Contemporary Management Research
Pages 305-314, Vol. 6, No. 4, December 2010

Providing a Trustworthy Trading Environment with a New Authentication Protocol in Online Auctions

Ying Sai
Loyola Marymount University
E-Mail: ysai@lmu.edu

ABSTRACT

This research takes a two-pronged approach, identifying and then proposing a solution for the basic problem keeping many potential users from engaging in online auction trading, and discouraging those who do use these sites from buying or selling high-value items. The problem? ---The absence of a reliable user registration process. To remedy this situation, this study proposes a new authentication protocol adding two levels of protection and providing users with a trustworthy trading environment through stronger identification and authentication functions.

Keywords: Online Auction, E-commerce Trust, User Authentication, eBay Reputation

INTRODUCTION

Since 1995, the year the most popular online auction site, eBay, was founded, hundreds of online auction sites have sprung up, only to fold just as quickly. At any time of the day, there could be thousands of online auctions in session and millions of people participating throughout the world. One of the interesting facts about online auctions is that the average sales price is only $30, while the average sales price for traditional auctions is $300 (Lucking-Reiley, Byran, Prasad, & Reeves, 2007). This indicates that, in general, the items sold through online auctions online tend to have a lesser value than the objects sold in traditional auctions (Lucking-Reiley, 2000). Finding ways to increase online auctions' average sales price could be crucial to improving the online auction business model.

In Section 2, this study starts at the root of users' sense of insecurity about buying and selling online: user registration. Section 3 focuses on how the weak user verification mechanism makes shill bidding and artificial raising of reputation scores an easy task. Section 4 presents a new authentication protocol. The last section

concludes with a discussion of the implications of this research and future work that might further benefit the growth of online auctions.

USER REGISTRATION

Problems with user authentication start at the very beginning of a user's online auction experience---user registration. On the surface, the significance of the user registration process at online auctions seems to be the same as at any other online services such as online shopping or online travel services sites. However, at online auction sites, user authentication has much more far-reaching effects on the fairness and trustworthiness of the auctions. In this section, we will first present what registration was like before, and then discuss the events that have led to modifications in the registration process and its current situation.

In online auctions, the user registration process was like that of any other online service in that users could set up multiple accounts with different user IDs and passwords. With multiple user IDs, one user can simultaneously participate in the same auction as different individuals. In addition, registration was free of charge, so anyone could set up as many user IDs as he wished. This flawed user registration process was essentially registering user IDs rather than actual users.

It was not surprising from 2000 to 2005, 70% of all online fraud reported was related to online auctions according to a fraud reporting agency (www.fraud.org). Since then, researchers have been working to identify problems, hoping to provide users with a fair and trustworthy online auction environment (Viegas, 2007). Knowing this problem, eBay offered an ID verification service through Equifax, a credit report agency, to cross-check user's contact information. But, credit cards do not provide any connection with the user's unique physical features; one person may use different names, bank accounts and addresses to obtain many credit cards. The severity of online auction fraud has become so great that it has attracted the attention of the Federal Bureau of Investigation (Wilcox, 2000).

EFFECTS ON USER BIDDING BEHAVIORS

In a traditional auction, the auction house performs the role of a mediator between the seller and the buyer by taking possession of the item first, then providing services such as verifying the authenticity of the item, estimating its market value, running the auction and collecting the payment (Kagel, 1998; Shaw, Blanning, Strader, & Whinston, 1999). However, in the online auction business, the sellers and buyers in online auctions not only have to make their own judgments on the authenticity, quality

and value of the item, and determine when to place bids, they also have to determine the trustworthiness of the buyers or sellers (Malaga, 2001; Resnick, Zeckhauser, Friedman, & Kuwabara, 2000; Segev, Beam & Shanthikumar, 2004).

Shill bidding

Shill bidding is the deliberate placing of bids (usually by sellers) to artificially drive up the price of an item (Dobrazynski, 2000). Now on eBay, bidding on one's own item is considered shill bidding and is prohibited at any online auction. That said, it remains difficult for auction authorities to detect since there are no face-to-face interactions in online auctions (FBI report, 2002). Vakrat & Seidmann (2000) have suggested that the most effective way of preventing shill bidding is to make it uneconomical for the seller to do so, and they also designed a fee schedule for auctioneer to discourage the seller from shill bidding. In the next section, we will explain how one user can user different IDs to defraud the system used to calculating seller reliability.

Reputation rating

Given that reputation is the foundation of all business transactions, it is especially true in person-to-person online transactions (Wang, Hidvegi, & Whinston, 2002). Online auction participants rely heavily upon reputation ratings that are provided by the online auction sites (Kauffman & Wood, 2005). Landon and Smith (1998) demonstrated that the users with a higher reputation rating tend to sell items at a higher price. Some sellers even set up filters in their auctions so only the buyers with or above a certain reputation point level are allowed to participate (Bapna, Goes, & Gupta, 2001). However, in online auctions, especially in person-to-person transactions, it is extremely difficult for buyers to gather information about the true condition of the item and about the honesty and responsiveness of the sellers.

Reputation systems usually contain two parts: numerical rating (1 for positive, 0 for neutral and -1 for negative) and a short comment (Gavish and Tucci, 2006). While reputation-rating systems have been receiving positive feedback from users, researchers quickly pointed out that there are several problems in the design of current systems, and significant challenges remain (Malaga, 2001; Resnick, Zeckhauser, Friedman, & Kuwabara, 2000).

One of the most difficult problems is how to ensure credibility in the ratings (Lin, Li, Janamanchi, & Whinston, 2006). A user could set up many fake transactions between different IDs, then raised the reputation scores on the two accounts that were

involved. As a result, the reputation ratings were artificially inflated. Current form of reputation rating systems is rating the user IDs, not the actual individual. In the remaining part of the paper, the author will set forth a user authentication protocol that could shine some light on the search for a solution for this problem.

USER AUTHENTICATION PROTOCOL

The author proposes a user authentication protocol to aid in authenticating online auction user's identity through the combination of a user's IP address, timestamp, user ID and cryptograph technique. It is designed to provide the online auction with more user information beyond just user IDs and passwords. Since the IP address is on the tickets, if two different user IDs from the same address are participating in the same auction, then the auction authority may have reason to suspect that these two user IDs might be controlled by the same person who is engaging in shill bidding or that the auction has been set up solely to inflate reputation ratings.

In the case of dynamic IP address used in part of the network, where IP address changes each time a user logs in. Given the trend that biometric identification techniques have become much more accessible to the average user, it is possible that in the near future fingerprint could be used in place of IP address in this protocol. In any case, with IP address or with biometric ID, the authentication protocol proposed here still valid.

The user authentication protocol involves three entities: (1) the user who plans to participate in an online auction, (2) the ticket booth, which authenticates users and issues tickets to the them, and (3) an online auction site, which will grant permission to the buyers who can present a valid ticket to place their bids in the auction. In this section, we present the various components of the user authentication protocol: the user authentication protocol model, the user's credentials, the ticket-granting protocol, and the service-granting protocol.

The model of user authentication

The ticket booth keeps a database of all users and their passwords; it also keeps a database of all the online auctions that are active at the time. The ticket serves as permission for a buyer to participate in an auction. One ticket is only valid for one buyer to place his bid in a single auction within a predetermined short timeframe. The ticket will automatically expire if the time limit is exceeded.

The authentication protocol provides two levels of protection: (1) only the user with correct password will obtain the session key, which only works in a limited time.

(2) Since only a single user and a single auction service share the session key, any message is encrypted and securely transmitted. It provides authentication at the beginning of the communication, then all further communication are assumed to come from the authenticated entity. It also provide authentication and encryption for each message sent from one entity to another. With an asymmetric key system, it also provides encrypted communication between users and auctions. Overall, it takes four steps for a buyer to place a bid in any single auction. Figure 1 illustrates the four steps.

Figure 1 Authentication protocol

1. Applying for a ticket.
2. Granting ticket.
3. Requesting to bid in an auction.
4. Permission to bid in an auction.

The user's credentials

To aid in defining the functions of the protocol, the following abbreviations and symbols are defined in Table 1.

Table 1 Definitions of symbols

Symbols	Definitions
u	user
s	Auction services
t	Ticket Booth
addr	Network address
times	Beginning and ending time for the ticket
KB_{xB}	X's secret key
$KB_{x,yB}$	Session key for x and y
$\{m\}KB_{xB}$	Message encrypted in x's secret key
$TB_{x,yB}$	X's ticket to use y
$AB_{x,yB}$	Authenticator from x to y

There are two types of credentials used in the authentication protocol: the application and the ticket. An application has the following structure:

$$A_{U,S} = \{u, time\}K_{U,S}$$

The buyer generates an application every time he wishes to participate in an auction. The application contains the user ID and a timestamp, which is all encrypted in a session key shared by the user and the auction. The application serves two purposes: it sends the plaintext, which is encrypted in a session key. By doing so, it shows that the buyer knows the session key. A ticket is used to securely pass the identity of the ticket holder to the auction. It also contains an IP address and timestamp that the auction can use to ensure that the user submitting the ticket is the same user to which the ticket was issued. A ticket has the following structure:

$$T_{u,s} = s, \{u, addr, times, K_{u,s}\}K_s$$

A ticket is good for a single buyer and for a single auction. It contains the buyer's user ID, the name of the auction, the IP address of the buyer, and a timestamp. This information is encrypted in the auction's secret key. Once the buyer obtains the ticket, he can use it one time to bid in the auction before the ticket expires. The buyer would not be able to decrypt the ticket or modify the contents of the ticket in any way, since he does not know the auction service's secret key, but he can present it to the auction in its encrypted form. No one on the network can read or modify the ticket.

Applying for a ticket and the Ticket Granting Process

Whenever a buyer decides to participate in an auction, he sends to the ticket booth an application, which contains the buyer's ID and the name of the auction in which he wishes to participate. The ticket booth checks the identity of the buyer. If the application is approved, then the ticket booth generates a session key to be used between the user and the auction service. It encrypts the session key with the user's secret key, and it then creates a ticket for the user that authenticates him to the auction site. The ticket is encrypted with the auction's secret key. Finally, the ticket booth sends both messages to the user.

The buyer now decrypts the first message with his password and retrieves the session key. The buyer saves both the session key and the second message which contains the ticket to the auction. This process is illustrated in Figure 2.

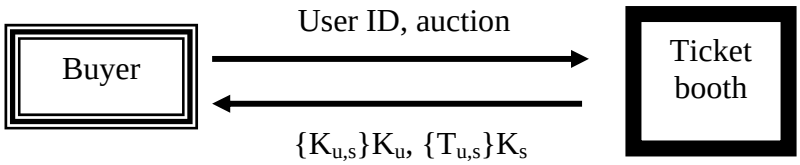

Figure 2 Ticket Granting Process

Service Granting Process

When the buyer sends the ticket to the auction, the auction decrypts the ticket and authenticates the buyer's identity. If everything matches, the auction knows that the user is who he claims to be, and grants the permission to bid in the auction. The auction and the buyer can encrypt future messages with the session key, if the buyer wishes to participate in the auction later. Since only the buyer and the auction service share this key, they both can assume that a future message encrypted with that key originated from the other party. This services-granting process is illustrated in Figure 3.

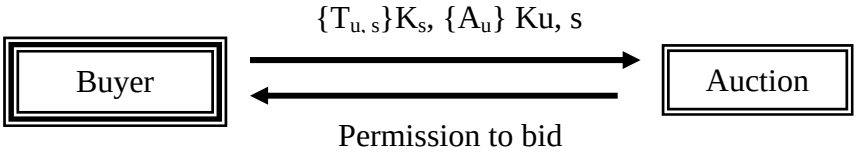

Figure 3 Service-Granting Process

CONCLUSIONS

This research has identified a fundamental problem in online auctions: the policy that allows one user to have multiple user IDs. Proposed protocol provides two levels of protection: first only the user with the correct password will obtain the session key; secondly, since only a single user and a single auction service share the session key, any message encrypted with it is securely transmitted and each ticket is only valid for one auction and for a very limited time.

The authentication protocol is a general-purpose authentication tool. It not only could be used in online auctions, it could also be applied to other e-commerce services as well. For example, in online dating services, this protocol could grant tickets to individuals, for use in obtaining dating services.

This research is only the beginning; many research topics in the area of identification and authentication remain. How the authentication protocol might be implemented in making the reputation rating system more meaningful and reliable would also be a question for significant research. Looking into future, as biometrics techniques become more accessible to the public, new approaches in identification/authentication technology could be applied to verification of users independent of user IDs.

REFERENCES

Bapna, R., Goes P., & Gupta, A. (2001). Simulating online Yankee auction to optimize seller revenue. Proceedings of the 34th Hawaii International Conference on System Sciences, USA.

Dobrazynski, J. (2000, June 07). F.B.I. Opens Investigation Of EBay Bids. *New York Times*, pp. C1.

FBI Report (2002). New Report Shows What Internet Scams Cost Americans Most, *Federal Bureau of Investigation Press Release*, FBI National Press Office, April 09, 2002.

Gavish, B., & Tucci, C. L. (2006). Fraudulent auctions on the internet. *Electronic Commerce Research*, 6(2), 127-140.

Kagel, J. (1998). Cross-game learning: experimental evidence from first-price and English common value auctions. *Economics Letters*, 49(2), 163-170.

Kauffman, R. J., & Wood, C. A. (2005). The effect of shilling on final prices in online auctions. *Electronic Commerce Research and Applications*, 4(1), 21-34.

Landon, S., & Smith, C. E. (1998). Quality expectation, reputation and price. *Southern Economic Journal*, 64(3), 628-647.

Lin, Z., Li, D., Janamanchi, B., & Whinston, A. (2006). Reputation distribution and consumer-to-consumer online auction market structure: an exploratory study. *Decision Support Systems*, 41(2), 435-448.

Lucking-Reiley, D. (2000). Auctions on the Internet: What's being auctioned, and How? *Journal of Industrial Economics*, 48(3), 227-252.

Lucking-Reiley, D., Byran, D., Prasad, N., & Reeves, D. (2007). Pennies from eBay: The determinants of price in online auctions. *Journal of Industrial Economics*, 55(2), 223-233.

Malaga, R. (2001). Web-based reputation management system: Problems and suggested solutions. *Electronic Commerce Research*, 1(4), 403-417.

Resnick, P., Zeckhauser, R., Friedman, E., & Kuwabara, K. (2000). Reputation systems. *Communications of the ACM*, 43(12), 45-48.

Segev, A., Beam, C., & Shanthikumar, J. G. (2004). Optimal design of internet-based auctions. *Information Technology and Management*, 2(2), 121-163.

Shaw, M., Blanning R., Strader. T., & Whinston, A. (1999). *Handbook of Electronic Commerce*. New York: Springer-Verlag Austin: R.G. Landes Co.

National Fraud Information Center. (2000). *Internet Fraud Statistics Report*. Retrieved September 10, 2009, from http://www.fraud.org/internet/intinfo.htm

Vakrat, Y., & Seidmann, A. (2000). Implications of the Bidders' Arrival Process on the Design of Online Auctions. Proceedings of the 33rd Hawaii International Conference on System Sciences, USA.

Viegas, J. (2007). *Pierre Omidyar: the Founder of Ebay (Internet Career Bios)*. The Rosen. New York: Publishing Group Inc..

Wang, Hidvegi & Whinston, A. (2002). Shill Bidding in Multi-round Online Auctions, Proceedings of the 35th Hawaii International Conference on System Sciences, USA.

Wilcox, R. (2000). Experts and amateurs: The role of experience in internet auctions. *Marketing Letters*, 11(4), 363-374.