CCLRC

GridPP
UK Computing for Particle Physics

LCG/EGEE/OSG Security Incident Response

Grid Operations workshop
CERN, 2 November 2004

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

Open Science Grid

LCG

egee
Enabling Grids for E-science in Europe

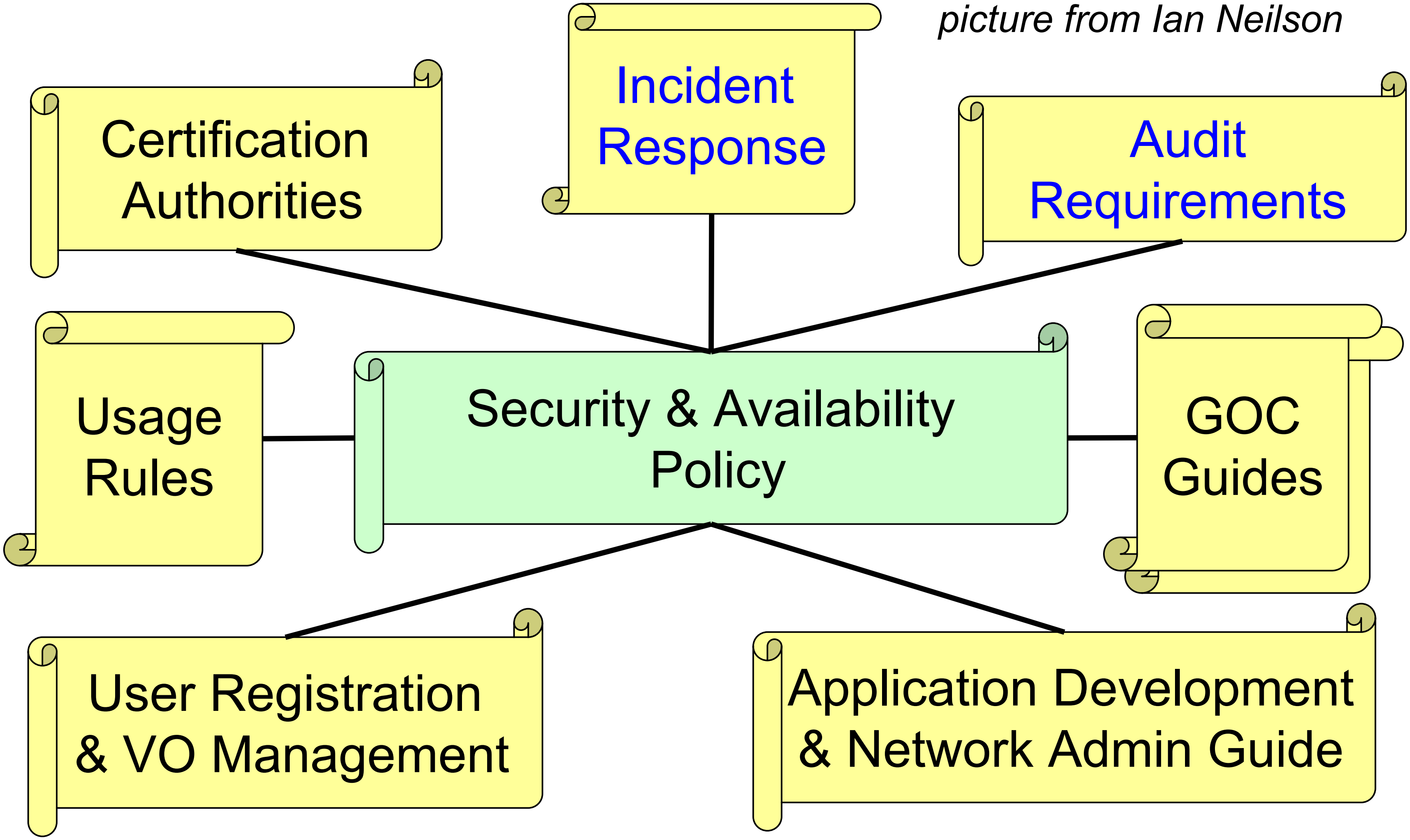
Outline

- Security Incident Response today
- Open Science Grid work in this area
  - *LCG/EGEE already agreed to base new procedures on this OSG work*
  - Show (some) slides by Bob Cowles (SLAC)
    - Talk given at HEPiX meeting (BNL, 22 Oct 04)
- LCG/EGEE
  - Operational Security Coordination Team
  - Show (some) slides by Ian Neilson (CERN)
    - Talk given at EGEE ROC Managers mtg (5 Oct 04)
- Summary

Incident Response Today (LCG/EGEE)

LCG/EGEE Policy

picture from Ian Neilson



Certification Authorities

Incident Response

Audit Requirements

Usage Rules

Security & Availability Policy

GOC Guides

User Registration & VO Management

Application Development & Network Admin Guide

http://cern.ch/proj-lcg-security/documents.html

Incident response today (1)

- When sites join LCG/EGEE
  - Provide security contact names
    - Including phone numbers
  - And a mail list for emergency contact
- LCG Audit Requirements

  See https://edms.cern.ch/document/428037/
  - Every site must keep (for at least 90 days)
    - *Jobmanager* and/or *gatekeeper* logfiles
    - Data transfer logs
    - Batch system and process activity records
  - Need to be preserved over system re-installs
  - Logs also needed for accounting

Incident response today (2)

- Agreement on Incident Response

  See *https://edms.cern.ch/document/428035/*
- What is an incident?
  - Investigation -> break in service
  - Misuse of remote Grid resources
  - Long-lived (>3 days) credentials stolen
- Sites must
  - Take local action to prevent disruption
  - Report to local security officers
  - Report to others via Grid CSIRT mail list

Open Science Grid

PPDG

Incident Response Plan for the Open Science Grid

Grid Operations Experience Workshop – HEPiX
22 Oct 2004

Bob Cowles – bob.cowles@slac.stanford.edu

Work supported by U. S. Department of Energy contract DE-AC02-76SF00515

Principles

- OSG is a project with little central control or resources – almost everything has to be done by the sites or the VOs
- Site security personnel will need to feel comfortable with grid use of resources
  - limited additional risks
  - local control over decisions

Centrally Provided

- List of site security points of contact
- Secure email communications
- Incident Tracking system
- Functions of the Grid Operations Center (GOC)
- Coordinate with other GOCs

Site Responsibilities – 1

- Have a site incident response plan in place (logs, evidence)
- Report grid-related incidents (hi-priority list)
- Remove compromised servers
- Refer press contacts to OSG Public Relations

Site Responsibilities – 2

- Report follow-up to email discussion list and Incident Tracking System
- Take appropriate care with sensitive material collected
- Provide appropriate law enforcement with materials for coordination, investigation and prosecution

Open Science Grid

Incident Classification

PPDG

- Potential to compromise grid infrastructure
- Potential to compromise grid service or VO
- Potential to compromise grid user

Open Science Grid

Response Teams

PPDG

- Self-organized body of volunteers
- Mailing list maintained by GOC
- Team organized for severe or complex incidents
- Team leader to coordinate efforts and maintain information flow with GOC and public relations

Incident Handling – 1

- Discovery and reporting
  - local procedures & GOC list notified
- Triage
  - verify incident and perform classification
- Containment
  - remove resources, services, users
- Initial notification
  - record known information in tracking system
- Analysis and Response

Open Science Grid

Incident Handling – 2

PPDG

- Tracking and progress notification
  - updates on discussion list & tracking system
- Escalation
  - form IRT if complex or widespread
- Reporting
  - CERTs, law enforcement, other GOCs, etc.
- Public Relations
- Post-incident analysis

Timeline

- *Jun 04 – Security TG formed*
- *Jul 04 – IR Activity formed*
- *Sep 04 – First draft of plan reviewed*
- **Oct 04 – Coordinate with EGEE/LCG**
- **Nov 04 – Present plan at 2nd EGEE mtg**
- **Dec 04 – Implementation**
- **Jan 05 – Implementation & testing**
- **Feb 05 – OSG-0; EGEE Review**

The Plan

http://computing.fnal.gov/docdb/osg_documents//Static/Lists//FullList.html

www.opensciencegrid.org

click on “Documents”

click on “Search the database and read documents”

click on “OSG Secuirty Incident Handling and Response”

LCG/EGEE Security Coordination

(OSCT: Operational Security Coordination Team)

Ian Neilson

Grid Deployment Group

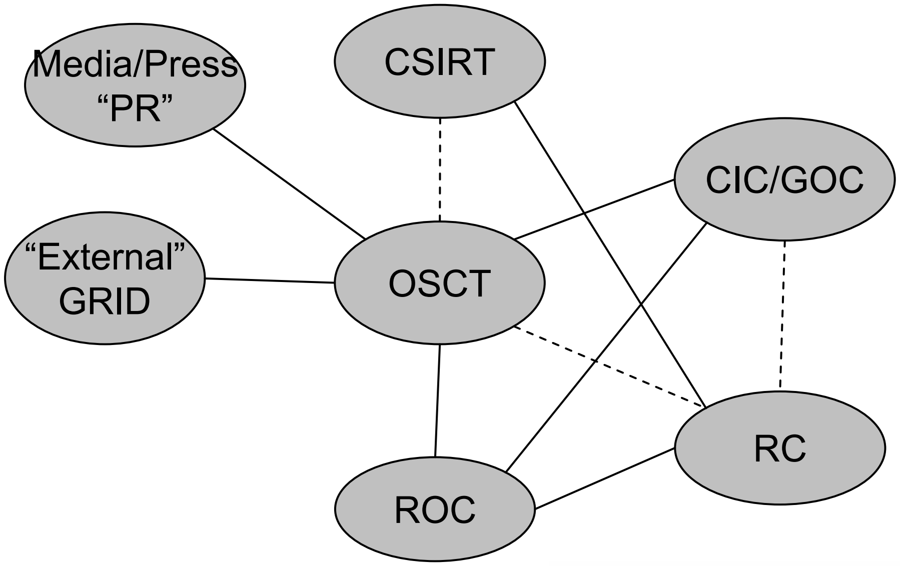
CERN

(talk given 5 Oct 2004)

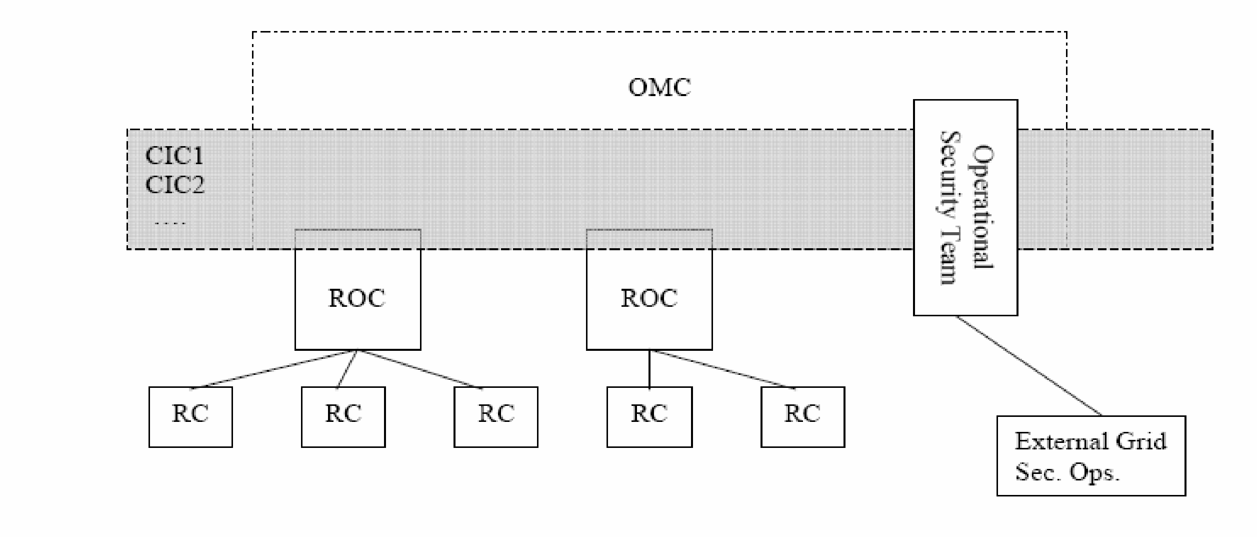
Security Coordination Objectives

- Ownership of …
  - Security incidents
    - From notification to resolution
    - Liaise with national/institute CERTs
  - Middleware security problems
    - Liaise with development & deployment groups
- Co-ordination of security monitoring
- Post-mortem analysis
- Access to team of experts
- Security Service Challenges - LCG

Security Coordination - Channels



EGEE operational channels still being established. Responsibilities and processes being defined.



Security Coordination – Comms.

- Incident Reporting List
  - **INCIDENT-SEC-L@xxx.yyy**
- Security Contacts Discussion List
  - **INCIDENT-DISCUSS@xxx.yyy**
- External contact
  - Reporting
  - Other grids
- MUST be Encrypted
  - How is this achieved and managed?
- Tracking system
  - MUST be secure
- Press and Public Relations

Security Coordination - Issues

- “Security Operations Centre”: what is it for EGEE/LCG?
  - Don’t think we can have “Central” control
    - So formulate activity as “coordination team”
  - Security contacts lists need management
    - Dead boxes, moderated boxes, etc etc
    - Do we have appropriate contact: site security or local admin?
  - Need to coordinate through Regional Operations Centres (ROC)
  - Need to utilise services from Core Infrastructure Centres (CIC)
    - Wherever possible - don’t duplicate channels
    - What is the relationships with LCG GOCs and EGEE CICs?
      - Are they the same?
  - Are we communicating with local site security team or grid ‘admin’ responsibles

Operational Security – where to start?

- “*Start small and keep it simple.*”
- Define basic structures
  - Where/how lists hosted
  - Where/how problems tracked
  - Who/where/how ‘experts’ organised
- JSPG review and update policy documents
- ROCs to take over management of contacts lists
  - Must integrate with site registration process
  - Establish what level of support is behind site security entries
  - Relationships with local/national CERT
  - Validate/test entries
- Exercise channels and raise awareness by Security Challenges – next slide.. *(Not shown here!)*

Summary

- There is much work ahead of us!
- We need to work **together** to define and maintain better incident response policies and procedures
  - Wherever possible should work towards common (or at least interoperable) procedures between Grid projects
    - Our applications are global
  - Must *add* to existing CSIRT procedures
    - Keep it simple to start with
- Much to discuss in the track on Operational Security (tomorrow)
  - And for discussion in the EGEE project conference (25th Nov 2004)