UK Computing for Particle Physics

Update on LCG/EGEE Security Policy and Procedures

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

LCG GDB Meeting,
CERN, 18 May 2005

www.eu-egee.org

Information Society

Overview

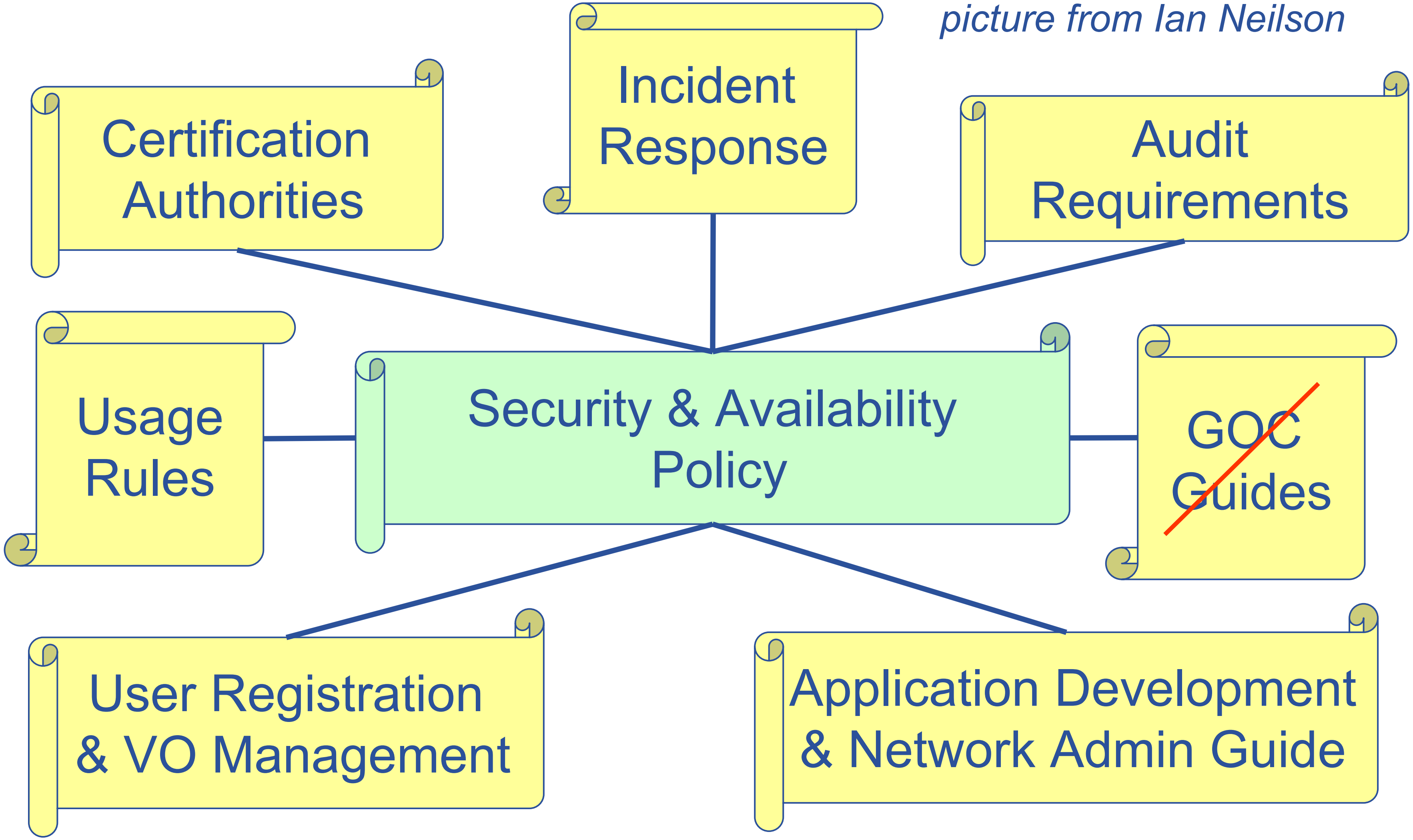
Work of the Joint (LCG/EGEE) Security Policy Group

- ***In collaboration with US Open Science Grid (OSG)***

- Security Policy Documents (at end of 2004)
  - **And plans for review**
- Work in progress
  - **User Acceptable Use Policy**
    - Not yet in EDMS
  - **VO Security Policy (and AUP)**
    - https://edms.cern.ch/document/ 573348/
  - **Incident Response**
    - https://edms.cern.ch/document/428035/
  - ***Seeking GDB and EGEE approval (first 2) within 30 days***
- Other JSPG activities

EGEE/LCG Security Policy (end 2004)

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

Current Policy documents

- **Go through one by one**
- **Show an original slide as presented to GDB at time of approval (or introduction from document)**
  - With comments

Security and Availability Policy

Top Level Policy document (approved Oct 2003)

- **Objectives**
  - Agreed set of statements
    - *Attitude* of the project towards security and availability
    - *Authority* for defined actions
    - *Responsibilities* on individuals and bodies
- **Promote the LHC science mission**
- **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, Administrators, Developers (systems and applications), and VOs**
- **Does NOT override local policies**
- **Procedures, rules, guides etc contained in separate documents**

Usage Rules

"Rules for Use of the LCG-1 Computing Resources"

  - Approved July 2003

- **To be agreed to by *all* users (signed via private key in browser) when they register with LCG-1**
- **Deliberately based on current EDG Usage Rules**
  - Does not override sites rules and policies
  - Only allows professional use
- **Once discussions start on changes**
  - Chance we never converge!
- **We know that they are far from perfect**
- **Are there major objections today?**
  - One comment says we should define the list of user data fields (as agreed at the last GDB)
- **Use now and work on better version for Jan 2004** ***(too optimistic!)***
  - Consult lawyers?

User Registration and VO Management

- **First document**
  - ***User Registration and VO management for LCG-1 in 2003***
  - Approved July 2003
- **User registers on LCG-1 web site (one central)**
  - Agrees to and “signs” Usage Rules
  - Agrees to personal data being distributed to all LCG-1 sites
    - For use of site/resource managers ONLY
- *Last name, First name, Institution, e-mail address, telephone number, experiment*
- **Distributed to all LCG-1 sites (down to Tier 2)**
  - Can be used for pre-registration if required
- ***Checks made by Expt/VO managers***

User Registration (2)

- Second Document
  - *Requirements for LCG User Registration and VO Membership Management*
  - Approved May 2004
- Use existing experiment processes and databases
- Task force created to propose the technical solution
- Many discussions with CERN HR, User Office, Experiment Secretariats, VO managers, …
- Technical solution agreed in Sep 2004
- Status presented to GDB by Maria Dimou in Feb 2005
- VOMRS front-end (FNAL)
  - linked to CERN HR DBs
- VOMS (with groups and roles)
- LHC users *must* register with the experiment first
- User Registration Workshop – 23-26 May 2005 (CERN)
- Transition from current system planned for second half 2005

Certification Authorities

"Approval of LCG-1 Certificate Authorities"

  - **Approved June 2003**

- **The LCG-1 Security Group proposes the list of accepted CA's from two sources:**
  - The list of "traditional" CA's, issuing long-lived (12 months or more) certificates, comes from the EDG CA Group
  - The list of additional CA's (online short-lived, special cases, etc.) is generated by the LCG-1 Security Group
- **Proposed additions to these lists above will be circulated to the GDB and to the LCG-1 site security contacts for objection prior to implementation**
- **The LCG-1 operations team maintains the necessary information (certificates, signing policy, CRL's) and distribution mechanisms for CA's on both sub-lists**
- **All LCG-1 resources will install the full list of approved CA's**

Incident Response

- **Approved July 2003**
- **Procedures for LCG-1 start (before GOC)**
  - Incidents, communications, enforcement, escalation etc
- **Party discovering incident responsible for**
    - Taking local action
    - Informing all other security contacts
- **Difficult to be precise at this stage – we have to learn!**
- **We have created an ops security list (before GOC)**
  - Default site entry is the Contact person but an operational list would be better
- **LCG-1 sites need to refine and improve**
- **All sites must buy-in to the procedures**

Audit Requirements

Audit Requirements for LCG-1

- Approved July 2003

- **Keep gatekeeper and jobmanager logs**
- **SE/GridFTP**
  - Keep input and output data transfer logs
- **Batch system**
  - Keep jobmanager logs (or batch system logs)
  - Need to trace process activity – pacct logs
- **Central storage of all logfiles. Rather than on the WN**
  - To survive reinstalls etc.
- **To be kept for at least 90 days by** all **sites**
- **(comment: many sites are not keeping pacct logs)**

GOC Guides

- **3 new GOC guides presented at March 2004 GDB**
  - Resource Administrators Guide
  - Service Level Agreement
  - Procedure for Site Self Audit
- **Approved May 2004**
- **But not really security policy**
  - And not clear to what extent being used/followed
- **Therefore removed from the policy set**
  - Agreed by GDB in Dec 2004
- **Future work in these areas: GOCs & ROCs (not JSPG)**

Application Development and Network Admin Guide

Guide to LCG Application, Middleware & Network Security

- Approved July 2004

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.

Policy Revision during 2005

- **Original deadline for review of 2003 documents was 1 year from GDB approval**
  - Too optimistic!
- ***All* documents are valid (for LCG & EGEE) until replaced or removed (even if “LCG”, “LCG-1”, etc…)**
  - Decision of GDB in Jan 2004
- **Need to revise ALL documents during 2005**
  - Make them more general, simpler and shorter
  - And up to date
- **Next to be tackled is the “Security and Availability Policy”**
- **To be formally approved by LCG and EGEE management**
- **New documents (not revisions)**
  - Site Registration Policy and Procedures
  - VO Security Policy

Site Registration

Site Registration Policy & Procedure

- Approved Mar 2005 (presented to GDB by Maria Dimou Feb 05)

- LCG/EGEE operating security policies place responsibilities on all participants.
- This site registration policy and procedure document aims to ensure that resource providers understand and have agreed to honour their responsibilities and that they have the necessary information available to perform their duties.
- Another reason for this procedure is to record at the level of the Grid Operation Centre (GOC) valid Resource Administrators' and Site Security Contact information, in order for the Core Infrastructure Centre (CIC) and the Regional Operations Centre (ROC) to promptly act, in case of service change or problem.

Current Usage Rules

- **During registration with a VO**
- **User agrees to acceptance of current "Usage Rules"**
  - "Rules for Use of the LCG-1 Computing Resources"
  - https://edms.cern.ch/document/ 428036/
- **This document is too long (5 pages)**
  - Very few users actually read it!
- **It is too LCG specific (even LCG-1!)**
  - It was based on the EDG Security Policy
- **Therefore it needs updating**
- **Open Science Grid just published their User AUP**
  - We want/need to be compatible
- **SEE-Grid AUP also recently published**
  - Also based on OSG AUP
  - We took ideas from this too

New User AUP

- **New draft User AUP**
  - Heavily based on OSG AUP
  - Modified for use in EGEE/LCG
  - Then discussed during ISGC 2005 (Taipei)
    - A common AUP for OSG/LCG/EGEE
      - *And national Grids?*
- **A single User AUP for *all* VOs on EGEE**
  - Short and simple
- **VOs define their objectives and AUP**
- **Sites can then consider these when deciding whether to support the VO or not**
- **Will no longer need to merge VO and Auth LDAP entries – AUP is tied to each VO**

User AUP (Version: *The Taipei Accord 29 April 2005*)

USER AGREEMENT (accepted during registration with a VO)

1) You may only perform work, or transmit or store data consistent with the activities and policies of the Virtual Organizations of which you are a member, and only on resources authorized for use by those Virtual Organizations.

2) You will not attempt to circumvent administrative or security controls on the use of resources. If you are informed that some aspect of your grid usage is creating a problem, you will adjust your usage and investigate ways to resolve the complaint.

User AUP (2)

3) You will immediately report any suspected compromise of your grid credentials or suspected misuse of grid resources to incident reporting locations specified by the Virtual Organization(s) affected and credential issuing authorities as specified in their agreements and policy statements.

4) You are aware that resource providers have the right to regulate access as they deem necessary for either operational or security-related reasons and that your use of the Grid is also bound by the rules and policies of the organizations through which you obtain access, e. g. your home institute, your national network and/or your internet service provider(s).

Comments: Also bound by policies of resource providers and Grid Infrastructure – add words?

VO Security Policy

- **Draft document (discussed twice in JSPG)**
  - Author: Ian Neilson
- **https://edms.cern.ch/document/ 573348/**
- **Following the decision after Den Haag to split the security aspects from the registration procedures**
  - VO Registration procedures presented in EGEE-03 SA1 session
- **This draft VO Security Policy document, is now ready for discussion and approval soon**
  - Please provide comments to Ian Neilson
- **There are 5 main sections in the document**
  - Present each here briefly

Aims

- **Aims**
  - Defines responsibilities placed on VO members and the VO as a whole (via VO managers)
  - To ensure that all Grid participants can properly fulfil their roles re interactions with a VO
- **Exclusions**
  - Does not address dispute procedures
    - These need to be addressed by VO and Grid management

VO Registration Requirements

- **To satisfy Grid security requirements**
- **VO enrolment MUST capture and maintain**
  - VO Name
  - VO AUP
  - Contact details for VO manager and at least one alternate
  - Generic contact e-mail address for VO managers
  - URL of one or more VO membership servers

VO AUP

- **VO must publish an AUP**
  - Can be light-weight (see example later)
- **Describe goals of the VO**
- **Define expected acceptable usage**
- **Define incident reporting channels**
- **A community of responsible users with common goal**
- **Require all VO members to**
  - Act within constraints of the VO AUP
  - Bind VO members to the general Grid User AUP
- **Must state which VO management body gives authority to the policy**

VO Community Responsibilities

- **Both ordinary members and VO managers**
- **VO managers must**
  - Ensure VO registration and membership server management meets agreed User Registration Requirements
    - E.g. maintain accurate user contact info
  - Suspend members if requested to do so by site security, GOC, ROC
  - Cooperate fully in investigation of security incidents
  - Respect privacy policy re user’s personal information
- **VO members must**
  - Abide by User AUP
  - Cooperate fully in investigation of security incidents

Sample VO AUP

“This Acceptable Use Policy applies to all members of *[VO Name]* Virtual Organisation, hereafter referred to as the VO, with reference to use of the LCG/EGEE Grid infrastructure, hereafter referred to as the Grid. The *[owner body]* owns and gives authority to this policy. The goal of the VO is to *[describe here the objectives of the VO]*. Members and Managers of the VO agree to be bound by the Grid Acceptable Usage Rules, VO Security Policy and other relevant Grid Policies, and to use the Grid only in the furtherance of the stated goal of the VO.”

New Incident Response

- Based on work by Open Science Grid
- We use the OSG document as is
  - But with a covering document explaining differences
- https://edms.cern.ch/document/428035
- Propose that this is presented at next GDB
  - (as part of a general report on operational security?)

Other Topics

- **LHC User Registration Task Force**
  - Workshop next week
- **EGEE Operational Security Coordination Team**
  - Proposed to GDB in July 2004
  - Now getting more active (see EGEE-03 Athens agenda)
    - Security Service Challenges, Incident Response, Security Monitoring, Forensics, Best practice (docs)
- **Security Risk Analysis**
  - Important to prioritise future work
- **Vulnerability Identification and Reduction**
  - Also proposed to GDB in July 2004
  - Started as GridPP activity in Jan 2004 (developers checklist)
    - Presented to EGEE-03 in Athens – general agreement
    - Starting now
    - Evaluate gLite 1 and LCG 2.4.x (improve quality and fix problems)

Useful Links

- Meetings - Agenda, presentations, minutes etc

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

- JSPG Web site

http://proj-lcg-security.web.cern.ch/

- Policy documents at

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

Summary

- **Most policy documents need revision during 2005**
- **We are now seeking approval of 2 documents (30 days)**
  - User AUP
  - VO Security Policy (AUP)
- **Will also invite comments from all sites, VO's and other Grids**
- **And approval by EGEE ROC managers**
- **Security Incident Response (and operational security?)**
  - Present at next GDB?
- **Next JSPG meeting**
  - 13/14 June (CERN)
  - Risk Analysis
  - Operations and User Reg Task Force
  - Revision of top-level policy document