

Towards a Security Model to Bridge Internet Desktop Grids and Service Grids

Gabriel Caillat(1) , Oleg Lodygensky(1), Etienne Urbah(1), Gilles Fedak(2) , and Haiwu He(2)

(1)
Laboratoire de l'Accelérateur Lineaire,
Universite Paris Sud, Orsay
{gcaillat, lodygens, urbah}@lal.in2p3.fr

(2)
INRIA Saclay, LRI,
Universite Paris Sud, Orsay
{fedak, haiwu.he}@lri.fr

Europar / SGS 2008

Summary

- Service Grid and Desktop Grid Definitions
- Service Grid and Desktop Grids Security Models
- Bridging SG and DG
 - The SuperWorker approach
 - The Giding-in approach
- Bridging XtremWeb and EGEE
- Conclusion

Service Grids

- EGEE, NorduGrid, National Grid Service...
- Dedicated and known computing resources.
- High quality of service.
- High security (Authentication, Encryption)

- Difficult to join as resource and/or user

- Difficult to maintain

Desktop Grids

- BOINC, XtremWeb, Xgrid...
 - One of the largest distributed computing system
 - Anyone can join at any time
 - No special expertise to maintain
-
- Low Quality of Service
 - Low security, anonymous computing resources / users

Security Model of Service Grids

- Grid Security Infrastructure (EGEE)
- Secured authentication and communications
- based on:
 - public key encryption (auth. and com.)
 - X.509 certificates (auth.)
 - SSL (com.)
- Managed by trustable Certificate Authorities and VO Management Services.

Security Model of Desktop Grids

- **Boinc is asymmetric:**
 - Open to the web
 - Many anonymous volunteers must trust a few well known projects. Reverse is not true
 - Enforced by a private/public key to authenticate the project, jobs and results.
- **XtremWeb is P2P:**
 - Open to the web
 - Any participant can be user and/or volunteer
 - Unix like user rights/access rights and optional sandboxing to protect the platform
 - Enforced by private/public key to authenticate the coordinator
- **Xgrid is (too) easy:**
 - Optional single password for authentication

Bridging SG's and DG's

- Part of the EDGeS european FP7 infrastructure project
More information at www.edges-grid.eu
- Two main approaches:
 - The Superworker
 - The Gliding-in

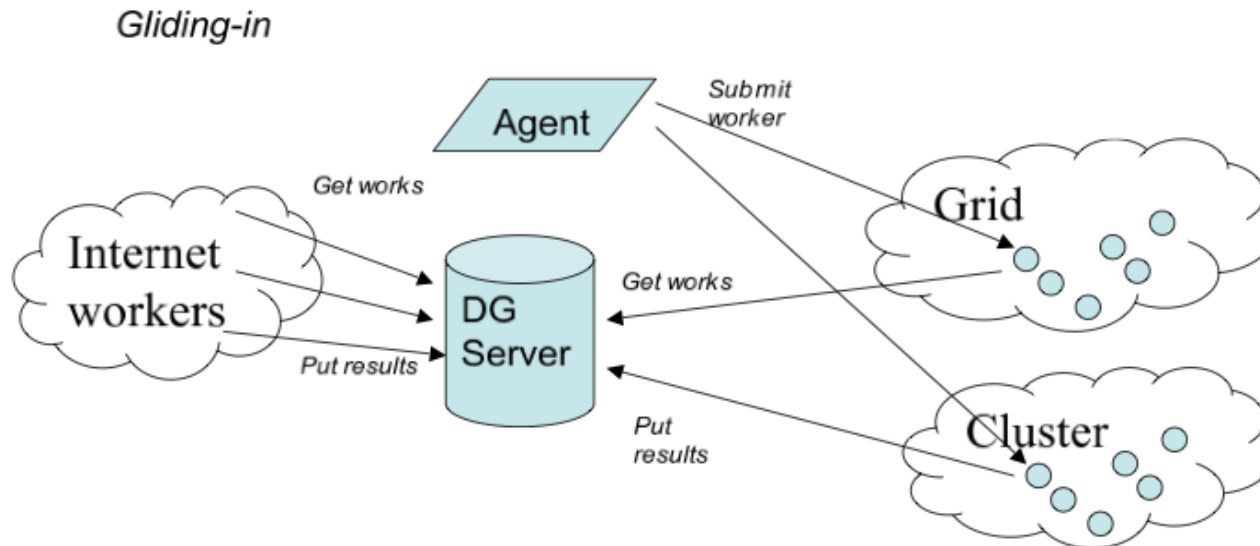
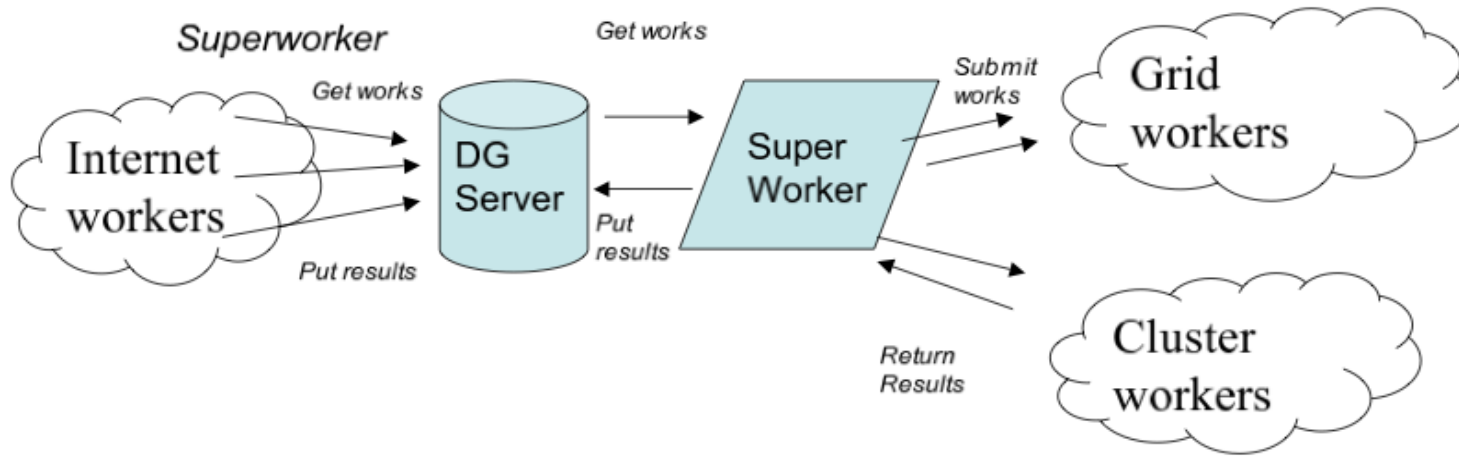
Bridging SG's and DG's

- The superworker approach:
 - proposed by the Lattice project and the SZTAKI Desktop Grid
 - is a centralized agent between DG and SG.
 - can be considered as a scheduler by itself
- It does not requires modification of the infrastructures
- Jobs are wrapped and then run on the grid with the good user id
- Since it's centralized, it can be a bottleneck
- Round trip per work unit is increased
- Single and low fault-tolerant point of failure

Bridging SG's and DG's

- The Gliding-in approach (aka Pilot Job):
 - Consist in running the DG worker on the SG as a regular task
 - At execution time, worker pulls and execute a job from DG server
 - It then returns the results to the DG server
 - can be considered as a scheduler by itself
- Load is balanced between grids
- Fault tolerant
- Performant due to direct link between DG server and SG computing element
- Pilot job owner may be different from final job owner.
It then breaks grids security rules

SuperWorker VS Gliding-in



Bridging XtremWeb and EGEE

- How to aggregate EGEE worker nodes in a XtremWeb platform?
- XtremWeb responsible for user authentication and workers integrity
- XtremWeb responsible for secured communications
- XtremWeb responsible for applications and results integrity
- XtremWeb responsible for logging

Bridging XtremWeb and EGEE

- The Gliding-in technology has been preferred
- XtremWeb server must have a valid certificate
- Authentication ensured by:
 - user registration by XtremWeb coordinator
 - X.509 certification system integrated in XtremWeb
- Only users with a valid certificate may run jobs on EGEE
- XtremWeb worker software is submitted to EGEE using JSDL wrapper, and comes with a proxy of the user's certificate
- EGEE computing nodes integrity is ensured by the XtremWeb sandboxing features

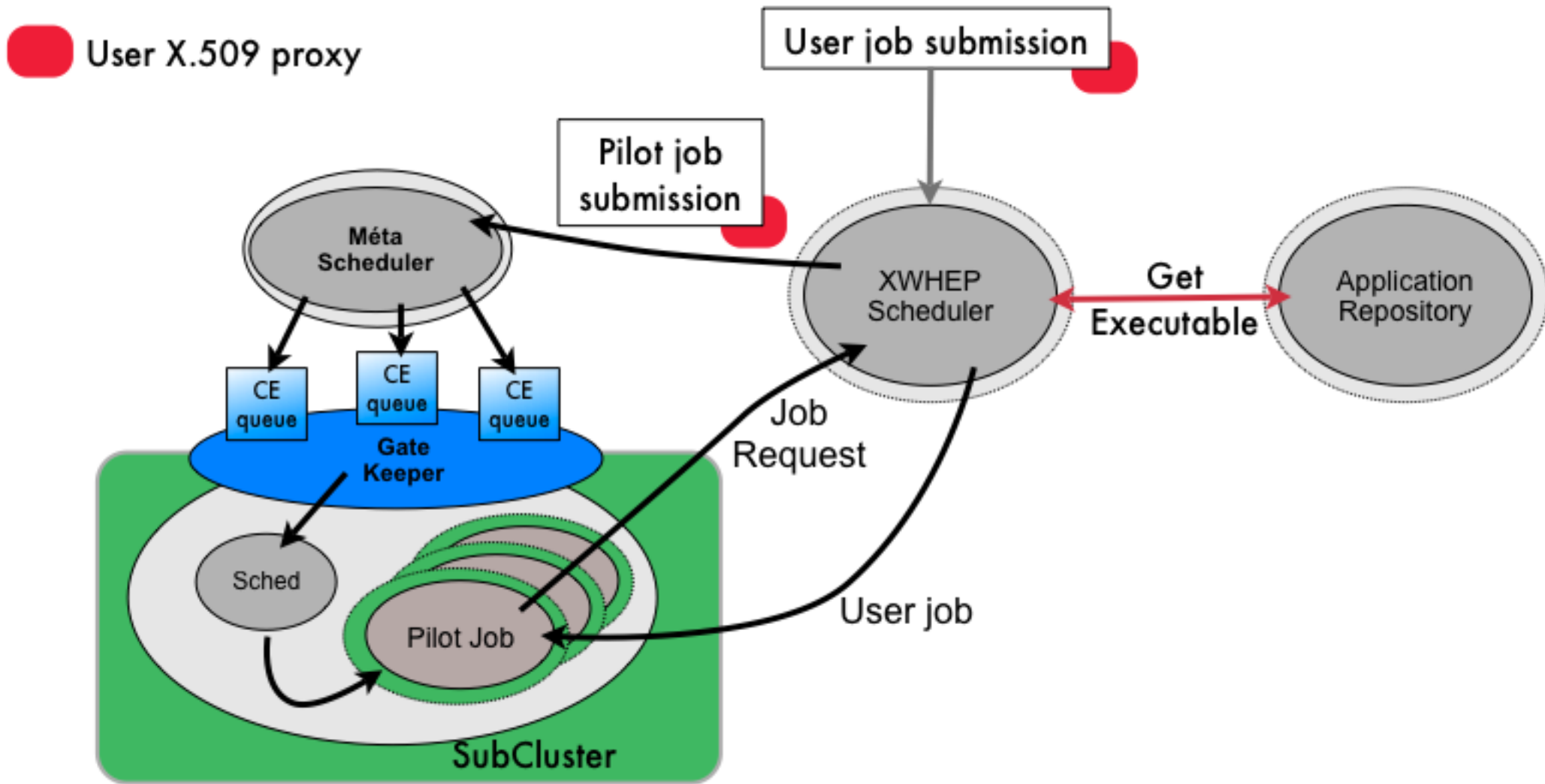
Bridging XtremWeb and EGEE

- Applications, parameters and results are secured:
 - Inside XtremWeb thanks to its user rights and access rights management system
 - Inside EGEE thanks to the central coordinator
- Outside, while transfer between the domains, security is ensured by:
 - encryption through SSL tunnels
 - workers connect to coordinator for which they have the public key
- This prevents from:
 - malicious persons that try to intercept and read connections
 - malicious persons to connect to coordinator
 - EGEE worker nodes to connect to a wrong coordinator

Bridging XtremWeb and EGEE

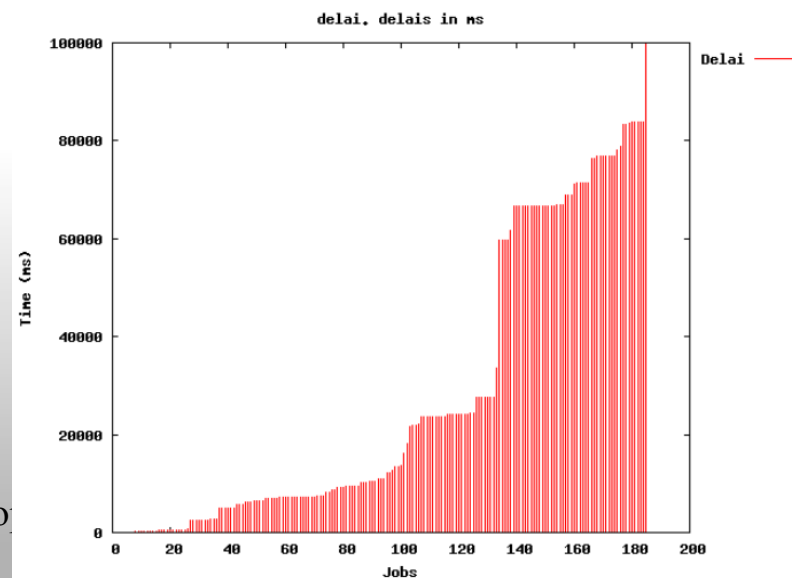
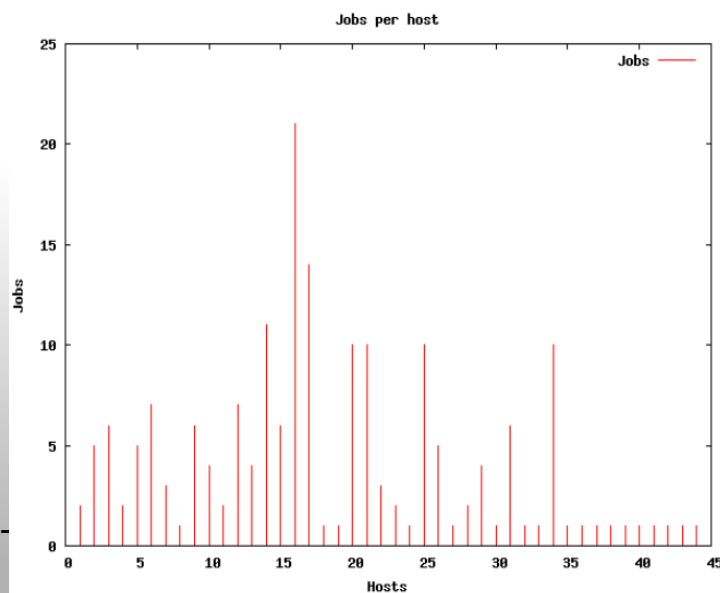
- XtremWeb ensures its own security
- EGEE security level is achieved by user authentication, X.509 certification and sandboxing.
- Applications, parameters and results are secured by:
 - XtremWeb user rights and access rights systems
 - Secured communications

Pilot Job Mechanism



XtremWeb to EGEE Performances

- 185 tasks sent to an XtremWeb platform of 34 volunteer PC's and 10 EGEE worker nodes
- Good distribution of the jobs among ressources
- Execution time depends on type of available ressources (OS, CPU...)



Conclusion

- Gliding-in model may stress SG and DG security requirements
- Our implementation fills these gaps:
 - Anonymous users are segregated from certified ones
 - High security level for both the EGEE grid and volunteer PC's

Thank you...

