Contribution ID: **132** Type: **poster**

The Grid Security Vulnerability and Risk Assessment activity EGEE-II.

Wednesday 9 May 2007 17:30 (20 minutes)

Describe the scientific/technical community and the scientific/technical activity using (planning to use) the EGEE infrastructure. A high-level description is needed (neither a detailed specialist report nor a list of references).

The Grid Security Vulnerability Group is composed of security experts in EGEE
drawn from many regions. The purpose of the activity is to find existing security
vulnerabilities in the deployed infrastructure, assess their risk and prioritize
their resolution.

Describe the added value of the Grid for the scientific/technical activity you (plan to) do on the Grid. This should include the scale of the activity and of the potential user community and the relevance for other scientific or business applications

The aim is to "incrementally make the Grid more secure and thus provide better
sustainability of the deployed infrastructure". This is to make sure the
infrastructure is available for legitimate users, and prevent its use or damage
by those who should not use it. The Grid has large resources and as such is an
attractive target for attack. This work is relevant to the user community
because users need to know what to do if they find, or suspect they have
found, a vulnerability within the Grid Middleware or deployment.

Report on the experience (or the proposed activity). It would be very important to mention key services which are essential for the success of your activity on the EGEE infrastructure.

We have setup a process for handling vulnerabilities, and a strategy for Risk
Assessments, along with the appropriate infrastructure. Issues of varying risk
have been effectively processed.

With a forward look to future evolution, discuss the issues you have encountered (or that you expect) in using the EGEE infrastructure. Wherever possible, point out the experience limitations (both in terms of existing services or missing functionality)

This activity needs to be publicised within both the user community and the sites, to ensure that issues found are handled by the appropriate process and resolved in a timely manner. Testing and code walkthroughs are another aspect of vulnerability detection, including attacks using automated tools. We also plan to provide guidelines for developers to help them avoid developing vulnerable software.

Author: Dr CORNWALL, Linda Ann (RAL)

Presenter: Dr CORNWALL, Linda Ann (RAL)

Session Classification: Poster and Demo Session

Track Classification: Poster session