Fine-Grain Access Control for Securing Shared Resources in Computational Grids

Ali Raza Butt, Sumalatha Adabala, Nirav H. Kapadia
School of ECE, Purdue University, W Lafayette, IN 47907
{butta, adabala, kapadia}@purdue.edu

Renato Figueiredo
Dept. of ECE, Northwestern University, Evanston, IL 60208
renato@ece.nwu.edu

Josè A. B. Fortes
Dept. of ECE, University of Florida, Gainesville, FL 32611
fortes@ufl.edu

Computational grids provide computing power by sharing resources across administrative domains. This sharing, coupled with the need to execute untrusted code from arbitrary users, introduces security hazards. This paper addresses the security implications of making a computing resource available to untrusted applications via computational grids. It highlights the problems and limitations of current grid environments and proposes a technique that employs runtime monitoring and a restricted shell. The technique can be used for setting-up an execution environment that supports the full legitimate use allowed by the security policy of a shared resource. Performance analysis shows up to 2.14 times execution overhead improvement for shell-based applications. The approach proves effective and provides a substrate for hybrid techniques that combine static and dynamic mechanisms to minimize monitoring overheads.

Key Phrases: access control, grid environments, grid security, Unix access model.