less urgent than the other tasks
- Aim for first draft in July 2003
  - Will come naturally out of discussions on procedures
  - But version 1 – only by Jan 2004
- Lawyers need to be involved
  - Perhaps the most sensitive document

Network Connectivity

- The usual ongoing discussion
  - Large farms run with no routable IP addresses
  - Network Address Translation (NAT) causes problems
  - No offsite connectivity from worker nodes
- From Security view: This is encouraged!
  - Biggest threat is likely to be major DOS attack
- BUT connection to EDG RB is required to transfer Sandbox
- We propose: Limit to GridFTP ports and known sites
  - Then limited contact may be possible?

Firewalls

- Important issue
- Being tackled today by CERN team and site managers as part of LCG-0 rollout
  - Maintain list of required ports
- This seems sufficient for now
  - But is it really?
  - One of the areas of diversity in the Site survey

Authentication

- Brief discussion at end of meeting
  - Needs more discussion
- Two main issues
  - Who defines the list of trusted CA's?
    - LCG or other Grid projects?
  - How to introduce new types of CA (online)?
    - E.g. Kerberos CA at FNAL
    - Could be task for LCG
- Today (continue like this for next 6 months?)
  - But we must agree compromises for July
  - European CA PMA is run by EDG
    - Next meeting tbd – May/June
  - New North America PMA being created
  - GGF discussing PMA coordination now

Future meetings

- Bi-weekly phone conference
  - experiment reps welcome but not essential
- Monthly face-to-face meeting
- Next meeting: 7th May (CERN)
  - Most urgent topic: 3-month Implementation plan
  - Plus phone conf if we can fit in around Easter