LCG/GDB Security Update

(Report from the LCG Security Group)

CERN

15 June 2004

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

Overview

- Joint (LCG) Security Group meetings
  - 19 May & 4 June 2004
  - Next meeting: 1 July 2004
- Security warning
- LCG expansion concerns
- Policy documents
  - New Guide to Application & Network security
- CA approval procedures
- EGEE Site Security requirements
- Summary

LCG Security warning

- Growing interest in Grid
  - TeraGrid attack
  - Article in New Scientist magazine (22 May)
    - "Hacking the Grid"
  - Talk at 2600 hacker conference (9-11 July)
- An attack is inevitable!
- All sites need to be aware
- Keep each other informed
  - via the Security Contacts list
- Follow LCG Incident Response procedures
  - Important role for GOC
- Warning sent to all security contacts on 10th June
- Planning to test security as part of LCG service challenges

Concerns re LCG expansion

- LCG is now very large
- All new sites receive the security policy documents
- There is a mail list to ask questions
  - But very little use!
- Tier1 security contacts are usually the official site security officer
  - Tier2 contacts are more often local to the resource
- Tier1 managers are present in GDB
  - Tier2 managers often are not
- Do all LCG sites understand their responsibilities?
- We are starting to consider a Site Registration process
  - E.g. sign agreement to policy documents?
- All very important for incident response

Guide to LCG Application & Network Security

- The final document in the policy and procedures set
- V1.4 (7th June) now ready for GDB comment
- Main author: Ian Neilson (LCG Security Officer)
- Aim
  - It is a *Guide* and not *Policy*
  - Guide choices in design, planning and deployment of LCG Grid services
  - Identify key areas of best practice
- BUT, it contains important recommendations for deploying a secure production Grid
  - Important for GDB to approve the Guide

Guide: Application and Service Development

- LCG expects development processes that
  - Support adequate and documented treatment of security
- E.g. Current misalignment
  - IP connectivity from anywhere to anywhere
  - Incoming: weakens site
  - Outgoing: distributed DOS
- Current firewall requirements in Appendix B
  - LCG Security Group considers these inappropriate for a production Grid
  - Application developers MUST NOT rely on the current settings – not a minimal set

Some recommendations (development)

- Design and development process
- Coding practice
- Communications security
  - Authentication
  - Encryption
  - Use existing protocols
- Functional security
  - Authorization
  - Degrade and fail gracefully
  - Logging
  - Avoid leakage of information

Application and Service Deployment

- LCG expects security instructions in documentation
- Evaluate risks
- Establish clear network access control policy
- Apply configuration management and automate
- Keep systems patched for security updates
- Configure and retain audit logs

CA approval procedures

- Current process takes too long
  - All new CAs or any changes need GDB approval
    - Takes 2 weeks
    - Experience shows there has been no discussion
  - CA details currently linked to LCG releases
- EU Grid PMA now exists
  - EGEE will use all CAs approved by the PMA
- Proposed new streamlined LCG process
  - Accept the EU Grid PMA approved list
  - Release CA rpms independently on LCG releases
  - But NOT mandatory on all sites during a 2 week period of discussion
  - Any additional CAs still follow the existing procedure

EGEE Site Security Requirements

- The Joint Security Group has been asked to submit a list of Top 10 site requirements
  - For discussion at the EGEE Middleware Security Group Meeting (16-17 June)
- A draft list has been prepared
  - sent to the LCG site security contacts (8 June)
- Just two responses to date
  - Consider use of SELinux
  - List of some known security problems today
- The Network and Applications Security Guide and the GGF Site AAA requirements guide are also important input

"Top 10" security requirements (middleware)

- Sites in control of local security policy
- Audit/track at individual user level
- Sites control local AuthZ policy
- Authorize, limit or forbid IP connectivity
- Hooks/logging for intrusion detection
- Consistent and appropriate audit logs
- Development and deployment of secure middleware
- Able to cope with distributed AuthZ (user, VO, site)
- Shutdown and restart services gracefully
- Robust VO and user registration tools (procedures)

Summary

- GDB is invited to
  - Either now or by e-mail
  - Discuss and approve the Application and Network Security Guide
  - Comment on new CA approval process
  - Comment on EGEE Site Security Requirements
  - Consider how to improve the integration of Tier 2 sites as LCG expands