Contribution ID: **92** Type: **oral presentation**

Addressing the Pilot Security Problem With gLExec

Thursday, September 6, 2007 4:50 PM (20 minutes)

Pilot jobs are becoming increasingly popular in the Grid world. Experiments like ATLAS and CDF are
using them in production, while others, like CMS, are actively evaluating them.

Pilot jobs enter Grid sites using a generic pilot credential, and once on a worker node, call home to fetch the job of an actual user.

However, this operation mode poses several new security problems when used in the traditional Grid environment:
- Executing the code of another user without authenticating and authorizing the end user violates the security policies of any site that requires full knowledge and control of all users of its resources.
- All processes run under the same UID, allowing a malicious user to steal the credentials of both the pilot and potentially any other user handled by the same pilot infrastructure.

To solve this problem, a site-trusted, and necessarily setuid utility is needed to authorize the end user and switch to the correct local UID.

gLExec is a Grid-aware suexec derivative, developed for EGEE by the NIKHEF group. Recently it has been integrated with the distributed OSG security infrastructure making it easy to deploy on OSG worker nodes.

The initial OSG deployment of gLExec on worker nodes has been completed at Fermilab and the CDF and CMS experiments have been actively using it for several months.

An architectural overview and the experience gathered will be presented.

Primary authors: YOCUM, Dan (Fermilab); VENEKAMP, Gerben (NIKHEF); SFILIGOI, Igor (Fermilab); KOEROO, Oscar (NIKHEF)

Co-authors: GROEP, David (NIKHEF); PETRAVICK, Don (Fermilab)

Presenter: SFILIGOI, Igor (Fermilab)

Session Classification: Computer facilities, production grids and networking

Track Classification: Computer facilities, production grids and networking