Security Issues for Electronic Auctions

Colin Boyd[1], Wenbo Mao
Trusted E-Services Laboratory
HP Laboratories Bristol
HPL-2000-90
10th July, 2000*

electronic auctions

The security requirements for protocols for electronic auctions are discussed. Prominent research proposals are discussed and compared with the existing state of implemented electronic auctions on the Internet. Some promising research directions are proposed.

[1] Information Security Research Centre, Queensland University of Technology, Australia
* Internal Accession Date Only Approved for External Publication

Security Issues for Electronic Auctions

Colin Boyd
Information Security Research Centre
Queensland University of Technology, Australia

Wenbo Mao
Hewlett-Packard Laboratories
Bristol, UK

May 12, 2000

Abstract

The security requirements for protocols for electronic auctions are discussed. Prominent research proposals are discussed and compared with the existing state of implemented electronic auctions on the Internet. Some promising research directions are proposed.

1 Introduction

Trading can be divided into three phases: price negotiation, payment, and goods delivery. Until recently, most basic research in secure electronic commerce has concentrated on the latter two phases of trading; in particular there have been many sophisticated payment schemes proposed such as electronic cash with anonymity and double-spending detection.

Auctions are a form of price negotiation that enable efficient trading of scarce resources. As well as the well known long-standing auction houses selling fine arts, auctions have been widely used in recent times to obtain optimal revenue for such diverse items as national radio spectrum, mineral rights and US treasury securities.

Over the last couple of years there has been an explosion of small scale Internet auction sites, of which there are hundreds available today[1]. At the same time cryptologists have started to actively design and analyse secure protocols suitable for a variety of auction types and applications.

The purpose of this report is to consider the possible security requirements for electronic auctions, to review the prominent solutions that have been proposed up to now, and to suggest some possible promising research

[1]See, for example, the we sites `www.auctionwatch.com` or `www.auctioninsider.com`.

directions. The next section introduces some of the terminology and concepts of auctions. Then, in order to gain insight into the security requirements, the vulnerabilities of currently used Internet auction sites will be considered along with the countermeasures employed. The security requirements are then outlined followed by a survey of the prominent research proposals in the area is given, along with an assessment of their strengths and weaknesses. Finally some research directions are proposed.

2 Types of Auction

The mathematical theory of auctions has been studied by economists for at least 40 years. In this section only the basic ideas and definitions will be presented. Several authors have discussed these concepts, including Kumar and Feldman [5].

There are various criteria that may be used to classify auction types. Generally auction rules govern answers to the questions:

- When may bids be made?
- What value of bids may be made?
- What price will the winner(s) pay?

Open Cry Auction. This is the traditional type of auction in which bids are broadcast to all participants.

English Auctions. The auctioneer invites bids. Once a bid has been made only higher bids may be made subsequently. The winner of the auction is the final bidder.

Dutch Auctions [2] The auctioneer offers the goods at a high price. If no bidder accepts the offer, the offer price is lowered until a bidder accepts. The winner of the auction is the first bidder. (If several bidders accept then the price may be increased again.)

Sealed Bid Auctions. Bidders all commit to their bids during a first phase but the bid values sealed. In the second phase the bids are opened. The highest bidder wins. Sealed bid auctions may entail several rounds in which the bids may increase until a winner is found.

Multi-item auctions offer multiple copies of an identical item for sale at the same time.

Discriminative (or Yankee) Auction. A multi-item auction in which each winner pays the price they bid.

[2] It should e noted that many Internet auction sites use the term Dutch Auction to descri e an open cry multi-item non-discriminative auction.

Non-discriminative auction. A multi-item auction in which each winner pays the price of the lowest winning bid.

Vickrey (or Second Price) Auction. [3]

A sealed bid single item auction in which the winner pays the second highest price bid. This type of auction has some attractive properties. The expected revenue is the same as for English or Dutch auctions with reasonable assumptions, while it is distinguished from these in that each bidder's best strategy is to bid his true valuation.

Reserve Price. The minimum (starting) bid value for a valid bid.

Bid increment. The minimum difference between bids. Many sealed bid auction schemes assume that the bids are chosen from some initially defined finite set.

Bid Close Time. A time after which no new bids are allowed. In an English auction the bid close time may be fixed or may be defined by a period of inactivity (or a combination of both).

3 Internet Auction Security Today

All current Internet auction sites seem to work in essentially the same way. They use open cry auctions and are characterised by a total trust in the auctioneer with regard to fairness. Trade through Internet auctions during 1999 has been estimated at $4.5 billion[4] and this is confidently expected to increase significantly in coming years. According to figures published by the US Internet Fraud Watch, a service of the National Consumer League[5] online auction saled accounted for 87% of Internet fraud in the US in 1999 (an increase from 68% in 1998). The average loss is reported as $293.

Typical abuses in Internet auction include the following.

Bid shielding in which a high value bid is withdrawn at the last minute allows a low bid to be accepted. A number of individuals have claimed that this fraud is rife on some sites. Sites such as eBay maintain that it is necessary to allow bids to be withdrawn but claim to have measures to detect and remove abusers.

Bid siphoning in which a seller observing an auction makes direct contact to a bidder to offer an alternative (or equivalent) item available directly to the bidder. This can allow sellers to obtain buyers for their goods without paying the commission to the auction site.

[3] William Vickrey (1914-1996) was awarded the Nobel Prize for Economic Science in 1996. See `www.nobel.se/announcement-96/economy96.html`.

[4] See `www.auctionwatch.com/awdaily/features/yearin`.

[5] See `www.fraud.org/internet/99final.htm`.

Shilling introduces spurious bids in order to force up the price. The shill collaborates with the seller and in the event of the shill winning the auction the item may be re-sold at a different site. In physical auctions shills can be detected through observation if they persistently offend, but this is harder to do on the Internet with so many different sites available.

Sniping is last minute bidding in the hope of preventing other bidders from responding. This applies mainly on sites which have a fixed bid close time although the possibility for delays through denial of service attacks on the Internet may aid in making this a reak attack on any site. Software is apparently available to aid in the practice. There are some opinions that the excitement of sniping can increase the price obtained[6].

Misrepresented or non-existent items are a common complaint of auction buyers. A major source of this problem in the US is that most buyers are not using credit cards for payment.

Auction sites have implemented a number of security measures to counter fraud [2]. Some of the most prominent are the following, but they vary from site to site.

Feedback on buyers and sellers may be given by auction sellers and winners. Feedback may be positive or negative. An obvious problem with this practice is that it means that buyers are not treated equally (sellers are usually allowed to reject bids without reason). In addition, obtaining and giving of feedback can be done fraudulently.

Credit card registration is used by some sites as a form of authentication. This prevent multiple identities being used as well as tracing of offenders. Many people are uneasy about giving credit card details for non-purchase purposes.

Insurance services are now offered by many auction sites to underwrite losses caused by fraud.

Escrow services have been introduced by various auction sites to allow buyers to wait until goods are received before authorising payment. These services can also allow use of credit cards in customer to customer payments. The escrow services make a profit from the float held and so can provide this service without charge.

[6]See `www.auctionwatch.com/awdaily/features/sniping/`.

4 Security Requirements in Electronic Auctions

In order to assess the security of any auction protocol it is essential to be know what are its security requirements. Unfortunately different authors assume different requirements, or attach differing importance to requirements. Furthermore, certain requirements are applicable only to certain types of auction. In this section we will look at the most common security requirements.

Fairness is probably the most important property required of an auction. Roughly this means that all participants should be treated equally. For example:

- the highest bidder(s) should win the auction.
- the auctions winner must pay, as determined by the published rules.
- no bidder should have more information than any other to determine their bid.

In different types of auctions, fairness requires different things. For example, in a sealed bid auction the following are typical requirements.

- During the bidding phase all bids should remain confidential.
- When the bidding phase has finished no bidder should be able to change their bid.
- During the opening phase all bids must be opened.
- The highest bid(s) must win the auction.

Confidentiality of bids is often seen as desirable, although this often excludes the winning bid since if the winning bid is published all bidders can check whether they are winners.

Anonymity of bidders is often seen as desirable. Again this often excludes the winning bidder.

Minimisation of trust in one party, particularly the auctioneer, is a generally desirable property for any secure system. The trust may be required for different properties, particularly for anonymity or for fairness.

5 A Survey of the Literature on Secure Auction Protocols

In this section we look briefly at some of the prominent research literature. Proposals are classified into either open cry or sealed bid auctions, with the

latter class divided according to whether users themselves or the auctioneers are required to reveal sealed bids.

5.1 Open Cry Auctions

Most academic authors have taken the view that open cry auctions have too many undesirable features to be practical in electronic environments. For example Harkavy *et al.* [4] discuss the slow completion rates and lack of anonymity inherent in open cry auctions. Furthermore several authors, notable Wellman and Wurman [11], have pointed out the difficulties of truly simulating open cry auctions in the unreliable and insecure environment of the Internet.

Nevertheless, Stubblebine and Syverson [9] have proposed a detailed design for an open cry auction protocol whose main aim is to remove the trust in the auctioneer required in today's implementations. In essence it simply requires bidders to digitally sign and then publish their bids. To prevent sniping attacks the bid close time is extended until a suitable period of inactivity is encountered.

To ensure fairness the authors assume the existence of a trusted notary and timestamping service. It is arguable that this assumption is not valid today in practice and, furthermore, this can be regarded as simply moving the trust to a different place. Anonymity and privacy are not provided and, although it is claimed that they could be provided by other means, it is difficult to see how because publicly verifiable signatures are required to ensure fairness.

5.2 Sealed Bid Auctions

There have been a number of proposed protocols for sealed bid auctions. We identify two different approaches depending on how the sealed bids are opened in the second phase. In the first case the bids are opened by the bidders themselves. A potential problem with this option is what should happen if a bidder refuses to open his bid. This may occur if the bidder has already seen the value of other unsealed bids and thinks his bid is too high. It may also occur due to a communications failure. If the bid is simply discarded then this allows a bidder to revoke his bid which is unfair to bidders who reveal their bid first. On the other hand, if the bidder is assumed to have a high bid, can this later be revoked (for example if a failed communication link is restored)?

The other approach is to have the bids opened by the auctioneer. As already mentioned, the auctioneer can usually be distributed using a suitable group oriented cryptogaphic mechanism (secret sharing or group decryption). Nevertheless, the auctioneer becomes trusted and it is interesting to ask what degree of trust is required for fairness as well as for confidentiality.

5.2.1 Bids opened by bidders

Sakurai and Miyazaki [7] have proposed an ingenious protocol which makes use of *undeniable signatures.* These signatures have the property that they can only be verified in cooperation with the signer using a *verification protocol.* In addition the signer can prove that a different message from the one signed cannot be verified, by using a *disavowal protocol.*

Each bid is an undeniable signature of the bid value chosen from a finite list of allowed values. Once all bidders have committed to their bid the auctioneer starts an iterative procedure from the highest bid. Each bidder must either prove that he bid that value (using the verification protocol) or prove that he did not bid that value (using the disavowal protocol). If nobody has bid the current value then the procedure is iterated with the value decremented. The procedure continues until a valid bid is found.

The advantage of the scheme is that only the bid of the winning bidder is revealed and there is no requirement for trust in the auctioneer since all bidders can verify the correctness of the verification and disavowal protocols. Its major disadvantage is the enormous computational and communications requirements, especially if the list of bidders or possible bid values is large. There is no information in the paper to decide what should happen if a bidder refuses to cooperate in any round.

A recent proposal by Viswanathan *et al.* [10] uses a series of cryptographic mechanisms in a modular fashion. Electronic cash technology with revocable anonymity is used to enable bidders to prove that they have registered for the auction in such a way that their identity can be revealed in the case of abuse. This enables a solution in the case that a user does not cooperate but, on the other hand, means that trust is required for anonymity services.

A non-interactive proof allows bidders to seal their bids in a way that shows that their identity is available to a trustee. Because the cash protocol provides anonymity, the anonymous bidders can reveal their bids without revealing their identity. A performance analysis in the paper indicates that the computational requirements are very favourable in comparison with most other proposed protocols. This approach clearly requires more trust than the proposal of Sakurai and Mayazaki because the trustee can revoke anonymity at any time (or refuse to do so). Furthermore, a collaboration between the coin mint and a bidder may allow a bidder to prevent his identity being revealed (this aspect is not explicitly addressed in the paper).

5.2.2 Bids opened by auctioneer

One of the first, and most often cited, papers on auctions protocols was published by Franklin and Reiter in 1996 [3]. They use a technique known as verifiable signature sharing (VSS) to share electronic coins amongst a dis-

tributed auctioneer, this being a type of *money escrow*. The basic proposal does not provide any bidder anonymity or bid privacy. An extension allows pseudonyms to be used but without any identity escrow such as used by Viswanathan *et al.* [10]. A possible problem with this proposal is that the coins need to be used in a spending protocol to be deposited,even though their value is known. This could mean that a bidder could still refuse to complete payment if his bid wins.

Harkavy *et al.* [4] proposed a sealed bid scheme for Vickrey auctions which hides the bids of all bidders by secret sharing amongst a set of auctioneers. A complex scheme of polynomial secret sharing in combination with bitwise (or any other base) splitting of bids is used. Some problems include that the selling price is not publicly verifiable even if it is published. This could allow the auctioneers to increase the price paid by the winner. There is a problem regarding resolution of tie breaks which give information on bids. Also high communications costs are recognised by authors. Because the secret sharing used is not publicly verifiable, the combiner of shares must also be trusted to act correctly.

Sako [6] recently gave a protocol designed to reduce the communications required in the scheme of Sakurai and Miyazaki. The scheme is broadly the same but the undeniable signature is replaced by a group encryption scheme which must be decrypted by a threshold of the distributed auctioneers. Consequently this scheme introduces trust assumptions on the auctioneer. This proposal retains high computational costs.

6 Some Proposals for Research Directions

There appear to be two important directions for interesting and useful further research into auction protocols.

Improving Efficiency. Many of the protocols with attractive security properties have very expensive computations and/or communications requirements. Improving the efficiency is likely to be essential to make them practical.

Protocols which use digital signatures, such as that of Sakurai and Mayazaki [7], are well suited to exploit batch verification. These algorithms [1] allow a server (the auctioneer in this case, as well as any users wishing to verify published values) to perform multiple signature verifications together in one operation in order to obtain significant computational savings.

Another idea is to look at ways to trade off anonymity for efficiency gains. This seems to be possible in schemes such as those of Sakurai and Mayzaki [7], Sako [6] and Harkavy *et al.* [4]. The idea is to ensure that bids are made in a sequence of bid bits which can be examined

separately (this idea is already used in [4]). For example, if bids are in the range 1..127 then the most significant bit may be examined first to see whether any bidder has bid 64 or more. If so then all other bids can be completely discarded, thereby reducing significant computations. Note that this reveals one bit of information about the discarded bids. There appears to be considerable scope for refinement of this idea.

Reducing Trust. There appears to be a conflict between the requirements for bidder accountability and fairness. In order to overcome this conflict many proposals assume that the auctioneer is trusted, although most of these allow the auctioneer to be distributed so that a minority of malicious auctioneers cannot compromise the protocol.

Publicly verifiable secret sharing can be used in place of the secret sharing used in the scheme of Harkavy *et al.* [4]. This immediately reduces the trust required in the auctioneer, since all values can be verified by any party. In addition, it allows the distributed auctioneers to ensure that their shares are correct without having to communicate with the other auctioneers.

A recent efficient publicly verifiable secret sharing scheme of Schoenmakers [8] seems well suited for auction applications. It has the additional very useful property of being *homomorphic*. This means that it is possible to check with one calculation whether *any* bidder has bid a certain bit. This can greatly reduce computational costs, particularly in combination with the trade-off of anonymity mentioned above.

Another promising approach to reducing trust through public verifiability is the use of convertible undeniable signatures. This mechanism allows users to commit to a bid in such a way that the cooperation of the bidder is required to verify the bid (as in the scheme of Sakurai and Miyazaki). However, if required a designated trustee can convert the signature into a publicy verifiable one. This ensures that the bidder can be forced to cooperate.

In addition to these general principles of auctions, there is also work to be done in different specialised auction formats. For example, few authors have considered multiple round sealed bid auctions which are characteristic of high value government run auctions. Furthermore, these auctions seem to have a number of specialised rules governing the order and value of the bids allowed. It would be a challenge to include such rules while maintaining accountability and privacy.

Another interesting specialisation is to micro-auctions for very small value items. Asymmetric cryptographic operations are expensive and it may not be worthwhile to collect the revenue from micro-auctions unless

such operations can be avoided, or at least spread over a number of different transactions. Stubblebine and Syverson [9] have proposed use of a chain of hash values to reduce the expense of related bids in their open cry auction protocol. This technique is the same as used in various micropayment schemes and would be worthwhile to examine as a mechanism for micro-auctions.

7 Conclusion

Electronic auctions are continuing to grow in popularity, but fraud seems to be a major problem. Most of the current proposals for secure auction protocols seems to suffer from inefficiency, while trust issues are also of some concern. Promising future research directions can use modern cryptographic mechanisms to address these shortcomings.

References

[1] Mihir Bellare, Juan A. Garay, and Tal Rabin. Fast batch verification for modular exponentiation and digital signatures. In *Advances in Cryptology - Eurocrypt'98*, pages 236–250. Springer-Verlag, 1998. Also available at `www-cse.ucsd.edu/users/mihir`.

[2] Josh Boyd. Safety on the auction block. *Information Security*, January 2000. `www.infosecuritymag.com`.

[3] Matthew K. Franklin and Michael K. Reiter. The design and implementation of a secure auction service. *IEEE Transaction on Software Engineering*, 22(5):302–312, May 1996.

[4] Michael Harkavy, J.D.Tygar, and Hiroaki Kikuchi. Electronic auctions with private bids. In *3rd Usenix Workshop on Electronic Commerce*, pages 61–83, 1998.

[5] Manoj Kumar and Stuart I. Feldman. Internet auctions. In *3rd Usenix Workshop on Electronic Commerce*, 1998. Also available at `www.ibm.com/iac/papers/auction_fp.ps`.

[6] Kazue Sako. An auction scheme which hides the bids of losers. In *Public Key Cryptography - PKC'2000*, pages 422–432. Springer-Verlag, 2000.

[7] Kouichi Sakurai and Shingo Miyazaki. A bulletin-board based digital auction scheme with bidding down strategy. In *CrypTEC'99*, pages 180–187. City University of Hong Kong Press, 1999.

[8] Berry Schoenmakers. A simple publicly verifiable secret sharing scheme and its application to electronic voting. In *Advances in Cryptology - CRYPTO'99*, pages 148–164. Springer-Verlag, 1999.

[9] Stuart G. Stubblebine and Paul F. Syverson. Fair on-line auctions without special trusted parties. In *Financial Cryptography '99*, pages 230–240. Springer-Verlag, 1999.

[10] Kapali Viswanathan, Colin Boyd, and Ed Dawson. A three phased scheme for sealed bid auction system design. In *Information Security and Privacy*. Springer-Verlag, 2000. To appear.

[11] Michael P. Wellman and Peter R. Wurman. Real time issues for internet auctions. In *First IEEE Workshop on Dependable and Real-Time E-Commerce Systems (DARE-98)*, June 1998.