LCG Security

LHCC Review, 25 November 2003

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

Overview

- LCG Security Group
  - Mandate and membership
- Meetings and web pages
- Policies and procedures
- Risk Analysis
- Future plans

LCG Security Group Mandate

- To advise and make recommendations to the Grid Deployment Manager and the GDB on all matters related to LCG-1 Security
  - *GDB makes the decisions*
- To continue work on the mandate of GDB WG3
  - Working Group 3 (Security) was one of 5 such groups
  - Policies and procedures on Registration, Authentication, Authorization and Security
- To produce and maintain
  - Implementation Plan (first 3 months, then for 12 months)
  - Acceptable Use Policy/Usage Guidelines
  - LCG-1 Security Policy
- Where necessary recommend the creation of focussed task-forces made-up of appropriate experts
  - *e.g. the "Security Contacts" group*

(n.b. GDB = Grid Deployment Board)

Membership

- Experiment representatives/VO managers
  - Alberto Masoni, ALICE
  - Rich Baker, Anders Waananen, ATLAS
  - David Stickland, Greg Graham, CMS
  - Joel Closier, LHCb
- Site Security Officers
  - Denise Heagerty (CERN), Dane Skow (FNAL)
- Site/Resource Managers
  - Dave Kelsey (RAL) - Chair
- Security middleware experts/developers
  - Roberto Cecchini (INFN), Akos Frohner (CERN)
- LCG management and the CERN LCG team
  - Ian Bird, Ian Neilson
- Non-LHC experiments/Grids
  - *Many sites also involved in other projects*
  - Bob Cowles (SLAC)

Meetings, Web etc

- Agenda, presentations, minutes etc

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

- LCG Security Group Web site

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

- Meetings
  - Started in April 2003
  - Met 11 times to date
    - 4 face to face and 7 phone conferences
- Report to the monthly GDB meetings

http://agenda.cern.ch/displayLevel.php?fid=3l181

Policies and procedures

6 documents approved to date (see LCG SEC web)

- Security and Availability Policy for LCG
  - Prepared jointly with GOC task force
- Approval of LCG-1 Certificate Authorities
- Audit Requirements for LCG-1
- Rules for Use of the LCG-1 Computing Resources
- Agreement on Incident Response for LCG-1
- User Registration and VO Management

4 more being written (with GOC group)

- LCG Procedures for Resource Administrators
- LCG Guide for Network Administrators
- LCG Procedure for Site Self-Audit
- LCG Service Level Agreement Guide

Security and Availability Policy

- Prepared jointly with GOC group
  - Editor: Trevor Daniels (RAL, GOC)
- 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

Policy: Ownership, maintenance and review

- The Policy is
  - Prepared and maintained by Security Group and GOC
  - Approved by GDB
  - Formally owned and adopted as policy by SC2
- Technical docs implementing or expounding policy
  - Procedures, guides, rules, …
  - Owned by the Security Group and GOC
    - timely and competent changes
    - GDB approval for initial docs and significant revisions
  - Must address the objectives of the policy
- Review the top-level policy at least every 2 years
  - Ratification by SC2 via GDB if major changes required

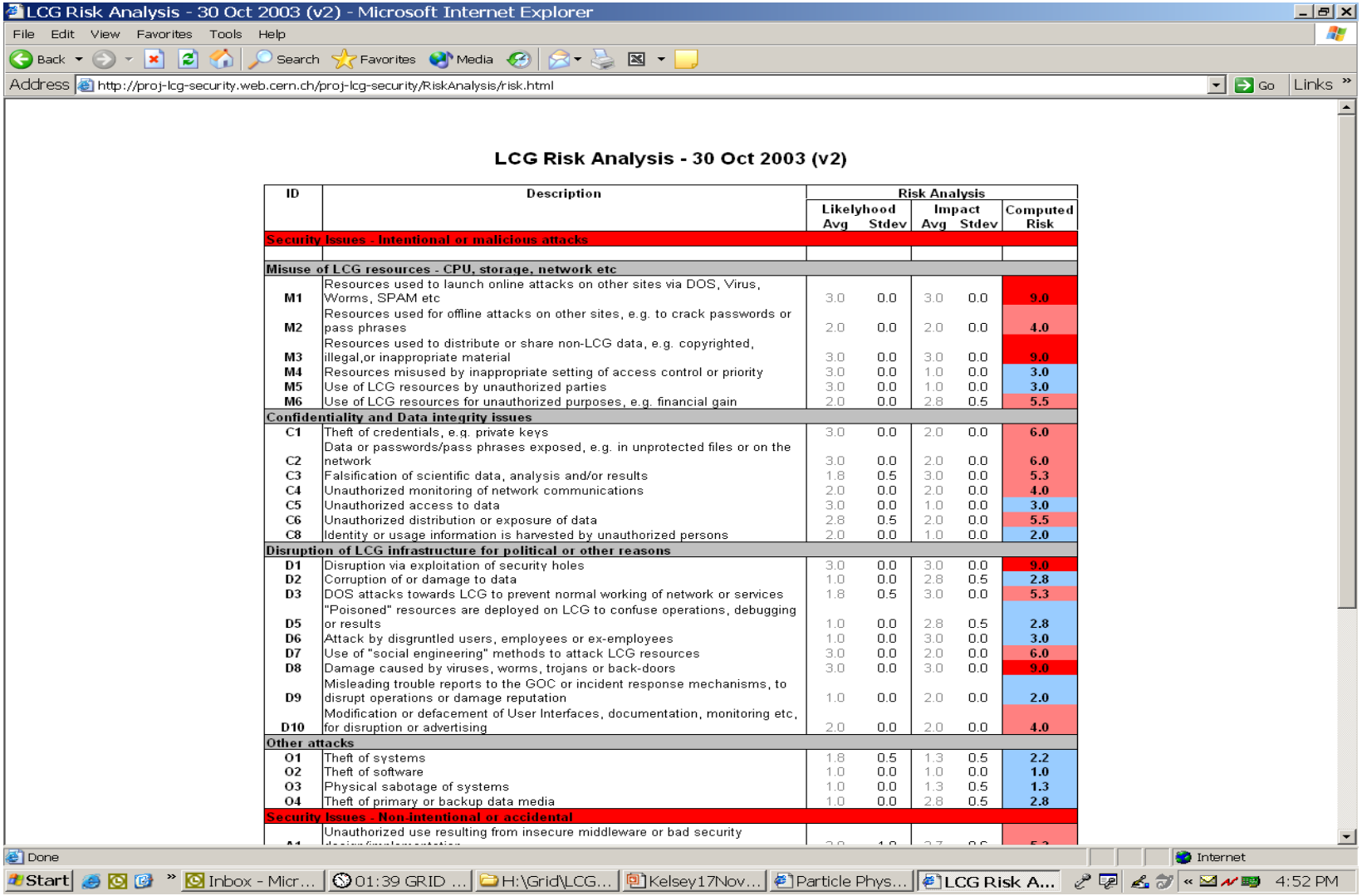
User Registration & VO Management

- User registers ***once*** with LCG (and not at individual sites)
  - http://lcg-registrar.cern.ch/ (using Grid certificate)
  - Accepts User Rules
  - Gives the agreed set of personal data
    - Agreement on a minimal set was important achievement
  - Requests to join one VO/Experiment
- Sites need robust VO Registration Authorities (RA) to check
  - The user actually made the request
  - User is valid member of the institute & experiment
  - That all user data looks reasonable
- The User data is distributed to all LCG sites
- Work needed on more robust scaleable procedures for 2004
  - To date only ~90 users have registered with LCG
  - Workshop on this topic at CERN – 15 to 17 December

Risk Analysis

- Identified Security risks in 2 main categories
  - Intentional or malicious
    - sub-categories
      - Misuse of LCG resources, Confidentiality or Data Integrity, Disruption for political or other reasons, Other attacks
  - Non-intentional or accidental
- Quantified Likelihood and Impact
  - Both on scale of low, medium, high (1 to 3)
- Risk = likelihood * impact
- Will use these to guide work and developments over next 12 months
- Started to define course of action for highest risk items

Risk Analysis (2)



LCG Risk Analysis - 30 Oct 2003 (v2)

ID	Description	Risk Analysis				
		Likelyhood Avg	Likelyhood Stdev	Impact Avg	Impact Stdev	Computed Risk
Security Issues - Intentional or malicious attacks						
Misuse of LCG resources - CPU, storage, network etc						
M1	Resources used to launch online attacks on other sites via DOS, Virus, Worms, SPAM etc	3.0	0.0	3.0	0.0	9.0
M2	Resources used for offline attacks on other sites, e.g. to crack passwords or pass phrases	2.0	0.0	2.0	0.0	4.0
M3	Resources used to distribute or share non-LCG data, e.g. copyrighted, illegal,or inappropriate material	3.0	0.0	3.0	0.0	9.0
M4	Resources misused by inappropriate setting of access control or priority	3.0	0.0	1.0	0.0	3.0
M5	Use of LCG resources by unauthorized parties	3.0	0.0	1.0	0.0	3.0
M6	Use of LCG resources for unauthorized purposes, e.g. financial gain	2.0	0.0	2.8	0.5	5.5
Confidentiality and Data integrity issues						
C1	Theft of credentials, e.g. private keys	3.0	0.0	2.0	0.0	6.0
C2	Data or passwords/pass phrases exposed, e.g. in unprotected files or on the network	3.0	0.0	2.0	0.0	6.0
C3	Falsification of scientific data, analysis and/or results	1.8	0.5	3.0	0.0	5.3
C4	Unauthorized monitoring of network communications	2.0	0.0	2.0	0.0	4.0
C5	Unauthorized access to data	3.0	0.0	1.0	0.0	3.0
C6	Unauthorized distribution or exposure of data	2.8	0.5	2.0	0.0	5.5
C8	Identity or usage information is harvested by unauthorized persons	2.0	0.0	1.0	0.0	2.0
Disruption of LCG infrastructure for political or other reasons						
D1	Disruption via exploitation of security holes	3.0	0.0	3.0	0.0	9.0
D2	Corruption of or damage to data	1.0	0.0	2.8	0.5	2.8
D3	DOS attacks towards LCG to prevent normal working of network or services	1.8	0.5	3.0	0.0	5.3
D5	"Poisoned" resources are deployed on LCG to confuse operations, debugging or results	1.0	0.0	2.8	0.5	2.8
D6	Attack by disgruntled users, employees or ex-employees	1.0	0.0	3.0	0.0	3.0
D7	Use of "social engineering" methods to attack LCG resources	3.0	0.0	2.0	0.0	6.0
D8	Damage caused by viruses, worms, trojans or back-doors	3.0	0.0	3.0	0.0	9.0
D9	Misleading trouble reports to the GOC or incident response mechanisms, to disrupt operations or damage reputation	1.0	0.0	2.0	0.0	2.0
D10	Modification or defacement of User Interfaces, documentation, monitoring etc, for disruption or advertising	2.0	0.0	2.0	0.0	4.0
Other attacks						
O1	Theft of systems	1.8	0.5	1.3	0.5	2.2
O2	Theft of software	1.0	0.0	1.0	0.0	1.0
O3	Physical sabotage of systems	1.0	0.0	1.3	0.5	1.3
O4	Theft of primary or backup data media	1.0	0.0	2.8	0.5	2.8
Security Issues - Non-intentional or accidental						
	Unauthorized use resulting from insecure middleware or bad security					

Future plans (1)

- Must manage risks identified in Risk Analysis
  - We need secure middleware to protect resources
    - Design and implementations
  - Grid security relatively immature
  - Very important for production Grids
- Many of the policy and procedure documents are for LCG-1 (2003)
  - Need reviewing for 2004 and beyond
- Define plan for next 12 months
- User Registration, VO Management and AuthZ
  - Workshop at CERN 15-17 December 2003
    - Review status and make plans for 2004

Future Plans (2)

- Authentication issues
  - Must agree the future PMA bodies for CA's
    - EGEE likely to take over this role for Europe
    - Collaborate with GridPMA.org, TERENA and GGF
  - Online CA services, credential repositories
    - KCA, SLAC Virtual Smart Card, MyProxy, …
    - Need to define best practice and minimum standards
- Authorization developments
  - VOMS (EDG) to be implemented soon in LCG
    - Confirms membership of VO, groups, roles
  - local AuthZ (EDG LCAS/LCMAPS, US CMS VOX) and VOMS-aware services are needed
    - To give the experiments the functionality they require
- We have already achieved a lot for LCG-1
  - But much more work still required!