Australian Government
Australian Institute of Criminology

<AHTCC>
AUSTRALIAN HIGH TECH CRIME CENTRE

no. 15 ▪ 2007 HIGH TECH CRIME BRIEF

The risk of criminal exploitation of online auctions

Advances in information technology and the internet have revolutionised the way we communicate, enabling borderless data transfer in real time. This significantly influences the way in which commerce operates, for example, electronic payment systems, and online auction sites. This is hardly surprising as the financial incentive in today's highly competitive market is significant, with the cost of an online transaction often being a fraction of the cost of a non-electronic transaction (De Young 2001).

Online auction models

Online auction sites provide buyers and sellers a global virtual market and storefront to buy and sell a wide range of merchandise through competitive bidding. They constitute one of the most successful internet-based business models.

Open-cry auction models, where bids are broadcast to all bidders, are more popular than sealed-bid auction models. Examples include:

- English auctions: bidders (buyers) seek to outbid each other interactively until the merchandise on sale has been sold or the auction expires.
- Dutch auctions: auctioneers (sellers) display multiple copies of identical merchandise and will sell them to the highest bidders.
- Reverse auctions: bidders indicate their desired merchandise and price. Auctioneers then negotiate a mutually agreeable price until a sale is made, e.g. priceline.com.
- Double-sided auctions: multiple bidders and multiple auctioneers bid simultaneously, e.g. the Hollywood Stock Exchange (http://www.hsx.com/).

An example of a sealed-bid model is the second price auction (also known as Vickrey auction) used in Google's Adword auction (Adams 2006). Bidders place their bids without revealing value and the winning bidder pays the amount of the second highest bidder.

Criminal exploitation of online auctions

Recent statistics (NW3C/FBI 2007) indicate that online auction fraud is the most prevalent offence type reported to the Internet Crime Complaint Center. Out of 207,492 complaints between 1 January and 31 December 2006, online auction fraud accounted for 45 percent of the 86,279 cases referred to US law enforcement agencies and 33 percent of the total reported dollar loss. It is important to recognise, however, that in comparison with the total volume of online transactions the number of complaints remains relatively small.

Ways in which online auctions can be exploited or manipulated by auctioneers and bidders are as follows (Adams 2006; Boyd & Mao 2000).

MANIPULATION BY AUCTIONEERS

- Shilling: to drive up the selling price, auctioneers spuriously place bids on their own auction (e.g. see eBay jewellery store… 2007).
- Bid siphoning: auctioneers avoid paying commissions to auction sites by contacting and transacting with interested bidders directly.
- Second chance offers: losing bidders of a closed auction are offered a second chance to purchase the same item off-site.
- Shell auction: with no intention of selling, auctions are established for the purpose of obtaining names and credit cards, which are then used to facilitate crimes such as identity theft.
- Misrepresentation: specifications for the merchandise for sale are intentionally described incorrectly or the actual quality of the merchandise is overstated.
- Failure to ship: auctioneers fail to send the merchandise upon receiving the money. In February 2005, a Queensland man was convicted in such a case.
- Counterfeits/pirated software: counterfeits, usually luxury items, and pirated software are offered for sale.
- Triangulation/fencing: stolen goods are offered for sale.
- Fee stacking: hidden costs are added to the transaction after the auction has ended.

Project no. 0074a

ISSN 1832-3413

The Australian High Tech Crime Centre funded this research.

DISCLAIMER
This research paper does not necessarily reflect the policy position of the Australian Government, the AIC or the AHTCC.

CONTACT
Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601

T: 02 6260 9200
F: 02 6260 9201
www.aic.gov.au

- Sale of non-existent merchandise: in August 2003, two men were charged in Illinois with using stolen identities to sell nonexistent goods in online auction sites.
- Using compromised accounts: in March 2007, a man was arrested on charges relating to hacking into two eBay users' accounts and using these accounts to sell nonexistent Apple iPods with an estimated worth of A$13,482 (eBay thief stole $42,000 2007).

MANIPULATION BY BIDDER

- Bid shielding: a dishonest bidder places a low bid while a colluding bidder places an inflated bid. The colluding bidder withdraws immediately upon winning the auction, resulting in a lower bid being accepted.
- Failure to pay: bidders fail to pay for the merchandise received.
- Buy and switch: buyers switch received merchandise with inferior merchandise and then request a refund.
- False-name bid: bids are made under fictitious names or using stolen credit cards.

Although some manipulation practices are currently criminalised in Australia (e.g. hacking into existing user accounts), many of these are civil matters (e.g. shilling).

Crime prevention measures

AUTHENTICATION MECHANISMS

Authenticating the identity of online auction site bidders and sellers is the primary fraud minimisation strategy. There are three ways in which individuals can be identified (Geihs, Kalcklsch & Grode 2003): by producing or disclosing something that they have (tokens such as cards), something that they know (such as passwords), or something related to who they are (biometrics such as fingerprints). There are others, such as the use of a person's name or location and a variety of behavioural and psychological characteristics that can be used to identify people.

On most online auction sites users are identified by their email address (and corresponding password). This can be used by fraudsters, however, to facilitate fraudulent transactions since the email address is a perfect pseudonym that does not reveal any links to the original user. Such password-based authentication has its share of disadvantages despite being cheap to deploy, easily revocable, and having wide user acceptance. In terms of user accountability, it might be hard to hold a user legally accountable for any actions attributed to them in a password-only authentication system. Moreover, most online auction sites only authenticate that the user has a valid email address, and clearly this is a weak form of authentication.

An additional security feature deployed by most online auctions is secure channel sign-in where the browser and the auction sites employ an SSL/TLS connection. This encrypts the user's password to ensure secure communication between the browser and the site, which helps to prevent password leakage via eavesdropping and illicit capture. However, a keylogger would still pick this up, if such a program were installed on the user's computer.

REPUTATION MECHANISMS

The Feedback Forum on eBay, a reputation mechanism, is one important means to produce trust and induce good behaviour among members. The centralised forum provides registered eBay users with opportunities to rate each other as positive, negative, or neutral and leave comments after completion of a transaction. Ratings can also be provided on the description of goods, communication, delivery time and postage and packing charges. The running total reputation score of each participant is the sum of positive ratings (from unique users) minus the sum of negative ratings (from unique users). In order to provide information about a participant's recent behaviour, the total of positive, negative and neutral ratings for three different time windows (past month, past six months and past 12 months) are displayed.

Reputation systems can, however, be exploited. For example, in ballot stuffing, sellers collude with bidders to give positive feedback on fictitious transactions, hence inflating the auctioneer's reputation (Bhattacharjee & Goel 2005).

PAYMENT SECURITY

Individuals can take action to reduce the risks of fraud by choosing safer payment options, including credit cards and online payment services such as PayPal, that offer some form of consumer protection. Buyers should avoid using instant wire transfers or any purportedly independent third party escrow payment services. There have been cases reported where escrow payment services are controlled by dishonest buyers/sellers to commit frauds. Individuals can also take steps to protect their passwords and other personal information to prevent identity theft.

EDUCATION

User education at the point of transaction and through the dissemination of media releases by authoritative institutions, such as the Internet Crime Complaint Center, enables users to keep abreast of the latest auction scams and the best fraud prevention measures available. There is a need for coordinated action by government agencies to ensure that the most effective advice is provided to the community.

FURTHER READING

All URLs were correct in June 2007

Adams CP 2006. *FTC Bureau of Economics roundtable on the economics of internet auctions: an executive summary*. http://www.ftc.gov/be/workshops/internetauction/Roundtable_Summary.pdf

Bhattacharjee R & Goel A 2005. Avoiding ballot stuffing in eBay-like reputation systems. *Proceedings of SIGCOMM 2005 workshops*. New York NY: ACM: 133–137

Boyd C & Mao W 2000. *Security issues for electronic auctions*. HP Laboratories Tech Report HPL-2000-90. http://www.hpl.hp.com/techreports/2000/HPL-2000-90.pdf

De Young R 2001. The internet's place in the banking industry. *Chicago Fed letter* no. 163. http://www.chicagofed.org/publications/fedletter/2001/cflmar2001_163.pdf

eBay jewellery store fined $400,000 for shill bidding 2007. *The register* 11 June

eBay thief stole $42,000 2007. *Sydney morning herald* 19 March

Geihs K, Kalcklsch R & Grode A 2003. Single sign-on in service-oriented computing. *Proceedings of ICSOC 2003* 2910 of LNCS: 384–394

National White Collar Crime Center and Federal Bureau of Investigation (NW3C/FBI) 2007. *2006 IC3 annual internet fraud report*. http://www.ic3.gov/media/annualreport/2005_IC3Report.pdf