

# Auditing Electronic Auction Systems

## Knowing the Risks

**Ladislav Beranek, Ph.D., CISA**, worked for Hewlett-Packard, CSOB Bank and other Czech IT companies as an IT security specialist. He specializes in IT security systems management, IT systems audit and IT security consultancy.

At present, many users participate in Internet-based (electronic) auction systems such as eBay (a US company with a revenue of US \$8.5 billion in 2008) or Aukro (a Czech company with a revenue of US \$100 million and 1 million users in 2008). In general, communication within an electronic auction system proceeds without the users being in physical contact or knowing anything of each other. As such, there are inherent risks in participating in electronic auctions. The primary risk is of losses resulting from nondelivery. While this risk is significant, there are other inherent threats in participating in electronic auctions, including the use of multiple identities to influence the auctions, identity theft and fabricated reputation.

What can be done to prevent and/or mitigate the risks inherent in electronic auctions? An effective approach includes the establishment of reputation mechanisms<sup>1</sup> (feedback rating system), user identity verification or fraud protection systems. The purpose of this paper is to highlight the nature of the various risks inherent in electronic auctions and to outline some controls to prevent and/or mitigate these risks.

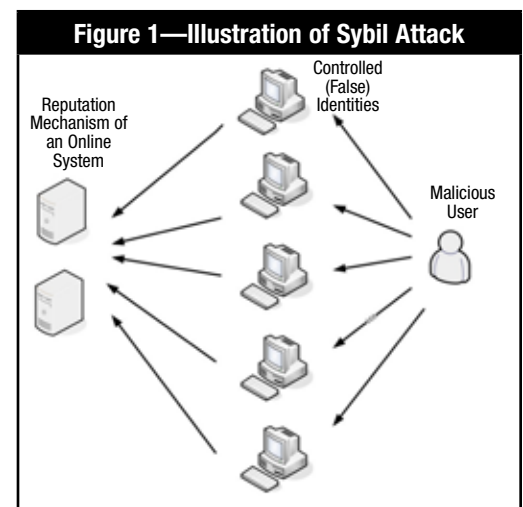
### ELECTRONIC AUCTION SYSTEM RISKS

Electronic auction systems pose many significant risks not traditionally considered in information system risk profiles. Most risks are difficult to quantify but have, nonetheless, serious potential implications, financial and otherwise (e.g., loss of electronic auction system credibility and thereby loss of customers).

The basis for the functionality of these systems is the creation of a trustful environment (trust in the system itself and trust among the users of this virtual world). As such, attacks on implemented mechanisms of trust could have a devastating effect on an electronic auction system. Therefore, risks connected with exposure of a trustful environment (reputation systems) are the focus of this article.

### Using Multiple Identities to Influence Electronic Auction Systems

In most electronic auction systems, it is not difficult to create a new identity. However, should individual users (or a group of users) control multiple identities, they could influence the reputation mechanisms in the online system for their own benefit (see **figure 1**). This behavior is called a “Sybil attack.”<sup>2</sup> In a Sybil attack, these identities are used in a coordinated fashion to influence the operations of an online system. For example, an attacker could create thousands of false identities to vote for one person in an election conducted online or use multiple identities to manipulate the reputation of an electronic auction user (a good reputation has shown to have a positive effect on the revenue of sellers<sup>3</sup>). The vulnerability of a system to a Sybil attack depends on how easy it is to create an identity in the particular online system. It also depends on how the system processes data obtained from the identities of the users of the online system. Nevertheless, in many applications, it is possible to stage the Sybil attack effectively using just a small number of controlled false identities.



### **Spurious Reputation**

If the creation of a new identity is not difficult and verification of user identities is not thorough, users can perform transactions without disclosing their real identity. It can result in a situation in which electronic auction users perform fraudulent actions and can escape the consequences of their behavior. They can discard their old electronic auction identity and acquire a new one (this behavior is called a “whitewashing attack”).

An example of this problem would be a user with a certain online identity (pseudonymity) who behaves well for a period of time and gains a good reputation through a series of well-performed transactions, and then commits fraud and leaves the original online identity to start a new one. Such a case was reported in May 2008 on the largest Czech electronic auction system, Aukro. The fraudsters used Aukro for a long time and earned a good reputation, expressed by positive evaluations from consumers. However, at some point, they began taking money from bidders without sending them auctioned goods, causing damages of more than US \$40,000.<sup>4</sup> Defense against such behavior is very difficult when real identities of users are not checked in detail and the creation of a new identity in the online system is easy.

### **Identity Theft**

Another major problem, identity theft, occurs when someone gains control over the identity of another user. One motivation for identity theft is for users to obtain a better reputation. Research shows that users with an established reputation can expect about 8 percent higher revenue than new sellers marketing the same goods.<sup>5</sup> More serious are targeted fraudulent actions to control a certain identity that is then used to perform fraudulent actions on electronic auctions. This is also called “account hijacking,” usually accomplished by phishing or password-guessing attacks. It is obvious that identities in electronic auction systems may have considerable economic value. They are sold for real money, often on electronic auctions and other electronic markets.

### **COUNTERMEASURES WITHIN ELECTRONIC AUCTION SYSTEMS**

An electronic auction system is a centralized online system with a central server that supports all functions of the electronic auction. The following mechanisms must be implemented within this system to ensure correct functioning

of respective electronic auctions: an identity verification system, fraud protection programs, secure payment mechanisms, escrow services, reputation (feedback rating) systems, trust mark seals, a complaint center and online dispute resolution services. In designing an effective audit, it is necessary to address a series of questions that will help determine the extent and details of the audit.

#### **Issue 1: Proper Identity Verification**

- How is identity verified?
- To what extent are data personally identifiable?
- Can users easily create multiple identities (accounts)?

Proper identity verification is the basic countermeasure against the use of multiple identities to influence electronic auction systems and against spurious reputations. Identity verification is the process by which users prove their real identity. Once verified, buyers or sellers are granted an icon or a mark to prove that their identities have been verified. In practice, identity verification on electronic auction systems is performed in one of the following ways:

- **E-mail verification**—The e-mail address used in the entry form is verified. The user may also be asked to physically mail in corroborating documents (e.g., identity documents). This method of identity verification is not too reliable because the user can forge identity documents.
- **Verification via the mailing address**—The electronic auction system operator verifies the data (name and address) entered into the system by the user. For example, the operator sends a letter with the system initialization password to the user. In this way, the user’s pseudonym can be associated with the user’s address. This method is more reliable than the first one because a successful delivery confirms the identity of a given user, at least to some degree.
- **Verification via fund transfer**—The user sends the electronic auction operator a small amount of money via a banking transfer or a payment card. The operator then associates the user’s pseudonym with a particular account number (e.g., payment card number). This method of identity verification is more reliable than previous methods (but not completely reliable because a stolen credit/payment card can be used to create a false identity). A disadvantage of this method is that many people are uneasy about providing credit/payment card details for nonpurchase purposes.

- **Trustful certification**—Trustful certification is based on a centralized authority whose purpose is to ensure that just one identity is associated with each person. Here, each new user is issued a certificate that will allow him/her to participate in the electronic auction. In reality, however, this method is not simple, because it practically requires face-to-face contact with every user to verify the user's identity. Therefore, this process may cause inconvenience for some users. For this process (of user identity verification) to be reliable, it cannot be automated. The process is costly and can result in slowing down the act of signing up new members. Also, the certification authority must secure a mechanism to revoke lost or stolen certificates. The main issues with this approach are its high cost and users' desire for privacy. For this reason, some electronic auction systems use this method only for chosen users (e.g., those who realize a considerable turnover on the particular electronic auction system). Such users are then marked by a special icon.

*Aukro.cz* uses verification via mailing address. This type of verification is not as reliable as, for example, verification via bank account (or credit card number); however, people in the Czech Republic are uneasy about giving credit card details for nonpurchase purposes (digital trust services are not as widespread in the Czech Republic).

In the US, electronic auction systems such as eBay use trustful certification. For example, VeriSign ([www.verisign.com](http://www.verisign.com)), a leading provider of digital trust services, provides verification services for buyers and sellers using its consumer authentication service (CAS), which is an XML-based web service for risk management and fraud prevention.

## Issue 2: Reputation System

- What is the functionality of the reputation system (the feedback rating system)? Is this system simple, graphical and understandable for the user? The perception of a reputation system by users is very important. When it is simple, graphical and understandable, users will trust it. If users consider the electronic auction system well designed and well managed, the system can operate successfully.
- Does the reputation mechanism of the online system deal with all identities identically? Does it filter the information obtained from new identities in a certain way? How does it create the reputation of new identities?
- How does the reputation system deal with newcomers?

- How does the reputation system deal with sellers and buyers with good feedback ratings?
- Does the reputation system give preference to sellers who consistently sell significant volumes of items and provide high standards of service (i.e., have high positive ratings)?
- Does the reputation system give preference to people with verified identities (see trustful certification)?
- To what extent are users' actions observable?

A reputation system operates by granting positive points for positive comments and negative points for negative comments. These points are then summarized. Potential buyers can always check the reputation (number of points) of sellers through their feedback ratings, which are accessible from the pages advertising any items they are selling. Thus, reputation serves as a basis for decision making on whether to enter into a transaction with a specific user (i.e., purchase of goods in an electronic auction). This mechanism is adopted by almost all electronic auction systems as a deterrent to fraud because most sellers are eager to maintain a good reputation to attract customers.

As mentioned previously, a Sybil attack can be used to influence the reputation of users (increasing or decreasing a reputation). The drawback is also the possibility of negative retaliatory feedback comments, which could affect the reputation of a buyer or a seller (also known as "racket by evaluation"). Of course, buyers or sellers with negative reputations can still use a different identity (username) or establish an account on a different electronic auction system.

Reputation systems are not effective against fraudulent "one-shot" sellers who do not intend to engage in subsequent transactions on the same electronic auction system.

On the other side, electronic auction systems mostly give preferential treatment to sellers who have consistently sold a significant volume of items, maintained a high positive feedback rating and provided a high standard of service. On *www.aukro.cz*, for example, such sellers are called "PowerSellers" and are granted a special icon. This icon is displayed next to the seller ID and acts as a strong assurance to buyers that they are dealing with an experienced, reputable seller.

## DEFENSE AGAINST THE USAGE OF MULTIPLE IDENTITIES

Generally, it is not easy to defend against the use of multiple identities to influence electronic auctions (Sybil attack). Because it can be a substantial problem, basic solutions are listed below:

- **Trustful certification**—As described and discussed previously, trustful certification is the only general solution capable of preventing the easy creation of multiple identities (with the aim to fraudulently influence an electronic auction). That means trustful certification is also the only approach fully capable of preventing a Sybil attack.
- **Verifying resources (users)**—The Completely Automated Public Turing Test to Tell Computers and Humans Apart (CAPTCHA)<sup>6</sup> verification to differentiate real users from robots, often used when registering at certain web sites, is an example of such an approach. The basic assumption for this method is that a Sybil attacker does not have sufficient resources (capabilities) to pass the required verification test for every identity the attacker has created for a planned Sybil attack. Other testing approaches include querying whether certain identities do not have fewer resources than expected (these tests include verification of computation capabilities, storage or memory capabilities, verification of network bandwidth, and eventually IP addresses). The reliability of most of these solutions is not very high because of potential measuring errors.
- **Analysis of users**—The analysis of users is usually utilized by large systems collecting data about consumers and trying to uncover cheating attempts. These systems analyze user behavior, exploring variances from the average consumer behavior in a given consumer segment. Automated analysis of the language used by participants in network discussions or techniques similar to click analysis (i.e., behavioral targeting) are other such methods.

Approaches exploiting social knowledge also belong to this category. The network of trust introduced in Pretty Good Privacy (PGP)<sup>7</sup> is an example of this approach. In such a case, social knowledge is used to limit the number of unknown, potentially malicious nodes. The number of such nodes is minimized as a result of minimum social interaction among “trustful” nodes and unknown, potentially malicious nodes. At present, social network methods able to detect attackers who use multiple identities have been designed. These methods use various graph algorithms.

- **Repeated fees for identity assignment or system usage**—This approach is a modification of the resource verification method. Here, identities are regularly subjected to

confirmation if the users want to continue using the system services. A regular fee for online system usage is generally a part of this method. This repeated validation of identities limits the number of entities that a Sybil attacker is able to create within a given time period with limited resources.

### Issue 3: Identity Theft

- Are suitable regulation and policies elaborated?
- Are web site sections with warnings and help for users published and easily accessible to users?
- Have appropriate prevention techniques and tools been implemented?
- Is a sound recovery plan in place in case of a successful attack?
- Has an effective incident response plan been developed well in advance?

Another major problem—identity theft—occurs when someone gains control over the identity of another user. However, the weakest link remains the uninformed, innocent customer who unwittingly responds to a phishing attack. Electronic auction users’ education is a critical success factor. It is crucial that suitable regulations and web site sections devoted to this problem are available to users.

### CONCLUSIONS AND RECOMMENDATIONS

This article has described the risks inherent in electronic auction systems and some controls to mitigate such risks. It is necessary to point out that a key aspect in decreasing these risks is public awareness of the best practices in buying and selling. Nevertheless, an auditor needs to review the control mechanisms used by electronic auction systems and make sure that all relevant risks are considered.

Electronic auction systems generally offer a certain level of protection, and fraud cases do not exceed a relatively small percentage of the total amount of transactions per year.<sup>8</sup> Electronic auction systems constantly keep increasing the level of security and trust in online trading, through the continuous implementation of antifraud measures and provision of guidelines for safe trading. At the same time, however, the nature of e-commerce makes it impossible to eliminate fraud completely, especially in countries that lack the necessary executive and legislative framework to deal with computer-related and cybercrime.

## ENDNOTES

<sup>1</sup> A reputation mechanism (reputation system) is an information system (centralized or distributed) that collects and evaluates automatically and systematically various subjective opinions about users within a respective online system (it determines the reputation of users and presents it in the appropriate manner for other users) with the aim of enabling the estimation of trustworthiness of a certain user. This estimation can serve as a basis for other users to determine whether to perform a transaction (e.g., purchase some goods in an online auction) with this user.

<sup>2</sup> The name Sybil was introduced in Douceur, J., "The Sybil Attack," International Workshop on Peer-to-Peer Systems, 2002, [www.cs.rice.edu/Conferences/IPTPS02/](http://www.cs.rice.edu/Conferences/IPTPS02/). He was influenced by the title of a book (and film) about a woman suffering from a mental disorder that caused her to take on multiple personalities with different patterns of behavior and amnesia.

<sup>3</sup> University of Michigan, "Established eBay Sellers Get Higher Prices for Good Reputations," *ScienceDaily*, 8 July 2006, [www.sciencedaily.com/releases/2006/07/060708083957.htm](http://www.sciencedaily.com/releases/2006/07/060708083957.htm)

<sup>4</sup> "Internet Auction Aukro.cz Hit by Swindlers," *Ihned.cz*, Czech Republic, 2008, [www.ihned.cz/c3-24886530-000000\\_d-internetovou-aukci-aukro-cz-zasahli-podvodnici](http://www.ihned.cz/c3-24886530-000000_d-internetovou-aukci-aukro-cz-zasahli-podvodnici)

<sup>5</sup> *Ibid.*

<sup>6</sup> CAPTCHA is the turing test that is used on the Internet to automatically distinguish real users from robots. The most frequently used test is based on an image in a picture with misshapen text. The user is to copy the displayed text into an appropriate input field. In doing so, it is supposed that the human brain will be able to distinguish the misshapen text, but Internet robots using optical character recognition (OCR) technology will not be capable of recognizing the text.

<sup>7</sup> Feisthammel, Patrick: "Explanation of the Web of Trust of PGP," [www.rubin.ch/pgp/weboftrust.en.html](http://www.rubin.ch/pgp/weboftrust.en.html)

<sup>8</sup> US Bureau of Justice Assistance, Internet Crime Report, USA, [www.ic3.gov/media/annualreport/2008\\_IC3Report.pdf](http://www.ic3.gov/media/annualreport/2008_IC3Report.pdf)

The *ISACA Journal* is published by ISACA®. Membership in the association, a voluntary organization serving IT governance professionals, entitles one to receive an annual subscription to the *ISACA Journal*.

Opinions expressed in the *ISACA Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of ISACA and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this *Journal*. *ISACA Journal* does not attest to the originality of authors' content.

© 2010 ISACA. All rights reserved.

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, MA 01970, to photocopy articles owned by ISACA, for a flat fee of US \$2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

[www.isaca.org](http://www.isaca.org)