Acknowledgments

I would like to thank my parents Ian and Bev Trevathan, and brother Shane, for their support. Thank you Sharith for helping me edit my publications.

Meow to Mr Gab.

Muchas gracias para mi querida amiga Andrea.

Accolade is also due to those who directly or indirectly contributed to this research.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

Online Auctions are extremely popular. Once the domain of highly skilled negotiators, online auctions have made auctioning accessible to everyone, regardless of whom they are. A novice can buy everyday items such as groceries and clothes, or can compete for rarities and collectables such as rock memorabilia and antiques. Likewise, a seller has access to virtually a worldwide consumer base. It also seems that non-conventional items can be sold via online auctions, which would probably not be sold anywhere else! For example, auctions for the following items have been held:

1. Mold on a sandwich that resembles the Virgin Mary;

2. A man willing to bang his head on a door until he is unconscious; and

3. A French Fry shaped like the Nike logo.

However, despite the overwhelming benefits and hype, there is a sinister and dark reality to auctioning online. Auction fraud is one of the fastest growing forms of Internet-based crime. Participants are anonymous and can engage in undesirable and fraudulent behaviour in an attempt to gain an unfair advantage. For example, the seller may misrepresent or not deliver an item. Likewise, a bidder can refuse to pay, or have his/her bid forged. Furthermore, the Auctioneer could block bids or influence the auction in a manner that maximises its revenue. Various cryptographic solutions have been proposed to fix many of these problems. However, most of these schemes are not suited to the auction style that is most commonly used online.

Certain types of bidding behaviour can also be used to influence the auction in an undesirable manner. One such type of behaviour is *shilling*, where the seller introduces fake bids into the auction in order to inflate the price. Shilling is prohibited in online auctions, however, it still continues to occur. Solutions to detect and/or prevent shill bidding tend to be outside the realm of cryptography. While online auctioneers claim to monitor their auctions for bad behaviour, there are no published methods on how to detect shill bidding. The problem is compounded with the advent of *software bidding agents*.

Software bidding agents are used to bid on a human's behalf. The Artificial Intelligence community has suggested that agent-based negotiation could eventually replace all human input. However, such a claim is flawed, as agents can also act in a fraudulent manner. While much research has been conducted into improving the performance of bidding agents, little attention has been given to the security implications. A bidding agent can be designed maliciously so that it harms the auction in some of the previously mentioned ways. This is a serious concern now that bidding agents are used for trading shares online.

Online share trading is a popular offshoot of more conventional online auctions. An individual can submit a buy or sell order to a broker, who then enters it into the share market. The privacy and security issues in online auctions are also manifest in online share trading. Although tightly regulated, there is even less security than online auctions. The extra parties involved in the auctioning process (i.e., broker, share market, regulatory authority, etc.) further complicate the privacy and security requirements. Limited attention has been paid to these issues, or the special auction type employed by this application.

There are many auction types including Vickrey, Dutch, Japanese, Combinatorial, etc. Existing auction security literature has mainly concentrated on Vickrey or sealed bid auctions. However, the most popular online auction type employed online resembles an *English* auction (e.g., eBay). In an English auction, one seller offers an item to several bidders where the highest price wins. In contrast, online share trading uses an auction type referred to as a *Continuous Double Auction* (CDA). A CDA has many buyers and sellers continually trading a commodity. The method for matching buy and sell bids (referred to as *clearing*) is much more sophisticated than English auctions. The privacy and security requirements for English auctions and CDAs differ dramatically from previously studied auction types. This book concentrates solely on English auctions and CDAs.

1.1 Aims

This book investigates privacy, security and fraud issues in online English and Continuous Double auctions. The main objective is to understand the characteristics of fraudulent auction behaviour, and propose mechanisms to combat it. With regard to the aforementioned problems, the research goals include:

1. Provide a security model for auctioning online that protects a bidder's personal information;
2. Construct a model for securely and anonymously trading shares online;
3. Explore the security implications of agent based negotiation;
4. Develop methods to detect certain types of auction fraud (i.e., shilling); and
5. Devise and evaluate alternate software mechanisms for clearing CDAs.

1.2 Methodology

Many of the issues investigated in this book are **illegal** to perform in actual commercial online auctions. This makes it difficult to assess the extent of fraudulent activity, and understand its nature. Furthermore, there is no way to evaluate the effectiveness of newly proposed security mechanisms. To accomplish the research goals, an online auction server has been constructed. This allows for experimentation in a controlled environment, without the risk of prosecution.

The server was used to test security theories and gauge practical performance and efficiency. The server can perform both simulated and real auctions. It has a software bidding agent interface, which allows auctions to be fully automated (i.e., no human input required). The auction server's software components are documented throughout the book. Descriptions are given regarding how tests were conducted, and their results.

This book *does not condone* the use of any of the discussed illegal themes, and does not support in any way their use other than for the purpose of research, and only then to assist

in the development of effective avoidance, deterrent and detection mechanisms to use to stop fraudulent behaviour.

1.3 Results

With regard to the aims stated in Section 1.1, the book results are as follows:

1) Online auction privacy and security issues have been extensively investigated. From this, a complete online auction security model for English auctions has been devised. This model uses cryptographic mechanisms to ensure bid authenticity, and provides verification that everyone has followed the auction protocol correctly. An individual remains anonymous provided they don't repudiate having made a bid. In the event of bid repudiation, two independent parties can work together to trace the bid's owner.

2) Privacy and security issues involved in online share trading are investigated, and a comprehensive set of security requirements are given for this auction type (i.e., CDAs). The online English auction security model is extended to encompass CDAs and application specific details pertinent to online share trading. This is the first secure auction scheme to specifically address share markets.

3) Two malicious bidding agents that engage in shilling behaviour have been constructed. A *simple shill bidding agent* inserts fake bids to inflate the price until it becomes too risky to continue. A *adaptive shill agent* uses knowledge from a series of auctions with substitutable items to revise its strategy. This is achieved using novel prediction methods. The agents allow us to understand a fraudulent bidder's nature, and help refine the proposed shill detection techniques.

4) A novel method to detect shill bidding in online English auctions is presented. Bidders are issued with a score based on their bidding behaviour. The score indicates the likelihood that the bidder is engaging in shilling. This can be used by other bidders to decide whether they want to participate in auctions held by a particular seller. The scheme is resilient in that it can detect colluding bidders and sellers that attempt to thwart the system.

5) Several new CDA market clearing algorithms are proposed, which are more efficient than the existing methods used in financial markets. These algorithms employ techniques such as waiting, subsidisation and prioritising to achieve a higher trade volume. Efficiency is measured in terms of the number of bids and amount of quantity matched. Comparisons are drawn between the optimal offline algorithm and the proposed online clearing algorithms.

As previously mentioned, the performance of the devised techniques has been tested using the online auction server. Test results are given and scrutinised in terms of existing literature. Many of the results can be practically applied in commercial online auctions.

1.4 Book Organisation

This book draws from e-Commerce, Information Security, Software Engineering and Artificial Intelligence.

This book is organised as follows. Chapter 2 introduces online auction concepts. It provides an overview of auction history, the types of auctions that exist, and the major commercial vendors in the online auction market. Chapter 3 discusses fraudulent bidding behaviour and the security and anonymity

problems with auctioning online. This chapter is the main thrust behind the security considerations of the research presented in this book. The software platform for conducting online English auctions and CDAs is introduced in Chapter 4. Chapter 5 presents an online English auction security model that seeks to remedy the identified privacy and security concerns. Chapter 6 discusses online share trading, and its similarities to online auctions in terms of privacy and security. An anonymous and secure CDA scheme for trading shares online is presented. Chapter 7 explores the security implications for agent-based negotiation, and presents bidding agents that bid in a fraudulent manner. Chapter 8 presents novel methods to detect shill bidding. Chapter 9 provides some concluding remarks and avenues for future work. Appendix A contrasts several algorithms for clearing share markets (i.e., matching buy and sell bids).

This book is designed to be read sequentially from start to finish, as later topics build upon previously introduced concepts. However, after reading Chapters 2 and 3, the reader can skip ahead if desired. English auctions are addressed in Chapters 4, 5, 7 and 8. CDAs are covered in Chapters 4, 6 and Appendix A. Note that Chapters 5 and 6 require that the reader has some background cryptographic knowledge as they contain complicated theoretical mathematics.