LCG/GDB Security

(Report from the LCG Security Group)

CERN, 9 September 2003

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

Overview

Topics

- Some issues from recent Security Group meetings
- LCG Security and Availability Policy (Draft 3)
  - For comment now
  - Aiming for approval at October GDB meeting

Security Group meetings

- *30th July (phone)*
- *28th August (CERN)*

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

Issues from recent LCG SEC meetings

- CSIRTS mail list (for incident response)
  - still awaiting entry for Taiwan and Tokyo
  - Raises concerns about response to an actual incident
- We learned that Budapest had joined LCG-1
  - But no security contact (on mail list)
  - What is the process for addition of sites?
  - Who should be informed?
  - The new sites also need to be informed of their responsibilities
- Deployment schedule does not address the need for fast response to any new security vulnerability
  - Needs to be done in hours (or days at most)

Issues (2)

- Security Audit/Testing
  - LCG should test software/implementations for security
    - As part of testing process
  - No one else is doing these tests!
  - Will need work to develop the tests
- CA key lengths
  - FNAL root CA has 4096 bits
  - Too long for Java
    - Import restrictions in some countries limit RSA to 2048
  - FNAL will reissue with 2048 bits
  - While investigations continue (legal situation)

Issues (3)

- Open connectivity
  - The Internet is a hostile place!
  - Site security officers tell us that full connectivity to large production facilities will not be possible
  - Strong desire to apply IP source address firewalls
  - Some sites ***cannot*** provide full connectivity to/from WN's
  - Needs policy and feedback to developers
- VOMS, VOX, AuthZ, User Registration
  - Workshop to be held in Nov/Dec 2003

Policy document

- *"LCG Security and Availability Policy"*
- Not asking for formal approval this time
  - Aim for October GDB meeting
- Concentrate today on approval and maintenance procedures
- and other general issues
- Trevor Daniels (GOC task force)
  - Main author
  - Working with Security Group

Background

- Originally Security Group was concentrating on a Risk Analysis document (to guide future work)
- With Security Policy early in 2004
- GOC task force convinced us otherwise
- Important for LCG to agree a high-level policy document asap
  - with the details defined in other documents

Objectives and Scope

- Objectives
  - *Attitude* of the project towards security and availability
  - *Authority* for defined actions
  - *Responsibilities* on individuals and bodies
- Control of resources and protection from abuse
- Minimise disruption to science
- Obligations to other network (inter- and intra- nets) users
- Broad scope: not just hacking!
- Maximise availability and integrity of services and data
- Resources, Users, Admins, Developers and applications
- Does NOT override local policies

Ownership and procedures

- Important point for discussion today
- High-Level policy document
  - For ratification by LCG project at highest level
    - Suggest POB (or PEB?)
  - For lifetime of LCG
  - Need to ensure stature and longevity of the Policy
- Technical docs implementing or expounding policy
  - Procedures, policies, guidelines, rules, …
  - Run by a technical body (propose Security Group)
    - timely and competent changes
    - GDB approval for initial docs and significant revisions
  - Must address the objectives of the policy
- Review top-level policy at least every 2 years
  - Ratification by POB if major changes required
- Do we need to define an appeals process?

Compliance and Sanctions

- Require Site self-audit at least every 2 years
  - Check policy (and associated procedures and practices) is being followed
  - Procedures to be defined by GOC
- Independent audit (by or for GOC) allowed if
  - Self audit not performed
  - Not following policy
  - At random
- Audits to be published (by GOC)
  - To whom?
- Sanctions defined for failure to comply
  - Sites (or admins) – remove services
  - Users – remove right of access

Policy document
Other issues during drafting

- Section 2: LCG Services and Resources
  - Include an example list of services?
- Section 3: Roles and Responsibilities
  - VO's
    - Important role for the user's employer (institute)
    - LCG must be available to all (so why include personnel screen)
  - Resource Admins
    - Who should they notify at their site?
    - Do we need to specify and/or police?
    - Risk assessment needs to involve developers
  - Developers
    - They select software as well as develop it
    - Do we need a developers guide (security model)?

Associated documents

- User Registration and VO Management (exists)
- User Rules (exists)
- Procedures for Resource Administrators
- Procedures for CA's (exists)
- Guide for network admins
- Procedures for site self-audit
- SLA Guide
- Incident Response (exists)
- Developers Guide?