Securing Grid Workflows with Trusted Computing
(Extended Abstract)

Po-Wah Yau*, Allan Tomlinson*, Shane Balfe†, Eimear Gallery‡

Information Security Group, Royal Holloway, University of London,

Egham, Surrey, TW20 0EX, UK

{p.yau, allan.tomlinson, s.balfe, e.m.gallery}@rhul.ac.uk

The Grid, a distributed computing paradigm, seeks to exploit the synergies of technology and social collaboration to solve data or computation-intensive problems. Solving such problems requires the management of multiple tasks, their relationships and execution to produce valid and reliable results — this is the focus of Grid workflow research [2]. The risk to a user's data and results is dramatically increased when using workflows, because the entire dataset is exposed to the Grid.

The use of reputation and provenance information has been proposed to avoid selecting 'untrusted' nodes when provisioning Grid jobs. However, this information may be unreliable or open to manipulation. We propose a scheme [3] that uses trusted platforms that are compliant with the Trusted Computing Group specifications. We make use of integrity measurement, sealing and platform attestation [1] to provide the following security services to Grid workflows: trusted resource provider selection, confidentiality of job information, integrity of job information, and audit data for process provenance.

Trust in a Workflow Resource Broker (WRB) is critical, as it is relied upon by a user to ensure that their workflow will be executed as expected, and thus produce valid results. A Resource Broker Verification Service (RBVS) is used by a Grid user to select a trusted WRB. Platform attestation may be used by the RBVS to evaluate trust in a WRB.

A workflow of Grid tasks is then created by a Grid user and is submitted to a WRB along with a security policy. The WRB maps the tasks to jobs for submission to resource providers that meet the user's security requirements. The WRB generates certifiable migratable key pairs where the use of each private key is contingent upon a platform state that reflects these requirements. Each private key is migrated to a resource provider. The corresponding public keys are used to encrypt unique symmetric keys, which in turn are used to protect the confidentiality and integrity of Grid jobs submitted to chosen resource providers. A similar method is used to protect intermediate data between resource providers processing consecutive jobs. In addition, platform attestation is used by resource providers to ensure that the previous job in the workflow was executed correctly. Full details and an analysis of the scheme can be found in [3].

References

[1] C. J. Mitchell. *Trusted Computing*, volume 6 of *IEE Professional Applications of Computing*. IEE Press, London, 2005.

[2] I. J. Taylor, E. Deelman, D. B. Gannon, and M. Shields, editors. *Workflows for e-Science: Scientific Workflows for Grids*. Springer, 2007.

[3] P. Yau, A. Tomlinson, S. Balfe, and E. M. Gallery. Securing grid workflows with trusted computing. In *Proceedings of the 8th International Conference on Computation Science (ICCS '08), Krakow, Poland, June 23–25, 2008*. Springer-Verlag LNCS, to appear, June 2008.