A Common Security Model for Conducting e-Auctions and e-Elections

EMMANOUIL MAGKOS[1], NIKOS ALEXANDRIS[1], VASSILIS CHRISSIKOPOULOS[2],

[1]Department of Informatics
University of Piraeus
80 Karaoli & Dimitriou, Piraeus 18534
GREECE
{emagos, alexandr}@unipi.gr

[2]Department of Archiving and Library Studies
Ionian University
Old Palace Corfu 49100
GREECE
vchris@ionio.gr

Abstract: - With the advent of new technologies, traditional systems are currently replaced with electronic ones. Throughout this transition, security concerns such as privacy and anonymity are increasingly raised. In this paper we consider, from a security point of view, electronic auctions and electronic voting systems. We present, at high level, a common model for securely conducting both systems. It is also shown how several application-specific requirements can be incorporated into this model.

Key-Words: - Privacy, Security, Cryptology, e-Auctions, e-Elections

1 Introduction

With the advent of new technologies, traditional systems are currently replaced with electronic ones. Throughout this transition several security concerns are increasingly raised, such as privacy and anonymity of electronic transactions. While in the real world security is usually established by physical means, in electronic communications the use of cryptographic mechanisms seems to be the only protection against malicious activities.

E-commerce transactions have already gain public acceptance in many countries. Furthermore, governments are making serious steps towards establishing an e-government infrastructure. In this paper we consider, from a security point of view, two of the most important vehicles for conducting e-commerce and e-government. Namely, we consider electronic auctions and electronic elections. We describe a security model, which can be used to conduct both systems. In addition, we examine how several application-specific requirements can be incorporated into this model.

Private e-Auctions. We are mainly concerned with private auctions, also known as *sealed auctions*. Sealed auctions emphasize security issues inherent in every e-commerce activity. In such auctions, bidders submit their evaluation (i.e., the bid) before the end of a bidding period. One bid is only allowed. After the bidding period ends, bids are opened and a winner is determined. The highest winner wins and pays the amount bid (*first-price* auction) or an amount equal to the second highest bid (*second-price* auction [1]). For a survey of auction types, the reader is referred to [2]. Several mechanisms for conducting private electronic auctions have been proposed by the research community (e.g. [3-5]).

e-Elections with central administration. This kind of elections with central administration has been seen as the most promising solution for Internet voting, because it offers efficient administration and demands low complexity of computation [6]. In such elections, a voter is authenticated, during registration, in a way that there can be no link between the final vote and the identity of the voter. Secure elections over the Internet have been the subject of thorough research (e.g. [7-9]).

2 Common Model Design

Auctions and elections are similar in many respects. For the following of this section we will present a model than can be used to implement both auctions and elections. The players are the *Users* and a *System Authority* (*SA*). There is also a list of *items I*

and a set of *Rules R*. An *Anonymous Channel* (see Remark 1) and a *Bulletin Board* (*BB*) are used as primitives. *BB* is a public broadcast channel with memory. Only *SA* can write to *BB*, while no party can erase any information from it.

Remark 1. Anonymous channels can be used to conceal the link between a message and its sender. They are usually implemented with a number of intermediary nodes (a *Mix*), which form an anonymity chain. Anonymity is preserved as long as there is at least one honest node [8].

There are essentially three phases in the protocol (Fig.1):

Submitting phase. A user selects an item *i* out of a set of possible items *I*. The user employs a commitment mechanism (see [10] for a discussion on cryptographic commitments) to encrypt *i*, and then uses an open communication channel to submit the encrypted item to *SA*. *SA* validates the encrypted item, i.e. ensures that it came from an authorized user. The transaction takes place in a way that there can be no link between the item *i* and the user's identity (see Remark 2). *SA* returns a proof of receipt for the submitted item. This proof will be used in the Claiming phase.

Remark 2. Concealing the item-identity link is easy to achieve by using *blind-signature* techniques [7,8]. Such cryptographic techniques allow for a document to be signed without revealing its contents. The effect is similar to placing the document and a sheet of carbon paper inside an envelope. If somebody signs the outside of the envelope, he will also sign the document inside.

Claiming phase. After the end of a publicly known period, *SA* publishes the committed items (partial results) on *BB*, for verifiability. The User may complain in case his committed item cannot be found on the board. For example, complaints can be done by broadcasting the proof of receipt which was obtained during the Submitting phase. Thus, a misbehaving authority will be exposed.

Tallying Phase. After the end of the Claiming phase, the user employs an *anonymous channel* to give away a secret *s* for the de-committal of *i*. This secret will be used by *SA* to decrypt the encrypted *i*. *SA* declares the winning item according to the set of rules *R* of the system. For verifiability, *SA* publishes all the de-committal secrets as well as the decrypted items (final results). Any observer can verify that there is full consistency between these results and the partial results which were given during the Claiming phase.

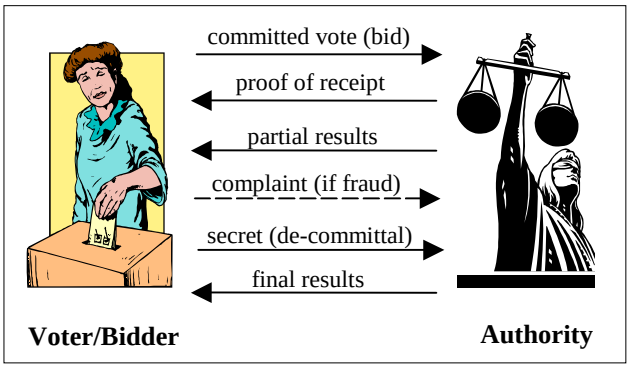

Fig.1 One protocol for two applications

In case of an electronic election, the users are voters, and the set of possible items can be any set of acceptable votes, e.g. "yes" or "no". In case of an electronic auction the users are bidders and there is a set of acceptable bids, e.g. 10, 20, …, 100. In both cases the communication channel could be an open network such as the Internet.

2.1 Security Requirements

We discuss several security requirements for our model. These requirements are general and do not depend on the particular aspects of the model (auction or election).

Accuracy. The system is accurate if:

- No validated item can be altered / eliminated from the final tally;
- No invalid item can be counted in the final tally.

Invulnerability. The system is invulnerable if:

- Only eligible users can submit an item;
- No eligible user can submit an item more than once (see also Remark 3).

Privacy. The system is private if:

- No one (including the system authority) can link the item to the user who has cast it;
- All items remain secret until the end of a publicly known period.

Verifiability. The system is verifiable if:

- Users can independently observe that their items have been counted correctly.

At high level, these security requirements are satisfied with the protocol of Fig.1.

Remark 3. While the second invulnerability requirement is an obvious requirement for e-voting as well as for private (sealed) auctions, there are several auction types, e.g. the public (ascending) auction, where a number of successive bids may be allowed. We do not deal with this kind of auctions.

2.2 Novel Security Requirements for our Model

In addition to the requirements discussed above, there are several security requirements that seem to be application specific, i.e. they can be met either only in e-voting applications, or only in e-auctions, but never in both.

One such major security requirement for electronic elections is *uncoercibility* for voters [11]. With uncoercibility, no voter is able to sell his vote to an information buyer, or prove his vote to an information coercer.

In addition, *non-repudiation* for bidders in private electronic auctions is another application-specific requirement [4]. With non-repudiation, no bidder should be able to withdraw his bid without being detected.

We show how these requirements can be incorporated into our model, i.e. become a pre-requisite for both secure auctions and elections.

Uncoercibility. Uncoercibility can be seen as a privacy requirement. So far it has only been addressed in the context of e-voting [12]. However uncoercibility seems to have applicability in the auctions field too. The need for uncoercibility in electronic auctions is motivated by the problem of *bid rigging* (also known as *collusion* of bidders).

Bid rigging works like this: a group of bidders (they are usually the bidders with the highest evaluation for the item) conspire with each other, thus forming a *ring*, in order to control the winning price for the item to be auctioned. They agree on a lowest winning price for this item, the *collusive price*. After the auction ends, all members of the ring may share the profit resulted by winning the item at a low price. In a *bid rotation* scenario, the members of a ring take turns winning each auction. There are many forms of collusive schemes in all type of auctions, private or public [2,13].

In the physical world, *private auctions* (i.e. where all bids are secret until the end of the bidding period) are more resistant to bid rigging than *public auctions* (i.e. where all bids are publicly announced during the auction). In a public auction, a member of the ring who decides to cheat on the ring will alert all other members, so bid rigging is difficult to deal with. However, in a private auction, a ring member can always deviate and outbid the other ring members, thus acquiring the item at a cost that is slightly greater than the collusive price. If the winner's identity is protected, then the ring is defeated. Otherwise, a black-party, i.e. *the coercer*, could take revenge on the winner.

In secure electronic auctions, bids are encrypted for privacy, and all encrypted bids are published for verifiability [4,14]. The bidders can prove the content of their bids by revealing any secret keys or randomness they used for the encryption. Furthermore, the encrypted winning bid is published at the end of the auction. Even if the bidders' identity is protected all ring members can prove to a coercer that their bid was not the winning bid.

From the above the need for uncoercibility in electronic auctions is obvious. If bidders are not able to prove their bid to a third party, then bidders will be discouraged from forming collusions.

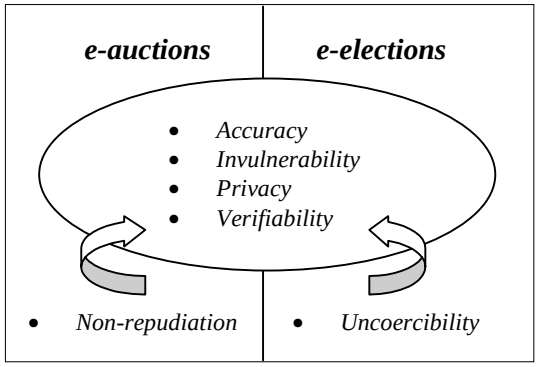

Fig. 2 Incorporating new requirements into our model

Non-repudiation. In private electronic auctions, non-repudiation of bidders is a major security concern, especially in systems where the anonymity of bidders must also be protected [4,14]. With non-repudiation, no bidder should be able to withdraw his bid without being detected, while at the same time the identity of the bidders is protected i.e. no one can link the bidder to the bid he has cast. This property has been addressed in [4].

Surprisingly, this property seems also to have applicability in electronic elections with central administration. This is motivated by the fact that in most election systems that have been proposed so far (e.g. [6,9], if a voter is registered for the election but then decides to abstain, the voting authority can cast a vote for an abstaining voter and get away with it. In such systems, impractical assumptions, e.g. that all registered voters who wish to abstain submit a blank ballot, are often made.

While it is *fair* for someone who submits an encrypted vote to abstain from the election thereafter, it is not *equitable* towards "society" [15]. By "society" we mean all voters, authorities and independent observers that wish to independently verify the correctness of the election results. Allowing a voter to abstain from the election after the Submitting phase (see Fig. 1), would be as fair

as allowing voters, in traditional elections, to vote without signing on the voters' list.

From the above, the need for non-repudiation in e-elections (with central administration), is obvious. Thus, both requirements of uncoercibility and non-repudiation can be incorporated into our model (see Fig. 2).

3 Conclusion

In this paper we presented a common security model for conducting e-auctions and e-elections. Our model supports systems with central administration, and so it can be considered practical for Internet applications. We examined how several application-specific requirements can be incorporated into this model. As a result, our model provides for security, independently of whether it will be used to support auctions or elections.

References:

[1] Vickrey, W. Counterspeculation, Auctions, and Competitive Sealed Tenders, *Journal of Finance*, Vol.16, No.8, 1961, pp. 8-37.

[2] Klemperer P. Auction Theory, A Guide to the Literature, *Journal of Economic Surveys*, Vol. 13, 1999.

[3] Harkavy M., Kikuchi H., Tygar J. Electronic Auctions with Private Bids, *3rd USENIX Workshop on Electronic Commerce*, USENIX Press, 1998, pp. 61-74.

[4] Magkos, E., Burmester, M., Chrissikopoulos, V. An Equitably Fair On-Line Auction Scheme, *1st International Conference on Electronic Commerce and Web Technologies, EC-WEB 2000*, LNCS Vol.1875, Springer-Verlag, 2000, pp. 72-83.

[5] Franklin M., Reiter M. The Design and Implementation of a Secure Auction Service, *IEEE Transactions on Software Engineering*, Vol.22, No.5, 1996, pp. 302-311.

[6] Herschberg, M. Secure Electronic Voting Using the World Wide Web. *Master's Thesis*, Massachusetts Institute of Technology, 1997.

[7] Chaum, D. Blind Signatures for Untraceable Payments, *Advances in Cryptology-CRYPTO '82*, Plenum Press, 1982, pp. 199-203.

[8] Chaum, D. Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms, *Communications of the ACM*, Vol.24, No.2, 1981, pp. 84-88.

[9] Cranor, L. Cytron, R. Sensus. A Security-Conscious Electronic Polling System for the Internet, *Hawaii International Conference on System Sciences*, Wailea, Hawaii, 1997.

[10] Schneier, B. *Applied Cryptography-Protocols, Algorithms and Source Code in C*, 2nd Edition, 1996.

[11] Benaloh, J., Tuinstra, D. Receipt-free Secret-Ballot Elections, *26th Annual ACM Symposium on the Theory of Computing*, 1994, pp. 544-553.

[12] Magkos, E., Burmester, M., Chrissikopoulos, V. Receipt-Freeness in Large-scale Elections without Untappable Channels, *1st IFIP Conference on E-Commerce / E-business / E-Government*, Zurich, Kluwer Academics Publishers, 2001, pp. 683-693.

[13] Mead, W. Natural Resource Disposal Policy: Oral Auction Versus Sealed Bids, *Natural Resources Journal*, Vol.7, 1987, pp. 195-224.

[14] Stajano F., Anderson R. The Cocaine Auction Protocol: On the Power of Anonymous broadcast, *3rd International Workshop on Information Hiding*, Lecture Notes in Computer Science, Springer-Verlag, 1999.

[15] Magkos, E., Chrissikopoulos, V. Equitably Fair Internet Voting. *Journal of Internet Technology*, Special issue on Network Security, April 2002, to be published.