LCG/GDB Security Update

(Report from the Joint LCG/EGEE Security Group)

CERN
13 July 2004

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

Overview

- Joint (LCG/EGEE) Security Group meetings
  http://agenda.cern.ch/displayLevel.php?fid=68
  - 1 July 2004
  - Next meeting: 18 August 2004
- Operational Security concerns
- Two documents
  - Guide to
    Application, Middleware & Network Security
  - Proposal for meeting the LCG User Registration and
    VO Membership Management Requirements

Operational Security concerns

- Recent discussion on the lcg-rollout list…
- Who is responsible for operational security?
  - The Joint Security Group?
    - No – this advises GDB and SA1 on policy/procedures
  - The LCG Security Officer (Ian Neilson)?
    - Not fully (seen as role for the GOC)
    - he advises the deployment team and has no backup
  - The GOC?
    - No – Not (yet) fully operational
  - EGEE/SA1?
    - No – well not yet.

Operational Security (2)

- What does “operational” mean?
- Two aspects (expectations)
  - “Operations”
    - Discover/own/chase/fix security incidents
    - Liaise with national/institute CERTs
    - Install/run appropriate monitoring/intrusion detection
    - Ensure known problems are patched or worked around
    - Analyse audit logs
    - Perform security LCG Service Challenges

  Create security operations team (Ian Neilson + CIC/ROC reps)
  - “Quality control”
    - Evaluate/test new middleware for security
    - Identify new security holes (middleware or deployment)
    - Work with middleware developers/deployment team

  Needs another team (“security evaluations”)
    - include expert users and expert sysadmins
    - LCG or EGEE?

Guide to LCG Application, Middleware & Network Security

- The final document in the policy and procedures set
- Main author: Ian Neilson (LCG Security Officer)
- *https://edms.cern.ch/document/452128*
- V1.4 discussed at June 2004 GDB
  - Should it be "policy" rather than "guide"?
  - I will not describe the document (see last GDB)
- V1.6 (2nd July) distributed for discussion now
- Changes since V1.4
  - Title – include "Middleware", i.e. *all* software
  - Updated appendix for current firewall ports
  - Introductory paragraph changed

Guide to LCG … security (2)

Introduction now says…

This document identifies areas of security practice which the LCG Security Group and the Grid Deployment Board consider must be addressed in application and middleware design, planning and deployment processes where such software is to be used by or on the LCG.

The LCG Security and Availability Policy states that

"All the requirements for the networking security of LCG Resources are expected to be adequately covered by each site's local security policies and practices".

This document also seeks to identify and clarify issues where local security policy and LCG security policy must be aligned.

User Registration and VO Membership Management

- Requirements document (V2.7)
  - *https://edms.cern.ch/document/428034*
  - approved by GDB in May 2004
- Task force created to propose the solution
- TF Membership
  - Maria Dimou (LCG Registrar, DTeam VO manager)
  - Joni Hahkala (VOMS Admin development leader)
  - Tanya Levshina (VOX leader)
  - Ian Neilson (LCG Security Officer) – Task Force leader
  - DPK
- Many discussions with CERN HR, User Office, Experiment Secretariats, VO managers, …

Task Force/Proposal

- Task Force mandate
  1. Meet robust registration procedures in the Requirements document
  2. Investigate the use of existing sources of user data
     - For LHC this means the CERN HR databases (ORGDB)
  3. Achieve all possible compatibility between the requirements and existing technical solutions for VODB
     - i.e. VOMS and VOX
- Today's "Proposal" document (V0.2)
  - *https://edms.cern.ch/document/481701*
  - Maria Dimou (editor)
  - addresses items 1 & 2
  - Item 3 is ongoing

The Registration and VO Data/Databases

- ORGDB
  - No direct read access at all, except via link from AuthN/VODB
  - As maintained by CERN HR/User Office/Experiment Secretariats
  - User fields required here: Family Name, Given Name, Institute Name, Phone Number, e-mail address
  - And contract, experiment participation end dates
- Authentication part of VODB
  - Authorised read access possible (site admins)
  - Live link to record in ORGDB (via db key)
  - User's DN(s) from certificate and DN of signing CA
  - Registration and Expiry dates
- Authorisation part of VODB
  - Used by AuthZ technology (attribute authority)
  - Groups, Roles, attributes assigned by VO manager
  - Suspension status flag

Task Force Conclusions

- ORGDB usable but not always of sufficient quality
  - For our concerns – see later
- Need to harden some ORGDB registration procedures
- Each VO must document their ORGDB registration procedures
  - The experiment secretariats handle expiry/renewal and external users differently
  - JSG will provide a template document
    - In spirit of meeting the LCG requirements
  - For other (non-LHC) VOs, sites can then use this type of info to decide whether to open resources
- See diagram for detailed registration flow
  - *https://edms.cern.ch/document/481701*

Proposal

- Every user (4 LHC expts) **must** register in ORGDB first
  - Already true for the majority
    - Advantages of using existing procedures
    - No duplication of effort or personal data
  - External users (e.g. people never coming to CERN) and short-term users (e.g. summer students)
    - Needs a simple, speedy and robust procedure
  - Non-VO people, e.g.testers/experiment independent people
    - must register in ORGDB (e.g. via LCG/IT)
- Eventual aim is to use the experiment participation end-date in ORGDB to trigger immediate suspension from the VO

Proposal (2)

- VODB expiry date
  - Not exceeding 1 year from date of VO registration
  - Less if institute-contract/ORGDB-registration expires before then
  - Care to be taken with transition to avoid large number of renewals at the same time
- Personal User Data will **only** reside in ORGDB
- There is no automatic membership of VODB. User has to complete a form and the VO manager has to approve

Proposal (3)

- User request web form requires sufficient info to establish a unique link to the record in ORGDB
  - Name, CERN_ID or birthdate
  - E-mail address **must** be identical to one of those recorded in ORGDB
    - Proof of possession of mailbox during the registration process
  - Confirms acceptance of the Usage Rules
  - The DN is extracted from the certificate loaded in browser
- VO manager still has to confirm that the DN is “correct”
  - As not (yet) collected by ORGDB
  - Personal certificate
  - Name of CA and Common Name look “reasonable”

Proposal (4)

- Certificate renewal does not trigger a VO membership renewal unless the DN changes
  - Need to cope with multiple DNs per user
- Site/Resource Administrators will be able to read user personal data via a request to VODB
  - No direct access to ORGDB
  - Mechanisms for Authorisation to be defined
  - Users agree to this when they register
- When VODB expiry date is reached, the VO membership is **immediately** suspended
  - Advance warning will be sent to the user
- There will be other possible reasons for suspension
  - E.g. following security problems

Concerns/Future aims

- DN not captured by ORGDB today
  - Long term aim to do this
- Too many users remain in ORGDB with out-of-date information
  - Need to improve the expiry/removal/renewal procedures
- Need to improve the quality of External User registration
  - Remote team leader to be involved
  - Allocation of CERN_ID for this class
- Truly external (not a VO member) can be added to VODB by the VO manager as long as there is an entry in ORGDB (e.g. LCG)
- The ORGDB participation end dates are not managed today
  - Propose to set one per experiment and enforce it

Other issues

- Unique name per VO member
  - For persistent name to use in access control lists
  - DN can change or user may have several
  - There is a proposal that the VO creates a unique (within the VO) name per user which is then tied to the user by AuthZ attribute server (VOMS role)
- Emergency contact (for security incident)
  - Team leader may not be best person
  - User's institute phone number not enough
    - Mobile, home phone, etc also useful
  - Not part of this registration process, but rather
    - A VO responsibility
    - see LCG Security & Availability policy

Summary

- GDB is invited to
  - Advise on security operations concerns/teams
  - Discuss and approve the Application, Middleware & Network Security Guide
  - Discuss and approve the Proposal for LCG User Registration and VO Membership management