

안전하고 효율적인 전자 경매 시스템에 관한 연구

박장수*, 서대희*, 이임영*, 김주한**
순천향대학교 정보기술공학부*
한국전자통신연구원**

A Study on Secure and Efficient in Electronic Auction System

Jang-Su Park*, Dae-Hee Seo*, Im-Yeong Lee*, Ju-Han Kim**
Division of Information Technology, Soonchunhyang Univ.*
Electronic and Telecommunications Research Institute**

요약

컴퓨터와 네트워크 발전으로 인한 인터넷의 확산은 오프라인으로 제공되던 많은 서비스들을 온라인화로 변화하는 계기가 되었다. 이러한 다양한 온라인 서비스중의 하나가 전자 경매이다. 전자 경매란 오프라인 경매 시스템의 취약점을 보완하여 온라인으로 경매가 가능하도록 하는 서비스이다.

따라서 본 논문에서는 상호 인증서 교환을 가정으로 하여 안전하고 효율적인 전자 경매 시스템 구축을 위해 공개키 암호화 방식과 해쉬 함수를 이용하면서 사용자의 편리성이 제공되는 전자 경매 시스템을 제안 및 구성하였다.

1. 서론

컴퓨터와 네트워크 발전으로 인한 인터넷의 급격한 확산은 소수 관심층만이 전자 상거래를 이용하는 단계에서 일반 대중에 의한 상거래 수단의 하나로 대중화 단계에 들어서고 있다. 인터넷을 이용한 전자 상거래의 경우 물건을 사고자 할 때 특정 장소에 가지 않고도 집에서 물건을 주문하고 받아 볼 수 있다. 이러한 편리성으로 인하여 인터넷을 이용한 전자 상거래 등은 폭발적으로 시장이 확대되고 있다. 특히 기존의 인터넷 쇼핑몰 이외에 다양한 형태의 전자 상거래 유형이 나타나고 있으며 그 중에서는 가장 주목을 끌고 있는 것이 바로 전자 경매이다. 기존의 오프라인 경매에서 사용자의 만족도를 만족 시킬 수 없는 부분을 대리 만족 시켜 주는 하나님의 응용 서비스로서 전자 상거래 환경에 재미라는 다분히 오락적인 요소를 제공한다. 따라서 사용자는 단지 구매에 대한 만족감 이외에도 오락적인 요소를 추가함으로써 현실 쇼핑의 만족도를 충족시킬 수 있는 인터넷 서비스 사업인 것이다.

그러나 단순히 경매를 위한 웹 페이지만을 구축하여 서비스를 제공할 경우, 경매과정이 불투명하거나, 사용자간의 공모를 통한 부정이 발생하게 된다면 전자 상거래 환경에서의 실제 적용은 많은 보안적문제점을 발생 시킬 수 있다. 따라서 안전하고 효율적인 전자 경매 서비스를 제공하기 위해서는 경매에 참가하는 사용자들에 대한 개인의 프라이버시 보호 및 경매 과정 시 모든 정보에 대한 안정성과 투명성을

보장해야 한다.

따라서 본 논문에서는 기존 전자 경매 시스템에 보안적취약점을 분석하여 전자 경매 시스템이 가져야 하는 보안적 요구 사항을 제시하고, 이를 만족시킬 수 있는 안전하고 효율적인 전자 경매 시스템을 제안 및 구현하고자 한다.

2. 기존방식 분석

본 장에서는 현재 상용화 서비스를 제공하고 있는 방식에 대해 알아보고 보안적취약점을 분석하고자 한다.

3.1 옥션

(주) 옥션(<http://www.acction.co.kr>)[4]은 128bit의 SSL암호화 전송 방식을 사용하고 있으며 적용되는 페이지는 회원가입, 로그인 시점과 카드결제가 되는 시점만 제공되고 있다. 또한 물품에 대한 입찰을 할 때 구매자가 보는 것은 판매자의 아이디이며, 입금확인 후에는 이름, 전화번호, 주소가 판·구매자(거래당사자)에게만 전송 된다.

그러나 옥션의 경우 사용자의 익명성을 제공하지 못하고 있으며 경매가 완료된 후에 발생할 수 있는 송·수신에 대한 부인봉쇄 서비스를 제공하지 못하고 있어 분쟁의 여지가 발생하고 있다. 또한 그 이외에 편리성 부분에 대한 취약점을 지적할 수 있다. 옥션의 경우 사용자 정보 및 제품 정보 이외의 많은 정보 요구로 인한 사용자의 편리성을 제공하지 못하고 있다.

3.2 eSALE

eSALE(<http://www.esale.co.kr>)[5]은 SSL 및 SET 암호화 전송 방식을 사용하고 있으며 SSL이 적용되는 페이지는 회원가입, 로그인 시점 SET이 적용되는 페이지는 카드결제가 되는 시점에서 제공되고 있다. 또한 물품에 대한 입찰을 할 때 구매자가 보는 것은 판매자의 아이디이며, 입금확인 후에는 이름, 전화번호, 주소가 판·구매자(거래당사자)에게만 전송 된다.

그러나 eSALE의 경우 사용자의 인증 부분에서 단순 ID를 기반으로 이루어져 사용자의 ID가 도용될 경우 발생할 수 있는 인증 문제와 더불어 경매가 완료된 후에 발생할 수 있는 송·수신자에 대한 부인봉쇄 서비스를 제공하지 못하고 있어 그 문제점을 지적할 수 있다. 또한 eSALE 서비스도 옥션과 같이 편리성 부분에서는 경매 정보 이외의 정보를 사용자 입력을 요구함으로써 발생할 수 있는 취약점을 지적 할 수 있다.

[표 1] 기존 방식 분석

	옵션	eSALE
기밀성	○	○
무결성	○	○
인증	○	X
부인봉쇄	X	X
공정성	○	○
편리성	X	X

3. 전자 경매 요구 사항

인터넷이라는 공개 통신로에서 전자 경매를 서비스할 경우
불법적 제 3자에 의한 사용자의 프라이버시와 경매 정보의
보안성을 유지하기 위해 다음과 같은 보안 요구 사항을 만족해야 한다.

① 기밀성

경매를 진행하는 동안 관련 정보들이 불법적인 제 3자에게 공개되지 않아야 한다

② 무결성

사용자들의 개인정보 및 경매 관련 정보들이 공개 통신로에서 불법적 제 3자에 의한 변·위조 되지 않아야 한다

③ 인증

오프라인 경매와는 달리 전자 경매는 정당한 사용자의 인증 과정이 필수적으로 요구된다.

④ 부인봉쇄

전자 상거래에서 발생하는 모든 거래에 대해 필요한 것으로서, 경매에서도 판매자가 제시한 경매 가격에 대한 전송 사실을 부인하거나 수신사실을 부인방지를 위한 서비스를 제공해야 한다.

⑤ 공정성

전자 경매 서비스에 대한 신뢰성을 확보할 수 있는 공정성을 제공해야 한다.

⑥ 편리성

전자 경매 시스템은 모든 사용자에게 쉬운 인터페이스를 통한 편리성을 제공해야 한다.

⑦ 독립성

경매 시스템의 각 구성요소들은 독립성을 통한 공모 방지 서비스를 제공해야 한다.

4. 제안 방식

본 장에서는 기존의 경매 시스템들의 보안적 취약점을 보완하기 위해 공개키 암호화 방식과 해쉬 함수를 이용한 안전한 전자 경매 시스템을 제안 및 구현하고자 한다.

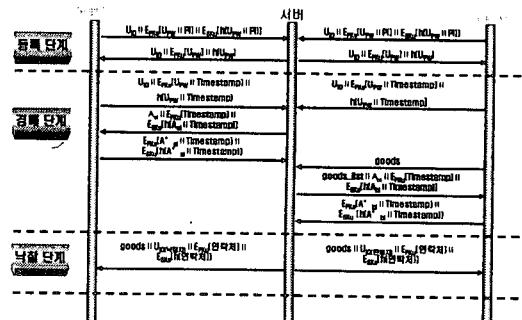
4.1 시스템 계수

다음은 안전하고 효율적인 전자 경매 시스템을 제안 및 구현하기 위한 시스템 계수를 기술한다.

- E_{PKu} : 사용자의 공개키 • E_{SKu} : 사용자의 비밀키
 - E_{PKs} : 서버의 공개키 • E_{SKs} : 서버의 비밀키
 - U_{ID} : 사용자의 아이디 • U_{PW} : 사용자의 패스워드
 - PI : 사용자의 정보 (Personal Information)
 - A_{si} : 물품등록 용지
 - $A_{\dot{si}}$: 기입된 물품등록 용지
 - $goods$: 상품명
 - $goods_list$: 상품명 리스트
 - A_{bi} : 입찰용지
 - $A_{\dot{bi}}$: 기입된 입찰용지
 - $Timestamp$: 타임스탬프

4.2 프로토콜

기존의 인터넷에서 서비스 중인 경매 시스템들의 프로토콜을 보면 기본적으로 물품등록, 입찰, 낙찰자 결정 및 공고, 낙찰대금 지급, 물품 배송의 순서대로 이루어지고 있다. 본 논문에서는 낙찰자 결정 및 공고까지 구현 한 것으로 [그림 1]과 같이 등록, 경매, 낙찰의 3단계로 이루어진다.



[그림 1] 제안방식 프로토콜

(1) 등록 단계

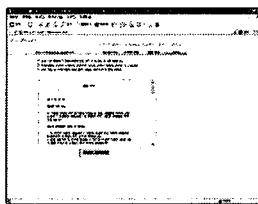
- ① 경매참가 희망자는 자신이 사용할 패스워드와 자신의 정보에 해쉬 한 값에 사용자의 서명을 한 것과 패스워드 자신의 정보를 서버의 공개키로 암호화 한 것과 자신이 사용할 ID를 서버에 전송한다. 사용자의 등록 정보 전송 내용은 다

음과 같다.

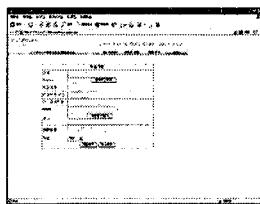
$$U_{ID} \parallel E_{PKs}[U_{PW} \parallel PI] \parallel E_{SKu}[h(U_{PW} \parallel PI)]$$

- ② 경매 서버는 등록을 요청한 경매 참가 희망자의 자격을 심사한 후, 희망자에게 유일한 ID 및 패스워드를 발급한다. ID와 패스워드 발급시 전송되는 내용은 다음과 같다.

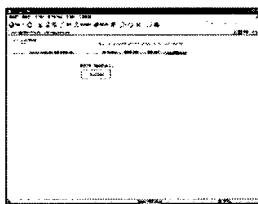
$$U_{ID} \parallel E_{PKu}[U_{PW}] \parallel h(U_{PW})$$



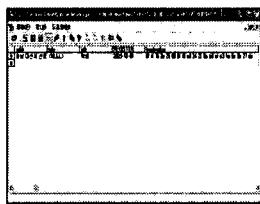
[그림 2] 약관



[그림 3] 회원가입



[그림 4] 가입 확인



[그림 5] 저장된 데이터

(2) 경매 단계

경매 단계의 사용자는 물건을 파는 판매자와 물건을 구입하는 구매자의 프로토콜로 구분된다.

• 판매자의 경매 프로토콜

- ① 등록 단계에서 발급 받은 ID와 패스워드로 경매사이트에 접속을 한다. 로그인시 전송되는 내용은 다음과 같다.

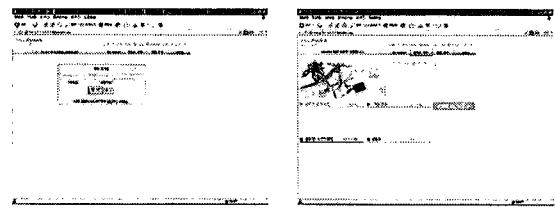
$$U_{ID} \parallel E_{PKs}[U_{PW} \parallel \text{Timestamp}] \parallel h(U_{PW} \parallel \text{Timestamp})$$

- ② 경매 서버는 판매자에게 물품등록용지와 판매자의 공개키로 *Timestamp*를 암호화 한 것과 물품등록용지와 *Timestamp*를 해쉬 한 값에 서버의 서명을 하여 전송한다. 물품등록용지 전송되는 내용은 다음과 같다.

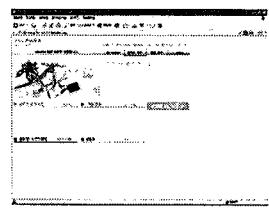
$$A_{si} \parallel E_{PKu}[\text{Timestamp}] \parallel E_{SKs}[h(A_{si} \parallel \text{Timestamp})]$$

- ③ 판매자는 물품등록용지를 받아 기입을 한 다음 *Timestamp*와 같이 서버의 공개키로 암호화 한 것과 기입된 물품등록용지와 *Timestamp*를 해쉬 한 값에 판매자의 서명 한 것을 전송한다. 물품등록시 전송되는 내용은 다음과 같다.

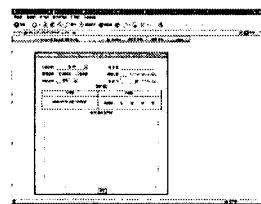
$$E_{PKs}[A^*_{si}] \parallel \text{Timestamp} \parallel E_{SKu}[h(A^*_{si} \parallel \text{Timestamp})]$$



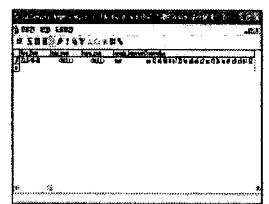
[그림 6] 로그인



[그림 7] 로그인 확인



[그림 8] 물품 등록 용지



[그림 9] 상품 데이터

• 구매자의 경매 프로토콜

- ① 로그인 과정은 판매자와 동일하다. 로그인시 전송되는 내용은 다음과 같다.

$$U_{ID} \parallel E_{PKs}[U_{PW} \parallel \text{Timestamp}] \parallel h(U_{PW} \parallel \text{Timestamp})$$

- ② 구매자는 자신의 필요로 하는 상품에 대한 정보를 서버에 요청을 한다.

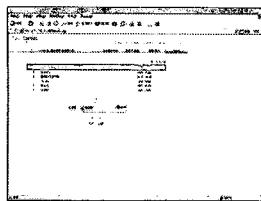
goods

- ③ 경매 서버에서는 구매자가 요청한 상품에 대한 상품리스트와 입찰용지와 구매자의 공개키로 암호화 한 *Timestamp*과 입찰용지와 *Timestamp*를 해쉬 한 값에 서버의 서명을 하여 전송한다. 전송되는 내용은 다음과 같다.

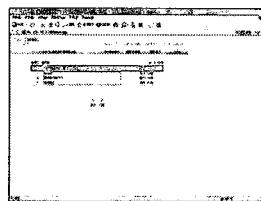
$$\text{good_list} \parallel A_{bi} \parallel E_{PKu}[\text{Timestamp}] \parallel E_{SKs}[h(A_{bi} \parallel \text{Timestamp})]$$

- ④ 구매자는 서버에게 받은 입찰용지에 기입을 한 다음 *Timestamp*과 같이 서버 공개키로 암호화 한 것과 기입된 입찰용지와 *Timestamp*이 해쉬 한 값에 구매자의 서명 한 것을 전송한다. 입찰시 전송되는 내용은 다음과 같다.

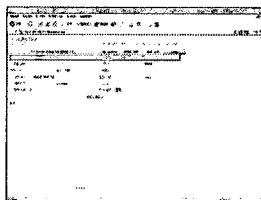
$$E_{PKs}[A^*_{bi} \parallel \text{Timestamp}] \parallel E_{SKu}[h(A^*_{bi} \parallel \text{Timestamp})]$$



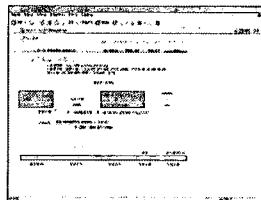
[그림 10] 물품 리스트



[그림 11] search 리스트



[그림 12] 상품 정보



[그림 13] 입찰 용지

ID	BuyerID	BuyerName	BuyerCost	BuyerPhone
1	100001	Buyer001	25000	02-99-43-45-56-25-78-88-54-38-01-00-42-2a-2b

[그림 14] 입찰 데이터

(3) 낙찰 단계

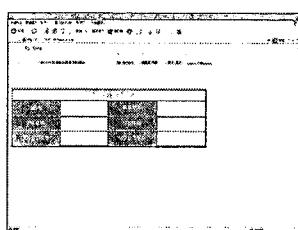
경매 서비스는 판매자와 구매자에게 낙찰공고를 하게 된다.

- ① 판매자에게는 상품명, 낙찰자ID, 낙찰자의 연락처를 전송한다. 전송되는 내용은 다음과 같다.

$goods \parallel U_{Id(\text{낙찰자})} \parallel E_{PKu[\text{연락처}]} \parallel E_{Sks[h(\text{연락처})]}$

- ② 구매자에게는 상품명, 판매자ID, 판매자의 연락처를 전송한다. 전송되는 내용은 다음과 같다.

$goods \parallel U_{Id(\text{판매자})} \parallel E_{PKu[\text{연락처}]} \parallel E_{Sks[h(\text{연락처})]}$



[그림 15] 낙찰 공고

5. 제안 방식 분석

제안 방식의 경우 기존 방식과 비교하여 다음과 같은 보안적인 특징을 제공한다.

- ① 기밀성 : 본 제안 방식에서는 공개키 암호화 방식을 이용해 불법적 제 3자에 의한 데이터의 기밀성 침해를 보완하

였다.

② 무결성 : 해쉬 함수를 이용하여 데이터의 위·변조를 해결하여 무결성의 보안 서비스를 제공하였다.

③ 인증 : 제안 방식은 초기 가정에서 인증서를 상호 교환함으로써 상호 인증을 통한 안전성을 유지하도록 하였다.

④ 부인봉쇄 : 사용자가 물품의 등록, 입찰의 사실을 부인할 경우 전자 서명을 이용하여 부인방지 서비스 제공이 가능하다.

⑤ 공정성 : 본 제안 방식에서는 경매 객체의 공정성을 부여하기 위해 상호 인증 서비스와 더불어 부인봉쇄 서비스를 제공함으로써 공모로 인해 발생 할 수 있는 공정성 침해 요소를 방지하였다.

⑥ 사용자의 편리성 : 회원가입시, 물품등록시, 입찰시 정보 입력을 최소한으로 하고 쉬운 인터페이스를 통하여 사용자의 편리성을 제공하였다.

6. 결론 및 향후 발전 방향

최근 인터넷 서비스는 다양화된 서비스 개발과 더불어 대중화를 통한 사용자 생활과 밀접한 연관 관계를 유지하고 있다.

그 중에서도 전자 경매 서비스의 경우 사용자의 상품 구매뿐만 아니라 서비스 사용시 경매라는 요소를 추가시킴으로써 그 효율성이 높아지고 있다.

본 논문에서는 안전성과 효율성을 동시에 만족할 수 있는 전자 경매 서비스를 제안 및 구현하였다. 제안된 방식의 경우 기존 방식에서 취약점으로 문제시 되고 있는 보안적 사항을 만족할 수 있었다.

그러나 본 방식의 경우 보안적인 서비스를 제공함으로써 발생할 수 있는 여러 가지 추가적인 연산량은 고려하지 않아 사용자의 편리성 부분에 대한 문제점을 완전히 해결하지 못하였다. 따라서 향후 본 논문에서 고려되었던 사항을 기반으로 모바일을 기반으로 한 경매 시스템을 제안 및 구성하기 위해 사용자의 편리성과 효율성 부분을 개선한 연구가 지속적으로 이루어져야 된다.

7. 참고 문헌

- [1] 최용락, 서우영, 이재광, 이임영, “컴퓨터 통신보안”, 도서출판 그린, 2001
- [2] 이임영, “전자상거래보안입문”, 생동출판사, 2001
- [3] 안철현, “인터넷 경매와 인터넷 쇼핑몰에 대한 인식차이와 사용의도에 관한 연구” 서울대학교 석사학위논문, 2000
- [5] (주) 옥션, <http://www.auction.co.kr>
- [6] (주) 이셀피아, <http://www.esale.co.kr>