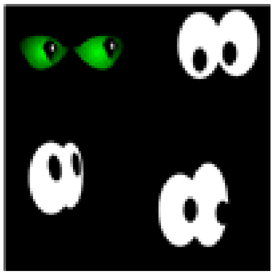
Crossroads
The ACM Student Magazine



Security, Anonymity and Trust in Electronic Auctions

by ***Jarrod Trevathan***

Introduction

Auctioning items over the Internet is a popular and lucrative industry.There are now many companies that conduct auctions online such as *eBay* [**5**] and *onSale* [**10**]. Online auctions have geographical advantages over traditional auctions as buyers and sellersare not required to be physically present at a central location (such as a hall or open air venue).This allows online auctions to be much larger and more elaborate than traditional auctions.However, it also provides opportunities for the auction participants to cheat.

A bidder can cheat by repudiating bids, failing to pay, or colluding with other bidders to affect the settlement price.Likewise, the seller of the item might fail to deliver the goods, or could be in collusion with some of the bidders.Someone could also forge a bid in an attempt to frame a bidder, or introduce fake bids in order to influence the auction proceedings.

Furthermore, bidders are required to trust the auctioneer with their identity and bid information.A corrupt auctioneer could award the auction to someone other than the legitimate winner.A bidder's personal information could also be sold to marketing agencies, or used for malicious purposes.

Commercial auction sites fail in many of the aforementioned circumstances. These sites only offer basic solutions that are designed to "clean up" after wrongdoing has taken place.However, cryptography can be used to solve some of these problems up-front.An "electronic auction" is a cryptographic scheme designed to securely conduct auctions while protecting the identitiesof the bidders.

In this article we describe two popular types of electronic auctions. We discuss the security issues associated with conducting these auctions and contrast the differing anonymity requirements.We also identify four main strategies for reducing the trust that bidders must place in the auctioneer.Furthermore, we present a basic example of an electronic auction scheme.This is used to illustrate the complexity involved in designing a secure and anonymous auction scheme.Finally, we discuss some of our research with regard to using group signature schemes to constructelectronic auctions.

Types of Auctions

The first known auctions were conducted in Babylon circa 500 BCwith the dubious application of auctioning women for marriage.The idea was extended to various goods and services in Ancient Rome [**4**].There are now a variety of auction types that have evolved to suit differing needs and applications.

The most well known auction is the *English auction*.This type of auction is commonly used in Real Estate where a bidder attempts to outbid all other bidders.The winner is the bidder with the highest bid andthey must pay an amount equal to this bid.An English auction is referred to as an *open* bid auction because everyone knows the amount that a bidder has bid.

A *Vickrey auction* is a lesser-known auction where bid amounts remain *sealed*, meaningno one knows the value of anyone else's bid.Vickrey auctions were invented in 1961 by Nobel Prize winner William Vickrey [**14**].A Vickrey auction consists of two stages: bidding and opening.During the bidding stage, bidders seal their bid (e.g., place it in an envelope) and submit it to the auctioneer.During the opening stage, the auctioneer opens all of the bids and determines the winner.The winner is the bidder with the highest bid.They are required to pay an amount equal to the second highest bid (i.e., the highest losing bid).

Vickrey auctions are popular in cryptographic research as they are less complicated to model compared to English auctions.This is because English auctions require a real-time communication channel between the auctioneer and bidders for price updates and winner determination.Vickrey auctions, on the other hand, only require a bidder to send a single message to the auctioneer.

Security

Online auctions are inherently insecure due to geographical scale and lack of accountability.Since participants are not physically present at the auction proceedings there are opportunities to cheat.For example, bidders can repudiate or forge bids and sellers might not deliver goods. Furthermore, the auctioneer could be corrupt.Auction security has been studied extensively in literature [1, 2, 6, 7, 8, 9, and 13].The primary goal of an electronic auction scheme is to ensure that the auction outcome is computed fairly.To understand the issues involved, we first review some problems encountered by traditional auctions and then examine various solutions employed by existing commercial auction sites.

Some problems with traditional English and Vickrey auctions include:

- **Shielding:** A bidder places an artificially high bid which is subsequently withdrawn just prior to the bid close time.This can have the effect of deterring other bidders with lower valuations from bidding.When the bid is withdrawn, the bidder may have another lower bid ready to win at the deflated price.
- **Shilling:** A bidder, or group of bidders (called shills), collude to artificially inflate the clearing pricefor the seller. If one of the shills accidentally wins, the item is resold in another auction.
- **Sniping:** A bidder refrains from making a bid until just prior to the bid close time. When the bid is made it is usually done so in a manner that does not allow any other bidder to respond in time.
- **Siphoning:** A non-participant observing an auction makes a lower offer directly to a bidder.The non-participant avoids the costs and risks associated with conducting an auction.
- **Misrepresented or non-existent items:** A seller might make false claims about the item for sale, or attemptto sell an item they do not have.

In an attempt to reduce these problems, existing commercial online auction sites offer remedies such as legislation and incentives.Firstly, laws can be made with regard to breaking the rules.For example, defaulting on payment could result in a fine and/or jail sentence.Another solution is to provide an incentive scheme to reward people that follow the rules.For example, eBay [5] offers a feedback system that allows buyers and sellers to create profiles about each other based on previous dealings.Anyone can view these profiles before engaging in business with the individual.A buyer or seller with a shady reputation can also be blacklisted from future auction proceedings.

Other solutions involve credit card registration, escrow services and insurance.Credit card registration can be used as both proof of identity and security for payment.In a similar manner, escrow services require all bidders to keep payment in escrow (security), which is either refunded or deposited depending on the auction outcome. Alternately, insurance can be offered to participants in situations where they suffer loss as a result of unfair behavior.However, none of these solutions is perfect.

Electronic auctions seek to use cryptographic protocols to enforce security and protect anonymity.This is done by constructing auction schemes from cryptographic building blocks such as encryption,digital signatures, secret sharing, and digital cash.First the basic components of an electronic auction scheme must be described.

There are several main activities (or stages) fundamental to an electronic auction protocol:

- **Initialization:** The auctioneer sets up the auction and advertises it (i.e., type of good, starting time, etc.).
- **Registration:** In order to participate in the auction, bidders must first register with the auctioneer (or a registrationmanager).This ensures that only valid bids are made and that bidders can be identified for payment purposes.It is desirable for registration to be a one-off procedure.Once a bidder has registered they should be able to participate in any number of auctions rather than re-registering for each new auction.
- **Bidding:** A registered bidder computes his/her bid and submits it to the auctioneer.The auctioneer checks the received bid to ensure that it conforms to the auction rules.
- **Winner Determination:** The auctioneer determines the winner according to the auction rules.It is desirable for this process to be publicly verifiable.

The following outlines the main security goals for electronic auction schemes:

- **Un-forgeable bids:** Bids must be un-forgeable, otherwise a bidder can be impersonated.
- **Non-repudiation:** Once a bidder has submitted a bid they must not be able to repudiate having made it.For example, if a bidder wins and does not want to pay, they might deny that they submitted the bid.
- **Publicly verifiable:** There must be some publicly available information by which all parties can be verifiedas having correctly followed the auction protocol.This should include evidence of registration, bidding, and proof of winner/loser.
- **Robustness:** The auction process must not be affected by invalid bids or by participants not correctly following the auction protocol.
- **Efficiency:** Efficiency issues also play a large role in the practicality of electronic auction schemes.Factors that influence the efficiency of a scheme include the computational and communicationoverhead required for registration, signing a bid, verifying a bid and winner determination.

Many of the schemes proposed in literature fail to achieve the basic security goals or are too inefficient to be practical. Furthermore, some schemes reveal too much information about a bidder, including his/her identity and bidding history.

Anonymity

A major problem with existing commercial auction sites is that there is no means to protect a bidder's identity.For example, the auctioneer knows everything about a bidder including his/her identity and the values of the bidshe/she submits.This is undesirable as such information can be used to target a bidder with unsolicited junk mail or for more malicious purposessuch as bid shielding.

There are varying levels of anonymity depending on whether the auction is English or Vickrey.However, the main objective for anonymity in an electronic auction scheme is:

> *To conceal the bidder-bid relationship so that no bidder can be associated with the bid they submit.*

Anonymity is often achieved by issuing bidders with a pseudonym (fake identity) that they can use to submit bids.Consider the following scenario for example:A bidder must register with two registration managers, denoted as RM1 and RM2 respectively.RM1 knows the bidder's real identity and issues the bidder with a certificate.The bidder presents this certificate to RM2.RM2 trusts the certificate and provides the bidder with a pseudonym that can be used when bidding.RM1 knows the bidder's identity, but not the corresponding pseudonym.RM2 knows the bidder's pseudonym, but not his/her identity.Here the bidder remains anonymous as long as RM1 and RM2 do not collude.

However, anonymity is at odds with non-repudiation.If an auction were completely anonymous, bidders would be able to repudiate bids as there is no way to tellwho submitted what bid.Therefore, it is desirable to have a mechanism to trace bidders in the event of a dispute.This can be thought of as an "identity escrow" scheme where an authority has the power to reveal the identity of who submitted the bid in question. In the example above, RM1 and RM2 could be called upon, under special circumstances, to reveal a bidder's identity bycombining their information.

Further anonymity issues include:

- **Confidentiality:** In a Vickrey auction once a bid has been sealed, it must remain sealed until the winner determination stage of the auction.
- **Privacy of losing bids:** In a Vickrey auction, the values of the losing bids must be kept secret (however,most schemes leak bid statistics).Further questions also arise over how much information is disclosed regarding the winner and winning bid.For example, should only the seller and winner know the amount of the winning bid?What information should the auctioneer learn about winning/losing bids?
- **Un-linkable bidding:** The auctioneer should not be able to learn information about individual bidders based onprevious auctions conducted.This information could be used in future auctions in a manner that disadvantages the bidder. Consider the following scenario in a Vickrey auction:a bidder (denoted by B1) submits a bid for $100.The second highest bid is $50, so B1 wins and has to pay only $50.In a future auction, B1 again bids $100 and again the second highest bid is $50.Since the auctioneer knows B1's valuation, the auctioneer enters a bid for $99.B1 wins and must pay $99. In doing so, the auctioneer has increased the auction's revenue by $49.

> In an English auction [9], linkable bidding within an auction is acceptable, as it is common for severalbids to come from one particular bidder.For example, two bidders might engage in a rally attempting to outbid each other.Observers and participants of an auction often gain entertainment value from watching the parties involved in such rallies.However, linking bids between subsequent auctions is not desirable.An auctioneer who knows the valuation of a bidder might set a higher reserve (minimum winning) price in future auctions involving that bidder.

The need for anonymity in a scheme must be weighed against the goals and purpose of the scheme.Too much anonymity allows bidders to repudiate bids, whereas not enough anonymity allows bidders to be profiledand cheated by the auctioneer.To help with issues of security and anonymity, it is therefore desirable to reduce the level of trust a bidder must place in the auctioneer.

Trust

A significant problem in electronic auction protocols is how to protect bidders from a corrupt auctioneer.A malicious auctioneer might influence the auction proceedings in a manner inconsistent with the auction rules.For example, the auctioneer might choose to block bids, insert fake bids, steal payments, profile bidders, open sealedbids prior to the opening stage, or award the item to someone other than the legitimate winner. Furthermore, there may be collusion between the auctioneer and some of the bidders (similar to shilling).

In general, all electronic schemes in literature can be classified according to how they deal with the trust problem.The following approaches to reducing the trust bidders place in the auctioneer have been identified:

Trusted Third Party

Since the auctioneer is a beneficiary, the assumption that he/she follows the auction protocol may not be realistic.An alternative could be that the bidder and the auctioneer provide a *trusted third party* (TTP) with informationso that when there is a dispute the TTP can be called upon to resolve the altercation.However, such a setup requires all parties to have confidence in the TTP.This essentially means that the bidders trade one evil for another.Furthermore, the TTP is an attractive security target and a bottleneck [9].

Threshold Trust

Threshold trust schemes protect against a corrupt auctioneer by distributing the role of the auctioneer across *n* servers.The auction can be considered secure/fair unless a threshold *t*, of the auction servers collude (where $t < n$).Threshold trust, however, requires much communication between bidders and the auction servers, as well as between theauction servers themselves [6].

Two-Server Trust

It can be argued that threshold trust is not effective, since collusion among auctioneer servers is beneficial to the whole group of auctioneers.An alternative approach is to split trust up among two servers owned by separate entities.Here the auction result can be trusted as long as the two entities do not collude.Two-server trust schemes effectively reduce the communication overhead involved in threshold trust schemes and thus far havealso proved to be computationally efficient.However, if one of the two servers decide not to co-operate, then the auction outcome cannot be determined. We will give an example of a two-server trust scheme in the next section [7, 13].

Distributed Bidder Trust

In this approach the auctioneer is not used.Instead, the bidders jointly compute the auction outcome.The merit of such an approach is that collusion amongst bidders is prevented unless all bidders are corrupt, which negatesthe reason for colluding in the first place.However, the downfall of this approach is that **all** bidders must participate during the winner determination stage. This is not reasonable, as when the number of bidders is large (e.g., several hundred) it would be virtually impossible to arrange a time for all bidders to be available to calculate the winner.Furthermore, if just one bidder decides not to participate, the auction outcome cannot be determined.In addition, much communication is required between bidders during the bidding and winner determination stages [1].

Example Electronic Auction

In this section, an English auction scheme based on two-server trust is presented.Note that this example fails some of the security and anonymity criteria stated earlier.It merely serves as an example to highlight the main issues associated with constructing a secure and anonymous electronicauction scheme.

In this example, there are three main parties involved: the bidders, two registration managers (RM1, RM2), and an auctioneer. The auctioneer controls a public bulletin board to which it writes the auction results.All parties can verify the auction proceedings via the bulletin board.Bulletin boards are used in many schemes proposed in literature (see [9, 13]).It is assumed that auction participants use a public key cryptosystem.

Initialization: The auctioneer sets up the auction. The auctioneer and the two registration managers publish their public keys.

Registration: Figure 1 illustrates the process involved in registration.

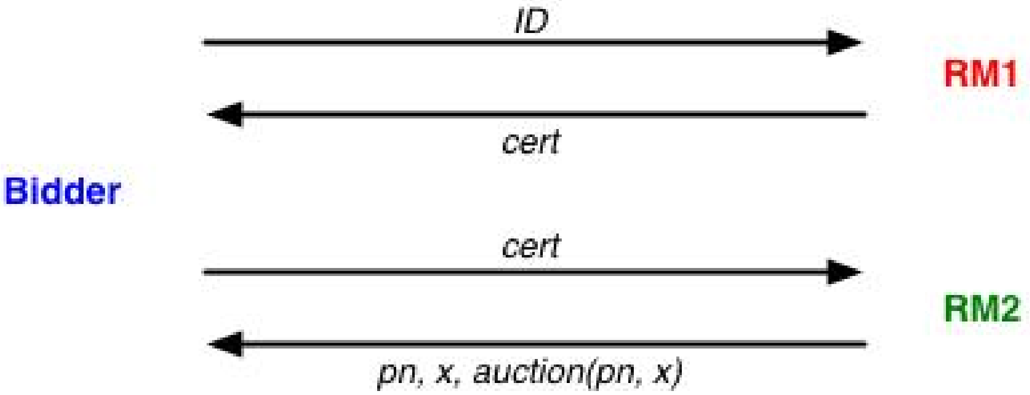


Figure 1: Registration.

1. A bidder registers his/her identity *ID* with RM1
2. RM1 provides the bidder with a certificate *cert* (signed using RM1's private key)
3. The bidder presents *cert* to RM2
4. RM2 checks RM1's signature on *cert* (using RM1's public key)
5. RM2 issues the bidder with a pseudonym *pn*, a secret key *x*, and an auction certificate *auction(pn, x)* as proof that *pn* and *x* are valid

Bidding: Figure 2 illustrates the process involved in bidding.

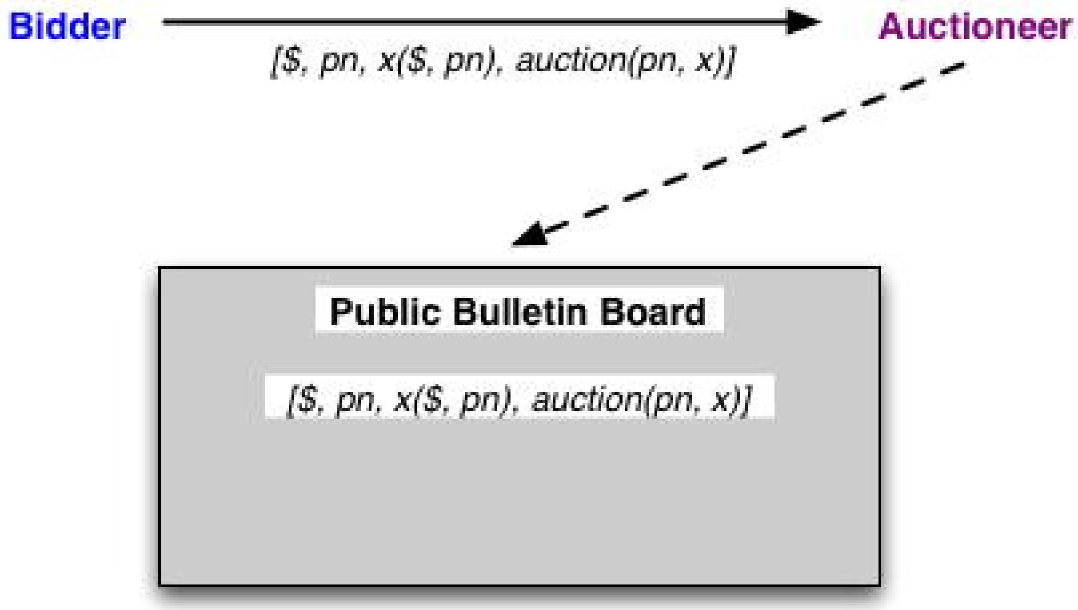

Bidder
Auctioneer
[$, pn, x($, pn), auction(pn, x)]
Public Bulletin Board
[$, pn, x($, pn), auction(pn, x)]

Figure 2: Bidding.

1. A bidder chooses his/her bid amount *$*
2. A bidder signs his/her bid *x($, pn)* using *x*
3. A bidder submits his/her bid to the auctioneer in the following form:

   [$, pn, x($, pn), auction(pn, x)]

4. The auctioneer checks *auction(pn, x)* (using RM2's public key)
5. if valid, the bid information is posted on the bulletin board, otherwise, the bid is discarded

Winner Determination: The auctioneer determines the auction outcome according to the auction rules and posts the result to the bulletin board.

Traceability: In the event of a bidder repudiating a bid, an optional traceability procedure can be run:

1. The auctioneer sends the disputed bid to RM1 and RM2
2. RM1 and RM2 recombine their information to reveal the *ID* corresponding to pseudonym *pn* that was used to submit the bid. This can be verified by checking *x($, pn)* and *auction(pn, x)*

In this scheme bids are un-forgeable, as they are signed using a bidder's secret key *x*. Neither of the registration managers is able to frame an individual bidder as they do not know the correspondencebetween *ID*, *pn*, or *x*.A traceability protocol can be run in the event that a bidder repudiates a bid.The auction proceedings are publicly verifiable via the bulletin board.The scheme is robust in the sense that the auctioneer can discard any bids without valid signatures.Bidders remain anonymous as long as RM1 and RM2 do not collude.

The problem with this example, however, is that bids are linkable because the same pseudonym is used for every bid.While this does not reveal the identity of the bidder, it does over time create a profile about the bidder'sbidding strategy.This information could also be used as the basis for a more sophisticated attack (explained in [12])that allows RM1 to learn the identity of a newly registered bidder.A further problem with this scheme is that RM2 could introduce fake bids into the auction in an attempt todisrupt the auction proceedings with a denial of service attack.Given that RM2 knows the value of every bidder's secret key *x*, RM2 can randomly sign fake bids using any *x*.

This simple example showed some of the issues and pitfalls of designing electronic auction schemes.

Research Directions - Group Signatures

The goal of our research is to investigate how group signature schemes can be applied to electronic auctions.The concept of group signatures was introduced by Chaum and van Heyst [3].A group signature scheme allows members of a group to sign messages on the group's behalf such that the resultingsignature does not reveal their identity. Signatures can be verified with respect to a single group public key, but does not reveal the identity of the signer.Only a designated group manager is able open signatures (reveal the signer's identity), in the case of a later dispute.Furthermore, it is not possible to decide whether two signatures have been issued by the same group member.

Group signatures have been employed by the electronic auction schemes presented in [8, 9].However, these schemes are very slow, that is, they require many modular computations to be performed and have much communication overhead.Furthermore, the use of group signatures by these schemes is complicated and somewhat different to how more conventionalgroup signature schemes work.Our research focuses on using group signatures in a simpler manner then what has been done in previous schemes. We are also applying this concept to a form of auction referred to as a continuous double auction, where there aremany buyers and many sellers (e.g., a share market)

[11].

In terms of an auction, the group manager corresponds to a registration manager. The bidders correspond to the group.Once registered, each bidder is able to sign messages (bids) on behalf of the group in such a way that it does notreveal the identity of the individual bidder that submitted the bid.Signatures can be verified by anyone, that is, the auctioneer, other bidders, and outside parties.In the case of a dispute, the registration manager can reveal the identity of the signer of a bid.The role of the auctioneer is merely to organize and run the auction.

Such an approach clearly requires the bidders to have full confidence in the registration manager who is a TTP.However, we are interested in actually distributing the role of the group manager across several parties (as in thresholdtrust schemes).To the best of our knowledge, group signatures have not been employed in such a manner before.We believe that group signature schemes naturally lend themselves to the electronic auction problem.

Conclusion

Online auctions are inherently insecure.Existing commercial auction sites only offer basic solutions to security and anonymity problems.All individuals are required to trust the auctioneer. Electronic auctions are cryptographic schemes designed to securely and anonymously conduct auctions.The main goals for a secure and anonymous electronic auction scheme are un-forgeable bids (to prevent framing), non-repudiation of bids, public verification of the auction proceedings, robustness, and to protect a bidder's anonymity.It is also highly desirable to reduce the trust that bidders have in the auctioneer.We identified four main approaches to trusting the auctioneer: trusted third party, threshold trust, two-server trust, and distributed bidder trust.We also presented an example of an electronic auction scheme based on the two-server trust approach. This example showed that it is hard to create an electronic auction scheme that satisfies the stated security andanonymity goals.We believe that the good approach to constructing electronic auctions is to use a group signature scheme.

Acknowledgments

The author would like to thank the following people for their contribution to this article: Dr Hossein Ghodosi, Marianne Brown, Bev Trevathan, and Mary Auker.

References

1 Brandt, F. (2003).Fully Private Auctions in a Constant Number of Rounds. *Seventh Annual Proceedings of Financial Cryptography*, FC'03.

2 Boyd, C. & Mao, W. (2000). Security Issues for Electronic Auctions. *Technical Report*, Hewlett Packard, TR-HPL-2000.

3 Chaum, D. & van Heyst, E. (1991). Group Signatures. *Eurocrypt'91*,pages 257-265.

4 Cassady, R. (1967). *Auctions and Auctioneering*. Berkeley: University of California Press.

5 eBay <**http://www.ebay.com**>.

6 Franklin, M. & Reiter, M. (1996). The Design and Implementation of a Secure Auction Service. *IEEE Transactions on Software Engineering*, vol. 22, pp. 302-312.

7 Naor, M., Pinkas, B., & Sumner, R. (1999). Privacy Preserving Auctions and Mechanism Design. *The 1st ACM Conferenceon Electronic Commerce*.

8 Nguyen, K. & Traore, J.(2000). An Online Public Auction Protocol Protecting Bidder Privacy. *Fifth Australasian Conference on Information Security and Privacy*, ACISP'00,pp. 427-442.

9 Omote, K. & Miyaji, A.(2001). A Practical English Auction with One-Time Registration. *Sixth Australasian Conference on Information Security and Privacy*, ACISP'01,pp. 221-234.

10 onSale <**http://www.onsale.com**>.

11 Trevathan, J. (2004). An Anonymous and Secure Continuous Double Auction Scheme. *Technical Report*, School of Information Technology, James Cook University.

12 Trevathan, J. & Ghodosi, H. (2004). Design Issues for Electronic Auctions. *Technical Report*, School of Information Technology, James Cook University.

13

Wang, C. & Leung, H.-f.(2004). Anonymity and Security in Continuous Double Auctions for Internet Retails Market,*37th Hawaii International Conference on System Sciences*.

Vickrey, W. (1961). Counter speculation, Auctions and Competitive Sealed Tenders. *Journal of Finance*, vol. 16, pp. 8-37.

Biography:

Jarrod Trevathan (**jarrod@cs.jcu.edu.au**) is a PhD student at the School of Information Technology, James Cook University.His research interests include cryptography, database security, multimedia, and electronic commerce.