Chapter 18
Sealed-Bid Auction Protocols

Kun Peng
Institute for Infocomm Research, Singapore

ABSTRACT

In the Internet era electronic commerce is an important and popular industry. Electronic auctions provide a key function in e-commerce, enabling effective and fair distribution of electronic as well as non-electronic goods. Like other fields of e-commerce, e-auctions face serious security threats. Fraud can be committed by bidders or auctioneers. Most popular Internet auctions sites use an open-cry bidding process. This can add excitement to an auction in progress and possibly encourage new bidders to join an auction. However, there are serious difficulties in maintaining the security requirements often required in commercial auctions, particularly in terms of protecting bid confidentiality and bidder privacy. Additionally, some of the current auction techniques are interactive and require many rounds of communication before completion so that more time is required to determine the final winning price. Intensive communication over the insecure Internet is also a problem from the perspective of availability of service and network security. For these reasons most recent research in this area has concentrated on sealed-bid auctions. Sealed-bid auctions are the focus of this chapter. In this chapter, security requirements in e-auction including correctness, fairness, non-repudiation, robustness, public verifiability, bid privacy, and other desired properties like price flexibility and rule flexibility are introduced. The existing approaches to realize them are investigated. The authors show that the key requirement is bid privacy and the main challenge to the design of an e-auction is how to protect bid privacy without compromising other requirements and properties. Techniques to achieve bid privacy are presented in this chapter according to different application environments.

DOI: 10.4018/978-1-4666-4030-6.ch018

Copyright © 2013, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.

INTRODUCTION

The sealed-bid auction has been a useful tool to distribute resources for many years. It usually contains four phases. Various sealing functions may be used to seal the bids and keep them secret before they are opened. Different auction rules may be used.

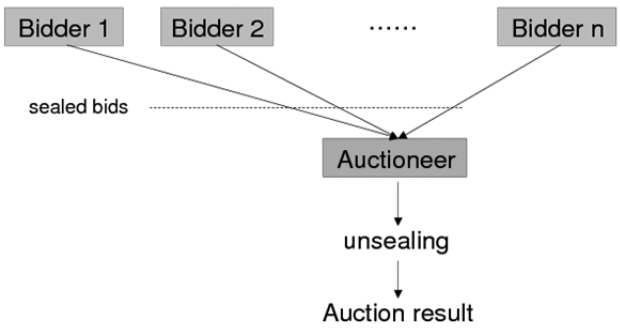
Auctions have a long history since 500 B.C., when Herodotus reported the use of an auction (Cassady, 1967). Auction was frequently used to liquidate property and estate goods during the Roman Empire (Cassady, 1967). They are an effective method to distribute goods fairly. In the traditional auction systems both the open cry auction, such as English auction and Dutch auction, and the sealed bid auction have been widely used. In the open cry auctions, the bids are cried out openly and the bidder with the highest bid win. If each time a bidder cries out a new bid higher than the last one, it is called English auction. If the auctioneer cries out the bids from the highest possible price one by one until a bidder accept the current bid, it is called Dutch auction. In a sealed-bid auction, a bidder has to submit a sealed bid before a closing time. After the closing time one or more auctioneers open the bids to decide the winners according to a pre-defined rule. Sealed-bid auction is illustrated in Figure 1 to including at least two phases, the bidding phase when the bids are sealed and the bid opening phase when the bids are opened.

In the Internet era electronic commerce is an important and popular industry. Electronic auction is a key function in e-commerce and can be used to distribute electronic as well as non-electronic goods effectively and fairly. Although still at its early stage, e-auction is developing fast. Internet auctions accounted for approximately $3 billion in sales in 1999 and have grown significantly to $15 billion in sales for the year 2002 (Prevention & Division, 2003). The most famous e-auction website, e-bay, has more than two million visitors a day. In a network environment, sealed-bid auction is preferred not only because of its convenience and quickness but also because of its potential ability to protect bid confidentiality and bidders' privacy.

The players in an auction include:

- Seller, who has one or more items (also called goods) to sell;
- Bidder, who submits a bid (the highest price he is willing to pay);
- Auctioneer, who acts on behalf of the seller to determine a winning price (clearing price) and a bidder as the winner.
- Winner, the bidder chosen by the auctioneer(s) to pay the seller the clearing price and get the goods.

Figure 1. Sealed-bid auction



37 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/sealed-bid-auction-protocols/76526

Related Content

Semantically Secure Classifiers for Privacy Preserving Data Mining
Sumana M., Hareesha K. S.and Sampath Kumar (2021). *Research Anthology on Privatizing and Securing Data (pp. 1066-1095).*
www.irma-international.org/chapter/semantically-secure-classifiers-for-privacy-preserving-data-mining/280217

Assessing the Security of Software Configurations
Afonso Araújo Netoand Marco Vieira (2012). *Threats, Countermeasures, and Advances in Applied Information Security (pp. 129-157).*
www.irma-international.org/chapter/assessing-security-software-configurations/65766

Identity-Based Encryption Protocol for Privacy and Authentication in Wireless Networks
Clifton Mulkeyand Dulal C. Kar (2014). *Network Security Technologies: Design and Applications (pp. 129-155).*
www.irma-international.org/chapter/identity-based-encryption-protocol-for-privacy-and-authentication-in-wireless-networks/105806

An Iterative CrowWhale-Based Optimization Model for Energy-Aware Multicast Routing in IoT
Dipali K. Shende, Yogesh S. Angaland S.C. Patil. (2022). *International Journal of Information Security and Privacy (pp. 1-24).*
www.irma-international.org/article/an-iterative-crowwhale-based-optimization-model-for-energy-aware-multicast-routing-in-iot/300317

Detection of Drive-by Download Attacks Using Machine Learning Approach
Monther Aldwairi, Musaab Hasanand Zayed Balbahaith (2017). *International Journal of Information Security and Privacy (pp. 16-28).*
www.irma-international.org/article/detection-of-drive-by-download-attacks-using-machine-learning-approach/187074