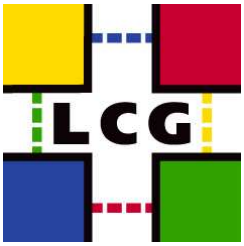

LCG Security Group

Agreement on Incident Response For LCG-1

Date:	**24th June 2003**
Version:	**1.1**
Status:	**Final**
Author:	**Dane Skow**

Document Log			
Issue	**Date**	**Author**	**Comment**
1.0	19 June 2003	Dane Skow	First circulation of this document format
1.1	24 June 2003	Dane Skow	Responses to comments. For 8 July GDB

1 Introduction

One of the consequences of engaging in the collaborative Grid computing is to accentuate the interdependence of various sites operations. It is considerably more likely that understanding events at one site requires information and collaboration from investigators at other sites. This document is intended to describe agreements on responsibilities and process for handling incidents in the LCG-1 Grid. We foresee a number of new connections and the need to establish the communications and follow-up channels required to deal with issues for LCG-1.

The general principles for incident response in the near term are that

1) the party discovering an incident is responsible for taking local action to prevent further disruption, and
2) that party is responsible for informing security personnel at all LCG-1 sites.

For users at LCG-1 sites, their responsibilities likely will be discharged by informing their site security officers. Initially the channel for informing all security personnel at participating sites will be via a common mailing list. As the grid operations concepts mature, it is expected that a catchall notification method will be developed for users without local security staff.

Below we try to outline a plan of action for the July rollout of LCG-1. There will certainly be modifications as we move toward the December production target. We should keep both targets in mind and address the immediate needs as best we can while identifying the areas that need work for production. Sections marked with red font are areas identified where coordination work is needed with groups beyond the LCG Security Group. In some cases, management structures need to be defined.

1.1 What is an incident ?

The definition of "incident" is not at all obvious, and will likely change over time as we gain experience. The proposed definition of incident is any of the following:

- any security investigation that causes a site to interrupt service (ie. disconnect a machine or bar a user)
- Any instance of suspected misuse of grid resources beyond the local site
- There is a reasonable possibility that credentials have been stolen and those credentials will not expire or be revoked within 3 days of the possible theft.

Incidents will be reported to project-lcg-security-csirts@cern.ch until an operations center is functioning.

Other events can be reported at the finding site's discretion. It is expected that, particularly in the early period, reports of the type "Hey, look what I found" will be educational and should be encouraged. They should clearly be tagged as INFORMATIONAL so that staff are not unnecessarily pulled out of bed, etc.

2 Communications

Users report incidents directly to the grid operations center or their local security personnel. Since it is unclear what, if any, operations center will be running in 2003, the presumption is the local security contacts will be the primary channel.

In the absence of an operational, trained, 24x7 operations staff, we'll use a mailing list consisting of all the incident reporting email addresses as the notification channel. This list is project-lcg-security-csirts@cern.ch.Use of the list will be open to any address from participating sites, but is expected to be limited to security personnel only. This list should not be generally advertised for user reports, for example, to avoid flooding.

A template incident report will be created for use by the reporting security staff and posted on the LCG security webpages at http://cern.ch/lcg-security/ so that common minimum information is captured in the report (contact information about the reporting party, IP address and names of involved machines, etc.). The involved sites will establish direct communications among the themselves, using whatever methods are appropriate for the incident. If secure communications are needed, they will be set up directly between the parties. Site security officers are encourage to maintain pre-established secure channels of communication.

Urgency and response time requirements are expected to be made clear by the person with the requirements. Otherwise, best effort will be assumed. Any party may request log extracts from any of the others.

The site maintaining the logs is expected to perform whatever data filtering or request verification is required by its own rules prior to data release. This protocol is expected to complete quickly and should not obstruct the investigation

3 Identity Theft

Grid credentials can be compromised in a number of ways and with varying degrees of certainty. It is expected that the reporting mechanisms are the same for all cases, but the investigation should distinguish between the following cases as soon as possible:

- Suspected cases (e.g. accessible private keys),
- Probable cases (e.g. cracked private key),
- Confirmed cases (e.g. unauthorized use).

Procedures need to be defined for the Operations Center follow-up required for each of the cases above. This will include informing incident response personnel at the LCG sites.

4 Misuse

The Grid Resource is expected to take whatever actions it deems necessary to protect its resources. This may include shutting off access to the identity associated with the unauthorized activity. Grid Resources observing misuse of other Grid resources initiated from within are expected to

disrupt that misuse (e.g. kill the local jobs carrying out the attack) and notify the attacked site. In both cases, the LCG-1 incident response list should be notified ASAP with details about the (suspected) misuse and actions taken

5 Enforcement

Sites who are victims of misuse may follow their own initiative for enforcing their usage policy. They may require some remedial action on the part of a user/site (e.g. complete some training), bar access for some period of time, or initiate prosecution through law enforcement channels. LCG sites and users will endeavor not to circumvent these enforcement mechanisms

Process and mechanisms for reporting breaches of the AUP to the VO and Grid managements and follow-up procedures needs to be defined—as do the management structures themselves.

6 Restoration

Sites may each set their own requirements for what is needed for restoration of access to their site. It is expected that cases of identity compromise that cannot be explained by the investigating site as resulting from innocent actions will require that the affected identities be replaced. Compromise of machines resulting in root/admin compromise require rebuilding the machine from a clean distribution unless secure change control logs (eg tripwire) are maintained. Compromise of a service key will require a new service key.

7 Escalation Procedures

A procedure for escalating issue resolution through the Grid management needs to be defined to settle cases where involved parties do not agree on resolution of an incident, or on matters of policy.

For the time being, the forum for dealing with incident response issues is a general discussion on the project-lcg-security-contacts@cern.ch mailing list. Issues that cannot be resolved there may be raised to the LCG Deployment Manager and/or to the Grid Deployment Board (GDB).

8 Approval by GDB

The LCG GDB is asked to do the following:

1. approve this incident response procedure as that to be used for LCG-1
2. Commit LCG-1 sites to work to this procedure, refining and improving it as experience guides
3. Work with operations and security groups to make sure noted procedures and agreements are developed.