Chapter IX
Trust and Privacy in Grid Resource Auctions

Kris Bubendorfer
Victoria University of Wellington, New Zealand

Ben Palmer
Victoria University of Wellington, New Zealand

Ian Welch
Victoria University of Wellington, New Zealand

ABSTRACT

A Grid resource broker is the arbiter for access to a Grid’s computational resources and therefore its performance and functionality has a wide-ranging influence on the utilization and performance of the Grid. Ideally, we want to avoid relying on a single ‘trusted’ resource broker because it may not be trustworthy. For example, a broker holding a resource auction could examine and reveal bid information to others, or defraud participants by subverting the auction results. The use of privacy preserving and verifiable auction protocols offers guarantees beyond those possible in real world auctions, making the electronic auctions as secure, or more secure, than their physical counterparts. In this chapter, we provide the background to understand privacy preserving and verifiable auction schemes and discuss the implications of adopting them on Grid architecture. We then evaluate a range of potential secure auction schemes and identify those that are most suitable to be adopted within for use in the Grid.

INTRODUCTION

One of the vital components of any Grid computing infrastructure is the resource broker. A Grid resource broker is the arbiter for access to a Grid’s computational resources and therefore its performance and functionality has a wide-ranging influence on the utilization and performance of the Grid. Market based mechanisms, such as auctions, have often (Buyya, Abramson, Giddy,
and Stockinger, 2002; Bubendorfer, Komisarczuk, Chard, and Desai, 2005; Chien, M., and W., 2005) been promoted as a solution for scalable resource economies because they are naturally decentralized, efficient and produce optimal allocations. Another advantage of such market-based mechanisms is that they are a natural fit with the principles of Utility computing (Eerola et al., 2003; Komisarczuk, Bubendorfer, and Chard, 2004) and efforts towards Grid commercialization (Dimitrakos et al., 2003; Graupner, Kotov, Andrzejak, and Trinks, 2003).

Ideally, we want to avoid relying on a single ‘trusted’ resource broker because it may not be trustworthy. For example, a broker holding a resource auction could examine the bids and reveal this information to others, or defraud participants by subverting the auction results. However, we can protect bid values by using a privacy preserving auction scheme. Fraud can be prevented by adding a verification protocol to the auction. The use of privacy preserving and verifiable auction protocols offers guarantees beyond those possible in real world auctions, making the electronic auctions as secure, or more secure, than their physical counterparts. The use of privacy preserving and verifiable auction protocols enables the construction of open and user centric Grid architectures. Indeed, it is possible to imagine such market oriented technologies underpinning peer based user-centric Grid communities, in which users can contribute and consume computing power on demand, purchase services and collectively provide the computing infrastructure.

In this chapter, we provide the background to understand privacy preserving and verifiable auction schemes and discuss the implications of adopting them on Grid architecture. We then evaluate a range of potential secure auction schemes and identify those that are most suitable to be adopted within for use in the Grid.

BACKGROUND

Auctions are favored as an efficient solution to the challenge of distributed resource allocation in both economic (Buyya et al., 2002; Bubendorfer et al., 2005; Chien et al., 2005) and can also be successfully applied in noneconomic (Malone, Fikes, Grant, and Howard, 1988) resource allocation systems. There are four main types of auction protocol; the English, Dutch, Sealed-Bid, and what has since become known as the Vickrey auction protocol. The English auction is the conventional open outcry, ascending price, multiple bid protocol. The Dutch auction is an open outcry, descending price, single bid protocol. The Sealed-Bid, or tender, is a sealed single bid, best price (1st price) protocol in which all bids are opened simultaneously. The Vickrey auction is similar to the Sealed-Bid auction, except that the winning bidder pays the amount of the second bid (2nd price). The second price bid mechanism results in a dominant strategy of truthful bidding in private value auctions, that is, bidding your true value will always give the best return regardless of other bidders strategies. It is worth noting that the revenue equivalence theorem states that all of the four main auction protocols return the same revenue in private value auctions (Vickrey, 1961), hence the selection of an auction protocol usually depends on implementation pragmatics such as messaging requirements.

When it comes to computational auctions however, it may not be possible to achieve QoS goals with a single representative good as the basis for resource allocations. Execution resources form an indivisible set, related and conditional upon the availability of each other. Game theorists term this as the combinatorial allocation problem (CAP) (Rothkopf, Pekec and Harstad, 1995), in which a set of components have a synergistic value that exceeds the sum of the individual parts. Because of preferential combinations and possible substitutions, bidders have preferences