Contribution ID: **41** Type: **oral presentation**

Security Incidents management in a Grid environment

Monday, September 3, 2007 2:20 PM (20 minutes)

Today's production Grids connect large numbers of distributed hosts using high throughput networks and hence are valuable targets for attackers. In the same way users transparently access any Grid service independently of its location, an attacker may attempt to propagate an attack to different sites that are part of a Grid. In order to contain and resolve the incident, and since such an attack may rapidly span many different administrative domains, efficient sharing of appropriate information between sites is important. Appointing an incident coordinator to obtain, correlate, filter and redistribute relevant information needed by sites in their local investigations has proven to be very effective to rapidly process the massive amount of data involved. Improving the trust between the site security teams, which may have different security standards, is an important factor in obtaining more relevant and accurate information. However, wider distribution increases the risk of voluntarily or involuntarily leaks of sensitive information outside of the community. Such leaks are not only dangerous because they may expose sensitive information, but also because they may discourage other sites from sharing their findings in the future. As a result, an essential part of the incident response relies on processes implementing appropriate and timely management and control of the information flow. This document describes the model adopted by the EGEE infrastructure, as well as issues encountered.

Submitted on behalf of Collaboration (ex, BaBar, ATLAS)

EGEE Operational Security Coordination Team

Primary author: Mr WARTEL, Romain (CERN)

Presenter: Dr SCHULZ, Markus (CERN)

Session Classification: Computer facilities, production grids and networking

Track Classification: Computer facilities, production grids and networking