Java보안기술을 이용한 전자 경매시스템 개발

윤 두 식† · 박 현 동† · 이 종 후† · 이 만 호†† · 류 재 철††

요 약

인터넷이 보다 대중화되면서 웹을 통한 다양한 서비스가 창출되고 있다. 경매분야도 예외는 아니어서 현재 국내외에 여러 사이트에서 전자경매가 활발하게 진행중이다. 그러나, 대부분의 전자경매 시스템은 보안기능이 취약하여 사용자에게 큰 피해를 초래할 수 있어 이에 대한 대책이 시급한 실정이다. 이에 본 논문에서는 사용자에게 보다 안전하면서 편리한 전자경매 환경을 제공하기 위하여 Java 보안기술을 이용한 전자경매 시스템을 설계 및 구현하였다.

Development of an electronic auction system using Java security

Doo-shik Yoon† · Hyun-dong Park† · Jong-hu Lee† · Man-ho Lee†† · Jae-cheol Ryu††

ABSTRACT

As the Internet has progressed, the auction service has been provided on several sites. But, most servers have security vulnerabilities; it causes the critical damage to the users. So the countermeasure to prevent the damage is needed immediately. In this paper, we design and implement the secure electronic auction system using the Java security techniques.

1. 서 론

인터넷 사용량의 급속한 증가로 98년 현재 인터넷 사용자는 1억 2천만 명을 헤아리고 있고, 2005년에는 전 세계 인터넷 사용자 수가 3억 5천만에 육박할 것으로 전망된다[1]. 이에 따라 사람들이 정보를 얻는데 있어 인터넷에 의존하는 비율이 더욱 높아지게 되었다. 인터넷을 통해 제공되는 서비스 형태의 종류는 그 수를 헤아릴 수 없을 만큼 많아지고, 그 중 홈뱅킹이나 전자상거래는 그 범위가 급속하게 넓어지고 있다. 이러한 서비스중의 하나로 전자경매를 생각할 수 있다.

경매는 공지된 물품에 대해 구매를 요구하는 구매자들이 구매하려는 가격을 제시함으로써 낙찰자를 결정하는 방법이다. 예전에는 규모가 큰 물품이나 소장가치가 있는 일부 귀중품에 한해 시행되었으나, 인터넷의 발전으로 웹상에서 일반 사용자들을 위한 생활용품에 까지 그 범위를 넓히고 있다. 그러나 기존의 경매는 시간과 공간적 제약을 많이 받고 있어, 일반 소비자들이 경매에 참가하기란 그렇게 쉬운 일이 아니었다. 최근 들어 일부에서는 이를 전산화함으로써 특정 계층이 아닌 일반소비자에게도 경매에 참가하도록 유도하려는 움직임이 일고 있다. 그러나, 단순히 경매를 위한 웹 페이지만을 구축하고, 경매 물품만 공고한다고 해서 완벽한 경매시스템을 구축했다고 말할 수는 없다. 인터넷 상에서 경매서버를 운영하기 위해서는 경매에 참가하는 사용자들에 대한 완벽한 보호, 경매 진행 시에 경매내용에 대한 안전성과 투명성을 보장해야 완벽한 전자경매라 할 수 있을 것이다. 이에 본 논

※ 본 연구는 한국과학재단 특정기초연구과제(과제번호 : 97-01-00-06-01-3)연구비 지원에 의해 수행되었음
† 준 회 원 : 충남대학교 대학원 컴퓨터과학과
†† 종신회원 : 충남대학교 컴퓨터과학과 교수
논문접수 : 1999년 3월 30일, 심사완료 : 1999년 12월 9일

문에서는 실세계의 경매 과정을 인터넷 상에서 구현함에 있어 고려해야 할 사용자 보호와 인증을 실현함으로써 안전한 전자경매 시스템을 구현하고자 한다.

2장에서는 현재 인터넷에서 운영되고 있는 전자경매 시스템의 현황과 문제점에 대해 알아보고, 전자경매 시스템에서 꼭 갖추어야 할 요구사항을 정립한다. 3장에서는 새로운 전자경매 프로토콜을 설계함으로써 기존 경매시스템에 대한 해결책을 제시한다. 4장에서는 설계된 프로토콜을 이용하여 실제 구현한 시스템에 대해 소개하고, 이를 구현하는데 있어 필수적인 요소기술에 대해 기술한다. 마지막으로 5장에서는 결론과 향후 연구방향에 대해 기술한다.

2. 경매시스템의 현황 및 요구사항

2.1 기존 시스템의 현황과 문제점

4년 전부터 등장한 인터넷 경매사이트들이 전자상거래를 이용한 온라인 쇼핑의 한 축을 형성하며 급속한 속도로 성장해 지난 97년의 거래액이 29억 달러에 이르게 됐다. 이런 성장세를 고려할 때 2002년에는 526억 달러 규모로 성장할 것으로 예상돼 인터넷 경매 사이트들이 초미의 관심사가 되고 있다. 현재 인터넷 사용자들에게 잘 알려져 있는 경매 사이트로는 E-bay (www.ebay.com), onsale(www.onsale.com), 야후경매(auctions.yahoo.com)등을 꼽을 수 있고, 국내에서도 ㈜옥션(www.auction.co.kr), 골드뱅크, 세진, 메타랜드 등 수 없이 많은 사이트들이 운영되고 있으며, 새로 개설되고 있다.

(1) EBAY

현재 전세계적으로 가장 많은 회원을 보유하고 있으며 가장 활발한 거래를 이루고 있는 회사가 E-bay이다. 1998년 현재 인터넷 전체 경매 시장에서 70%의 매출을 차지했고 제품분류 항목만도 1600종류를 넘어 컴퓨터 등 300여만개의 제품을 판매한다. 이 사이트에서는 사용자의 신용평가와 물품에 대한 적정가격 및 객관적인 평가를 위해 전문회사에 의뢰를 함으로써 인터넷 상에서 신뢰성 있는 경매를 할 수 있도록 보장하고 있다. 또한 경매를 위한 전용 브라우저를 개발함으로써 안전한 경매를 보장하고 있다. 하지만, 일반 브라우저를 이용하는 사용자들에게 새로운 브라우저를 이용한다는 것은 또 다른 부담일 수 있다.

(2) ONSALE

온세일을 통해 물건을 구매하려면 먼저 이용자 등록을 해야 한다. 자신이 이용하고 있는 신용카드에 대한 정보와 물건이 배달될 곳의 주소 그리고 비밀번호 등을 입력하면, 즉시 이용자 번호가 발급돼 경매에 참여할 수 있게 된다. 이때, 사용자의 신용카드에 대한 정보와 개인 등록정보 등은 브라우저에서 제공하는 암호화 모듈 (SSL)을 이용하게 된다. 미국과 캐나다 이외의 국가들은 브라우저에서 40비트 암호화 만을 제공하기 때문에 해커에 의해 기 전송된 정보가 노출될 가능성이 매우 높다. 또한 경매 참여시의 인증 메커니즘은 Basic Authentication으로 이용자 번호와 Password를 사용하기 때문에 이 역시 네트워크 상에 존재하는 해커들에 의해 도청/재사용 될 가능성을 배제 할 수 없는 실정이다.

현재 운영되고 있는 대부분의 경매 사이트들은 사용자들의 정보나 경매내용을 그대로 네트워크 상에 전송함으로써, 특히 정보에 대한 기밀성과 무결성을 보장하지 못하고 있다. 이를 해결하기 위해 SSL을 이용해 사용자의 브라우저와 서버간에 전송되는 메시지를 암호화를 함으로써 안전한 통신을 시도하고 있다. 대부분의 경매 사이트들은 회원제로 운영되고 있는데, 등록된 회원을 인증하기 위해 ID와 패스워드만을 이용하는 Basic Authentication방식에 의존한다. 그러나 이 방법은 도청/재전송 공격에 상당한 약점을 갖는다.

이 때문에 경매 단계에서 정당한 사용자를 사칭해 경매에 참여하는 제 3자를 막을 수 있는 방법이 없다. 또한, 이러한 제약으로 인해 실시간 경매를 이루지 못하고, 경매 마감시간을 길게 함으로써 물품을 구매하고자 하는 사용자들에게 시간적인 낭비를 초래하게 한다.

2.2 전자경매 시스템의 요구사항

경매는 돈과 결부되어 있기 때문에 정당한 사용자가 아니면 반드시 경매에 참여시켜서는 안되며, 정당한 사용자라 하더라도 인터넷의 특성상 그 내용이 인터넷에 연결된 제 3자에게 그대로 노출될 수 있기 때문에 이를 보호해 줄 도구가 필요하다. 이러한 보안서비스를 위해 암호화 통신이 요구된다[2, 3].

(1) 기밀성 및 무결성

인터넷은 그 특성상 네트워크를 통해 전송되는 모든 정보를 네트워크에 존재하는 모든 사람들이 읽고 변경

할 수 있다. 안전한 상거래를 위해 이 정보들은 참여 당사자들 이외에는 그 누구도 읽거나 변경할 수 없어야 한다. 경매도 인터넷 상거래의 일종으로써 경매를 진행하는 동안 사용자의 개인 정보에 대한 암호화가 선행되어 내용의 노출 이나 변경을 방지해 주어야 한다.

(2) 인증

서로의 얼굴을 마주보고 물품을 경매하는 실세계 경매와는 달리 인터넷 경매는 서로를 확인 할 수 없는 상황에서 경매를 진행해야 한다는 커다란 부담을 안고 있다. 기존의 인터넷 경매는 정당한 사용자임을 확인하기 위해 미리 등록과정을 마치고, 그 등록과정에서 발급된 사용자 ID와 password로써 진위 여부를 확인하고 있다. 이 방법은 매우 초보적인 방법으로써 악의의 제 3자가 얼마든지 도청해서 재 사용할 수 있고 또한 경매에 불법으로 참가한 후 경매 가격 조작 및 임의로 낙찰시킴으로써, 경매 물품에 대한 사용자와 서버간의 분쟁을 일으킬 소지가 상당히 많다. 인터넷 상에서 안전한 전자경매 시스템을 구축하기 위해서는 이러한 Basic Authentication의 틀을 벗어나 서버와 사용자간에 진정으로 믿을 만한 인증 메커니즘, 즉 전자서명 기술이 절실히 요구된다.

(3) 송/수신 부인봉쇄

경매 참가자가 제시한 가격에 대해 참가자가 전송 사실을 부인하거나 서버가 수신 사실을 부인하면 정상적인 경매 진행이 불가능해진다. 그러므로, 경매가 진행되는 동안에 전송되는 중요한 정보에 대한 전자서명이 추가되어 송/수신부인 봉쇄가 가능해져야 한다.

(4) 실시간 처리

실제 경매는 물품에 대한 공고가 나간 후 경매 시간이 빠르면 수분, 아무리 늦어도 1시간을 넘는 경우가 없다. 그러나 인터넷 경매는 물품 공고가 올라간 후 경매 시간이 짧으면 1시간, 보통 일주일 정도가 된다. 경매를 통해 빠른 시간내에 물품을 구매하고자 하는 사용자에게 이보다 불편한 일이 없을 것이다. 경매 서버측에서도 낙찰자가 결정된 이후에 낙찰자가 정당한 사용자 인지, 지불 능력이 있는지 등을 전화나 E-mail을 통해 다시 한번 체크해야 하므로 경매 진행 과정이 상당히 길어질 수 밖에 없었다. 이러한 모든 일들을 신속하게 처리함으로써 보다 빠른 경매 라이프 사이클을 유지할 필요성이 생겨나게 되었다.

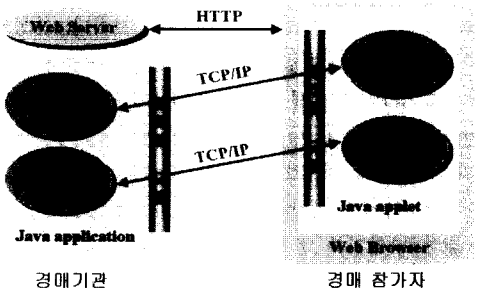
본 연구에서는 기존의 경매 서버가 가지고 있는 문제점들을 해결하기 위해 외부에 노출되어서는 안되는 모든 정보에 대한 암호화와 무결성을 제공한다. 또한, 전자서명을 이용한 송/수신 부인 봉쇄를 제공하여 보다 안전한 경매가 운영되도록 한다. 그리고, 암호화와 인증 메커니즘을 기반으로 경매 전반에 대한 전산화를 실현함으로써 실제 경매와 다름없는 실시간 경매를 구현한다. 3장에서는 기존의 경매사이트가 안고 있는 문제점들을 해결하기 위한 새로운 프로토콜을 제시한다.

3. 전자 경매 프로토콜의 설계

본 장에서는 기존의 경매 시스템들이 안고있는 문제점을 해결하기위해 Java 암호모듈을 이용한 안전한 전자 경매시스템 프로토콜을 제시한다.

3.1 시스템 구성

본 시스템의 전체 구성은 (그림 1)과 같다.



(그림 1) 전자 경매시스템 구성도

본 시스템의 각 구성요소는 다음과 같은 역할을 한다.

1) 웹 서버 (Web Server)
- 경매 물품 공고

2) 등록 서버 (Registration Server)
- 등록 회망자들과 공개키 교환. 이는 상대방의 서명을 확인하기 위해 사용
- 등록을 회망하는 사용자들로부터 등록 접수 및 유일한 ID발급

3) 경매 서버 (Auction Server)
- 등록한 사람들로부터 경매 참가 신청 접수

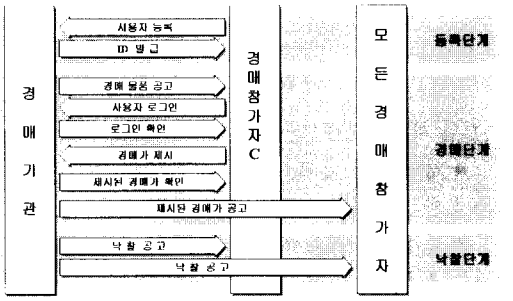
- 경매 참가자 데이터 베이스 유지 및 관리
- 경매시 모든 경매정보 관리 및 감시
- 제시된 경매가를 이용해 낙찰자 결정/통보

4) 등록 클라이언트 (Registration Client)
- 클라이언트를 위한 비밀키와 공개키를 생성한 후, 로컬 컴퓨터에 키 저장
- 등록 신청서의 데이터를 암호화하여 등록서버에 전송
- 발급받은 ID를 로컬 컴퓨터에 저장

5) 경매 클라이언트 (Auction Client)
- 경매 참가자로부터 경매서버로 전송하는 데이터를 암호화 및 서명한 후 전송
- 현재 제시되고 있는 모든 경매 상황을 경매 참가자에게 알려준다

3.2 경매 프로토콜

본 시스템은 (그림 2)와 같이 등록, 경매, 낙찰의 3단계로 이루어진다. 이 프로토콜은 기존에 서비스를 하고 있는 사이트의 경매 프로토콜과 큰 차이가 없지만, 전송중의 데이터에 대한 기밀성과 무결성, 전자서명 기술을 이용함으로써 안전성을 확보하고 실시간 처리를 지원할 수 있는 기능을 추가한 것이다. 등록단계는 경매에 참가하고자 하는 희망자가 경매서버에 등록을 하고 ID를 발급받는 단계이다. 경매단계는 경매서버에서 경매공고가 나오면 경매에 참여하고자 하는 참가자가 경매서버에 로그인 후, 경매가격을 제시함으로써 실제 경매를 진행하는 단계이다. 낙찰단계는 경매에 대한 낙찰자를 결정하고, 그 결과를 모든 참가자에게 알려주는 단계이다.



(그림 2) 전자경매 프로토콜

전자경매 프로토콜을 구현하기위해서는 메시지의 기밀성과 무결성, 전자서명을 위한 관용키/공개키 알고리즘을 사용한다. 각 단계에서 사용되는 암호화와 해쉬함수의 표기는 <표 1>과 같다.

〈표 1〉 암호 관련 기호

구 분	의 미
Ex	키 x로 메시지 암호화 예) E_{KS} : 세션키(관용키)로 암호화
C	참가자
S	서버
KSx	x가 생성한 세션키 예) KSc : 참가자의 세션키
Kux	x의 공개키 예) KUs : 서버의 공개키
KRx	x의 비밀키 예) KRc : 참가자의 비밀키
H[M]	메시지 M에 대한 해쉬값
C_{ID}	참가자 C의 ID
P_{ID}	경매물품의 ID

(1) 등록 단계

- 사용자 등록 : 경매에 참가를 희망하는 사용자가 미리 서버에 등록하는 단계이다. 경매참가 희망자는 해당 양식에 자신의 인적사항을 입력한 후 등록서버에 제출한다. 제출시 사용자의 인적사항과 기타 등록사항은 네트워크 상의 제 3자에게 노출되어서는 안되고, 또한 악의의 3자가 정당한 사용자를 사칭하여 거짓 등록을 하지 못하도록 등록정보를 사용자의 세션키(관용키)로 암호화하고, 사용자의 서명을 함께 서버에 전송하여야 한다. 등록정보를 암호화한 관용키는 서버의 공개키로 암호화되어 안전하게 전달된다. 또한 사용자의 인증서는 경매서버에 등록하기 전에 서로 교환할 수 있어야 한다. 본 논문에서는 등록단계에 사용자와 서버간에 서로의 공개키를 서로 교환함으로써 인증서를 교환했다고 전제한다. 내용은 다음과 같다.

$$E_{KS_C}[\text{사용자의 인적사항}] \| E_{KU_S}[KS_C] \| E_{KR_C}[H(\text{사용자의 인적사항})]$$

- ID 발급 : 경매 기관은 등록을 요청한 경매 참가 희망자의 자격을 심사한 후, 희망자에게 유일한 ID를 부여한다. 이때 ID는 서버의 전자서명을 붙여 전달한다. 사용자의 ID를 암호화하지 않는 이유는 사용자의 ID만으로는 제 3자가 사용자의 정보(이름이나

기타 등록사항)을 알 수 없기때문이다. 또한 ID에 서버의 전자서명을 붙이는 이유는 서버에서 발급한 ID가 정당한 것이고, 중간에 변조가 없음을 확인하기 위해서이다.

$$C_{ID} \| E_{KR_S}[H(C_{ID})]$$

(2) 경매 단계

- 사용자 로그인 : 경매에 참가하고자 하는 사용자는 정당한 참가자임을 증명하기 위해 서버에 로그인을 해야한다. 기존의 방식처럼 사용자의 ID와 패스워드를 가지고 등록할 경우 제 3자가 이를 갈취해 서버에 정당한 사용자로 로그인 할 수 있는 문제점이 있다. 이를 해결하기 위해 본 시스템에서는 사용자의 ID와 그에 대한 서명으로써 서버에 로그인한다. 사용자는 자신의 데이터에 대한 서명을 위해 로컬 컴퓨터에 저장되어 있는 비밀키를 복구할 필요가 있다. 이때 로컬 컴퓨터에 저장되어있는 비밀키를 복구하기 위해서는 사용자가 비밀키를 저장할 때 사용했던 패스 프레이즈를 이용한다. 패스 프레이즈에 대한 해쉬값을 세션치로 사용함으로써 비밀키를 저장하고 복구한다. 기존에 패스워드를 이용하는 방법은 8자 이내로 한정이 되기 때문에 입력할수있는 키보드의수 C_8 만큼만 시도를 하면 쉽게 알아낼 수 있는 맹점이 있기 때문에 본 연구에서는 이를 극복하기 위해 입력값을 길이에 구애를 받지 않는 패스 프레이즈를 이용한다. 패스 프레이즈가 해쉬 함수를 거치면 일정한 길이의 결과가 출력되는데, 이 값을 세션키로 이용하면 보다 안전한 세션키가 생성될 수 있는 것이다. 반면, ID에 대한 서명만으로 로그인을 할 경우 제 3자가 이 정보를 보관하고 있다가, 나중에 서버에 이 정보를 그대로 사용할 수 있는 재전송 공격이 가능하므로 ID와 TimeStamp를 동시에 사용함으로써 이를 방지할 수 있다. 서버는 사용자의 서명값을 사용자의 공개키로 복호화하여 ID와 TimeStamp값을 비교해 봄으로써 사용자의 정당성을 확인할 수 있다. 사용자가 서버에 로그인 시 전송되는 내용은 다음과 같다.

$$C_{ID} \| TimeStamp \| E_{KR_C}[H(C_{ID} \| TimeStamp)]$$

- 경매 시작 및 사용자의 경매가 제시 : 경매 시작시간이 되었거나, 경매에 참가할 수 있는 사용자 수에 이르면 곧바로 경매가 시작되는데, 경매 참가자는 애플릿으로 제공되는 경매 폼에 의해 경매를 진행할 수 있다. 참가자가 서버에 제시하는 경매정보는 경매물품의 ID (P_{ID})와 그에 대한 경매제시가격이다. 참가자가 경매정보를 서버에 전송할 때는 경매정보의 해쉬값을 구한 뒤 참가자의 서명을 붙임으로써 메시지의 무결성을 보장할 수 있고, 송신부인방지가 가능하다. 이때 해쉬함수의 입력값은 사용자의 ID, 경매정보(경매물품ID, 경매제시가), 그리고 메시지의 재사용을 막기 위한 타임스탬프등이 된다. 내용은 다음과 같다.

$$MsgOfC = C_{ID} \| \text{경매정보}(P_{ID}, \text{경매제시가}) \| \text{TimeStamp} \| E_{KR_C}[H(C_{ID} \| \text{경매정보} \| TimeStamp)]$$

- 제시된 경매가 확인 및 공고 : 경매서버는 경매 참가자 C가 제시한 경매정보에 대한 서명을 확인한 후, 경매가가 정당한 것임을 사용자에게 확인시켜줄 필요가 있다. 만일 이 사항을 경매가격을 제시한 참가자에게 확인시켜 주지 않는다면 참가자는 자신이 현재 제시한 경매가가 제대로 반영되었는지 확인할 수가 없고, 경매가 완료된 후에 사용자가 제시한 경매가를 서버가 받지 못했다고 주장할 수 있기 때문이다. 이처럼 수신부인봉쇄를 실현하기 위해 서버는 사용자의 메시지 (MsgOfC)에 자신의 서명을 붙여 경매가 제시자에게 전송한다. 또한 참가자 C가 경매가를 제시했을 때 현재 경매에 참가하고 있는 모든 참가자에게 현재 경매가를 공고함으로써 참가자들이 현재 경매가보다 더 높은 경매가를 제시하도록 해야한다. 제시된 경매내용이 서버에 의해 조작/변조되는 것을 방지하기 위해 참가자 C가 전송한 메시지(MsgOfC) 전체에 서버의 서명을 붙여 모든 참가자들에게 전송하는 방법을 이용한다. 이렇게 함으로써 각 참가자는 서버로부터 전송된 메시지의 서명을 확인하고, 필요한 경우 경매가를 제시한 참가자의 인증서를 이용해 경매가에 대한 정당성을 확인해 볼 수 있다. 이때 악의의 3자가 예전에 갈취했던 사용자의 경매제시가를 재사용하여 불법적으로 더 높은 가격을 제시함으로써 경매가를 저작할 가능성이 있다. 이를 방지하기 위해 서버는 현재 경매정보에 TimeStamp를 첨가하여 서명함으로써 이 문제를 해결할 수 있다. 서버가 각 참가자에게 전송하는 경매확인 메시지는 다음과 같다.

(3) 낙찰 단계

일정 시간동안 경매가가 올라가지 않거나, 1명을 제외한 모든 참가자가 경매포기를 했을 경우 낙찰자가 결정되며, 낙찰가는 가장 마지막에 제시되었던 경매가이다. 낙찰에 관한 정보는 모든 참가자에게 알려지게 되는데, 역시 낙찰자로 선택된 참가자의 경매정보와 서버의 전자서명을 붙여 모든 참가자에게 보냄으로써 낙찰가가 조작 및 변조되지 않았음을 확인할 수 있다. 참가자들에게 보내지는 낙찰정보는 다음과 같다.

$$MsgOfC_{\text{최종경매가제시자}} \| TimeStamp \|$$
$$E_{KR_S}[H(MsgOfC_{\text{최종경매가제시자}} \| \text{TimeStamp})]$$

이상에서와 같이 본 논문에서 설계한 프로토콜은 공개키와 관용키 알고리즘을 모두 이용함으로써 기존 시스템에서 제공하지 못하는 메시지 암호화와 무결성, 전자서명등을 제공함으로써 안전한 경매가 진행될 수 있다.

4. 전자경매 시스템 구현

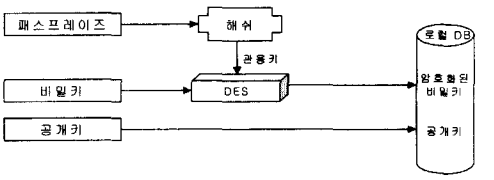
본 전자 경매시스템은 서버와 클라이언트 모듈로 크게 나뉘어 진다. 서버모듈은 서버 측에서 수행되는 Java Application이고, 클라이언트 모듈은 사용자의 웹 브라우저에서 수행되는 Java Applet이다. 이 모듈들에는 모두 암호화와 서명에 쓰이는 암호모듈(IAIK-JCE)을 포함하고 있기 때문에 네트워크 상에서 안전한 데이터 교환을 보장한다.

4.1 프로토콜의 구현

전자경매 시스템을 구동하기 전에 선행되어야 할 부분은 서로 상대방의 인증서를 전달하고 확인하는 과정이지만, 본 논문에서는 인증서를 생성하고 발급하는 CA가 구현되어 있지 않기 때문에 서버와 클라이언트가 공개키/비밀키 쌍을 생성 후, 등록단계에서 서로의 공개키를 교환하고 저장함으로써 상호 인증을 대신한다. 차후 CA가 구현될 경우 이 절차는 생략될 수 있다.

(1) 등록 단계

- 등록 서버 : 등록 서버는 경매 서버 머신에서 돌아가는 Java Application으로 초기에 서버의 공개키/비밀키쌍을 생성한다. 키를 생성한 후 안전한 곳에 보관해야 하는데, 공개키는 평문으로 저장해도 무관하지만, 비밀키는 외부에 공개가 되어서는 안되기 때문에 암호화 저장을 한다. 암호화에 쓰이는 관용키를 생성하기 위해 서버 관리자로부터 Passphrase를 입력받는다. Passphrase는 해쉬함수를 수행한 후, 그 결과를 관용키로 이용해 비밀키를 암호화한다. 키 저장과정은 (그림 3)과 같다.



(그림 3) 키 저장 과정

클라이언트의 접속을 확인하면, 서버는 클라이언트에게 자신의 공개키를 전송하고, 클라이언트로부터 등록정보를 기다린다.

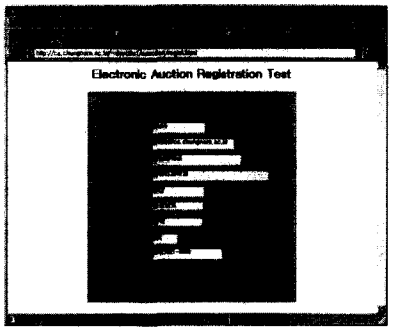
등록정보가 전송되면 서버는 등록 희망자의 자격을 심사한 후, 데이터 베이스에 등록정보를 저장하고, 클라이언트에게 유일한 ID를 발급한다. 이때, ID와 서버의 서명을 같이 전송함으로써 메시지의 무결성을 보장하게 된다.

- 등록 클라이언트

경매 서버에 등록을 희망하는 사용자가 웹 브라우저로 서버에 접속하게 되면, 등록 클라이언트 (Java Applet)가 웹 브라우저에 다운로드 된다. 이때 메시지 암호화와 서명에 쓰이는 공개키/비밀키쌍을 생성한다. 키쌍이 생성되면 이 역시 사용자만이 키를 복구할 수 있도록 암호화되어 로컬 컴퓨터에 저장된다. 서버에서와 마찬가지로 비밀키 저장을 위해 사용자에게 Passphrase를 문의하게 되는데, 원리는 (그림 3)과 동일하다.

키쌍이 안전하게 보관되면 Applet 폼의 등록 양식이 사용자에게 보여진다. 서버에 전송되는 등록정보는 네트워크 상의 다른 사람들에게 보여져서는 안되기 때문에 클라이언트가 생성한 관용키를 이용해 암호화해서 전송한다. 암호화에 사용된 관용키는 서버의 공개키를 이용해 암호화한 후 이 두 개의 메시지를 서버에 전송함으로써 메시지 기밀성을 보장받게 된다. (그림 4)는 웹 브라우저에 보여지는 등록정보 양식이다.

등록정보가 전송되면, 서버에서 유일한 ID가 발급되는데, 전송 받은 ID를 사용자의 로컬 컴퓨터에 암호화하여 저장함으로써 등록단계를 마치게 된다.



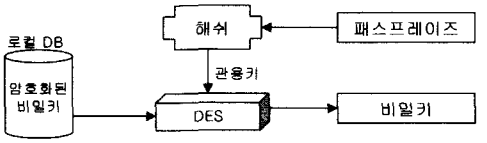
(그림 4) 등록정보 양식

(2) 경매 단계

● 경매 서버

경매 서버는 등록 서버와 마찬가지로 서버 머신에서 수행되는 Java Application이다. 경매 서버는 경매 진행의 모든 과정을 감시하고, 모든 참가자들에게 안전한 메시지 전송을 담당하는 역할을 한다. 경매 서버를 실행시키려면 먼저 서명에 사용되는 비밀키를 복구해야 하기 때문에 서버관리자의 Passphrase를 필요로 한다.

Passphrase를 입력받으면 이를 해쉬로 구한 값을 비밀키 복구를 위한 관용키로 이용한다. 관리자가 입력한 Passphrase가 다른 경우에는 3번까지 재 입력할 기회를 준다. 3회 이상 Phassphrase가 틀렸을 경우, 서버는 프로그램을 실행시킬 관리자가 정당하지 않다고 판단하고 자동으로 프로그램을 종료시킨다. 키 복구 과정은 (그림 5)와 같다.

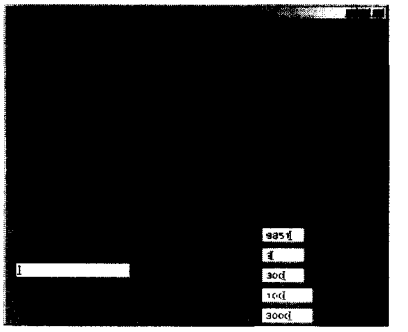


(그림 5) 키 복구 과정

관리자가 비밀키를 안전하게 복구하였으면, 클라이언트 접속을 위한 내용을 구성한다. 경매를 시작할 시간을 입력한 후, 경매 시작시간 이전에 참가를 희망하는 모든 경매참가 희망자의 적법성을 확인하고, 적법한 참가자일 경우에 경매 시작시간이 될 때까지 대기하도록 한다. 경매 시작시간이 되면 더 이상 참가희망자를 받지 않고 즉시 경매를 시작한다. 본 논문에서는 테스트 환경을 만들기 위해 한번의 경매가 이루어질 때마다 경매에 참가할 수 있는 인원을 제한한다. 따라서 경매를 시작할 수 있는 시점은 제한인원에 도달했거나, 경매 시작시간이 되었을 때이다.

시스템 구성이 완료되면 경매 서버는 경매 참가자들의 참여를 기다린다. 참가자수가 제한인원에 도달했거나, 경매 시작시간이 되면 경매가 시작되는데, 처음 시작할 때 모든 참가자들에게 초기 경매가를 공지한다.

경매 진행중 한 참가자가 경매가를 제시하면 서버는 경매 내용과 참가자의 서명을 확인한 후, 경매가 제시자의 메시지 전체와 TimeStamp, 또 그에 대한 서명을 붙여 모든 참가자에게 전송함으로써 경매 내용을 실시간으로 확인할 수 있도록 한다. 모든 참가자에게 보내지는 경매 상황은 사용자의 ID만을 이용함으로써 익명성을 보장받고, 서버 서명을 붙임으로써 경매 참가자들에게 무결성을 보장하게 된다. 서버측 관리자 역시 경매 진행상황을 볼 수 있도록 서버 모듈은 그 내용을 관리자에게 보여준다. (그림 6)은 관리자에게 보여주는 경매 진행 상황이다.

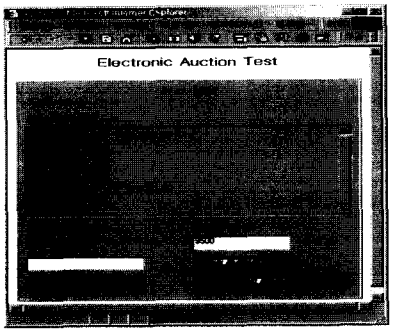


(그림 6) 경매 진행상황 - 서버측

● 경매 클라이언트

경매에 참가하기 위해서 사용자는 웹 브라우저를 이용해 서버에 접속해야 한다. 서버에 접속하면 Applet이 웹 브라우저에 다운로드되고, 경매를 시작하기 전에 서명을 위한 사용자의 비밀키를 복구한다. 사용자의 비밀키를 복구하기 위해 Passphrase를 문의하게 되는데, 이는 경매서버에서의 작동과 동일하다. 비밀키를 복구하고 경매에 참가하기 위해, 클라이언트 모듈은 사용자의 ID와 ID에 대한 서명을 이용해 서버에 로그인 하게 된다. 서버는 참가자의 ID와 서명을 확인하고 정당한 참가자임을 확인한다.

모든 참가자가 이 과정을 거치면 경매가 시작된다. 경매가 시작되면 화면에 초기 경매가가 제시되고, 참가자의 경매가를 기다린다. 참가자는 현재 경매가보다 높은 가격을 제시함으로써 경매를 실행하게 된다. 만일 현재 이하의 금액을 제시하면 클라이언트 모듈이 자동으로 이를 거부하고 새로운 가격을 제시하도록 메시지를 보여준다. 클라이언트가 전송하는 경매 내용은 참가자의 ID와 경매가격, 그리고 그에대한 전자서명이다. 참가자가 새로운 경매가를 제시하면 서버는 그 내용을 모든 참가자들에게 전송한다. 클라이언트는 그 내용에 대한 서명을 확인한 후, 참가자에게 현재 경매 상황을 보여주게 된다. (그림 7)은 실제 경매 과정을 보여준다.



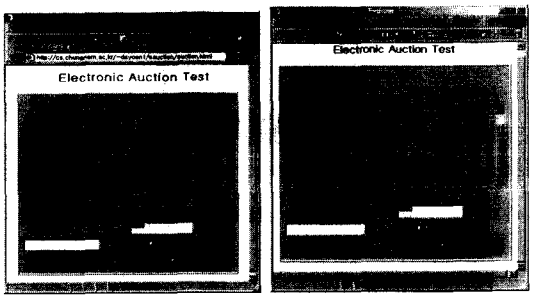
(그림 7) 경매 진행과정 - 사용자측

경매과정에서 일어나는 모든 내용은 서버의 데이터베이스에 기록되고, 일정기간 이상 보관하여 경매 종료 후에 일어날 수 있는 이의 신청에 대비한다.

(3) 낙찰 단계

참가자가 경매를 포기하고자 할 때에는 경매 포기 메시지를 서버에 전송하거나, 일정시간 이상 경매가를 제시하지 않으면 된다. 경매포기 메시지를 보내는 경우, 제 3자가 그 메시지를 변조하거나 본인으로 가장하여 포기메시지를 보내는 경우를 막기 위해 반드시 서명을 붙여 서버에 전송하고, 서버의 확인 메시지를 받는다.

경매가격이 일정 시간동안 오르지 않을 경우 서버는 자동으로 최후 경매가를 낙찰가로 결정한 후 모든 참가자들에게 알려준다. 모든 참가자들은 이 메시지를 확인하고 경매가 종료되었음을 알게 된다. (그림 8)은 낙찰 정보를 사용자에게 알려주는 과정이다. 낙찰자로 결정이 된 참가자는 서버에서 지원하는 지불 메커니즘에 의해 지불 단계를 거쳐야 한다. 본 시스템에서는 지불 단계는 구현되어있지 않다.



(그림 8) 낙찰자 확인과정

4.2 경매 시스템의 요소기술

본 시스템은 Java 암호모듈을 이용하여 실시간 전자경매시스템에 대한 기본적인 모델을 제공한다. Java는 인터넷상에서 다양한 서비스를 제공해줄 수 있는 가장 적합한 언어로 브라우저를 사용하고 있는 일반 사용자들에게 친숙한 인터페이스를 제공 할 수 있고, 다른 언어와 다르게 시스템 독립적이며 (System Independency), 가상 머신 (virtual machine)만 있으면 시간과 장소의 제약을 받지 않고 서비스를 받을 수 있다[4].

이를 전자상거래 시스템에 적용하기 위해서는 반드시 암호모듈이 필요한데 이러한 암호모듈 또한 제 3의 벤더에서 제공하는 Java 암호모듈을 이용함으로써 암호화와 서명에 대한 문제를 해결할 수 있다. 현재 인터넷에서 사용할 수 있는 암호모듈이 많은데 예를 들면, Cryptix, IAIK-JCE, J/CRYPTO, CEAL98등이 있다. 본 시스템에서는 IAIK-JCE를 이용해서 데이터 암호화 및 서명을 실현하고 있다[5].

또한 사용자의 브라우저에서 실행되는 경매 클라이언트(자바 애플릿)는 사용자의 컴퓨터에 인증서, 공개키, 비밀키등을 저장해야 할 필요가 있는데 이를 위해 사인드 애플릿(Signed Applet) 기술이 필수적이다.

(1) 인증서와 키 저장을 위한 사인드 애플릿 (Signed Applet)

자바 애플릿은 사용자의 컴퓨터에 인스톨되는 것이 아니기 때문에 사용자의 로컬 머신에 대한 보안제한이 존재한다[4]. 이는 자바의 샌드박스(SandBox)모델에 기인하는 것인데, 이러한 특성때문에 일반적인 클라이언

트 프로그램이 할 수 있는 기능에 비해 몇가지 제약을 갖을 수밖에 없다. 이런 제약조건이 존재한다면 애플릿 프로그램을 전자상거래 시스템에 적용하기란 불가능할 것이다. 제약조건을 풀어줌으로써 일반 응용프로그램과 동일한 효과를 얻을 수 있는 방법이 사인드 애플릿(Signed Applet)이다. 사인드 애플릿은 개발자의 비밀키로 프로그램에 서명을 하는 방법이다. 이렇게 서명을 함으로써 사용자는 개발자의 서명을 믿고 자신의 로컬머신에 자유로이 접근을 할 수 있도록 애플릿 프로그램에 권한을 부여하는 것이다.

개발자가 자신이 개발한 애플릿에 서명을 하기 위해서는 공인인증기관으로부터 개발자용 인증서를 발급받아야 한다. 그렇지 않으면 사용자는 개발자를 믿지 못할 것이며, 따라서 자신의 로컬 머신을 접근할 수 있는 권한을 부여하지도 않을 것이기 때문이다.

애플릿의 서명은 브라우저마다 그 형태가 다른데, 서명툴이 브라우저를 개발한 회사마다 각각 다르게 제공되고 있기 때문이다. 대표적인 서명툴로는 넷스케이프(Netscape)사의Signtool, 마이크로소프트(Microsoft)사의SDK for Java, 선(SUN Microsystems)사의 javakey/jarsigner등이 있다.

(2) 자바 암호모듈

자바에 암호모듈을 구성하기 위한 표준이 JCE (Java Cryptography Extension)이다[7]. 이러한 표준 표맷에 맞추어 개발된 제품이 인터넷 상에 많이 존재한다. 자바 암호라이브러리는 상용과 공개용 두가지로 나누어 볼 수 있다.

- 상용
  - JCE : 선 (SUN Microsystems) 사
  - J/CRYPTO : 빌트모아 (Biltmore) 사
  - CEAL 98 : 장미디어
- 공개용
  - Cryptix : Sysmetic사
  - IAIK-JCE : 오스트리아 Graz대학

예를 든 패키지들은 SUN사에서 지정한 JCE스팩을 따른다. 그러나 SUN사에서 개발한 JCE는 미국과 캐나다 이외의 국가에는 반출이 금지되고 있다. 따라서 공개용으로 제공하고 있는 Cryptix나 IAIK-JCE를 이용할 수 있다. 본 논문에서는 오스트리아 Graz대학에서 제공하는 IAIK-JCE를 사용하여 암호통신을 구현하였다. IAIK-JCE는 어플리케이션과 애플릿 프로그램에 모두 이용할 수 있는 암호라이브러리이다. IAIK-JCE에서 제공해 주는 함수를 구현시 모두 사용하는 것이 아니기 때문에 필요한 몇몇 함수만을 모아 몇 개의 모듈로 재구성하였다. IAIK-JCE에서 제공하는 함수자체를 변경하지 않고, 사용하지 않는 함수를 제거하고 필요한 함수들만을 사용함으로써 브라우저에서 다운로드할 때 시간을 줄일 수 있게 했다. 구현을 위해 사용된 알고리즘은 다음과 같다.

- 관용 암호 알고리즘 : 128비트 키를 사용하는 CBC 모드의 DES
- 공개키 알고리즘 : 1,024비트의 키를 사용하는 RSA
- 해쉬 알고리즘 : 160비트를 생성하는 SHA-1

5. 결론 및 향후 연구방향

인터넷의 급속한 확산과 정보 기술 발전은 일상생활과 비즈니스 관행을 근본적으로 변화시키고 있으며, 인터넷을 통한 다양한 비즈니스를 창출하고 있다. 그러나 보안상 매우 취약한 것으로 알려져 있는 인터넷 상에서 사업이나 개인의 사생활과 관련된 민감한 정보에 대한 보안 대책이 미흡한 것이 사실이다. 이는 단순한 정보 누출이 아닌 범죄로까지 이어질 수 있는 매우 심각한 문제이다.

본 논문에서는 인터넷에서 안전한 전자 경매 서비스를 제공하는 시스템을 설계 및 구현함으로써 실세계에서 행해지고 있는 경매 과정을 재현하며 비용감소와 안정성에 대한 새로운 방안을 모색하였다. 본 시스템은 Java로 구현되어 있기 때문에 사용자가 별도로 설치해야 하는 프로그램이 없고 암호모듈 역시 Java Applet용이므로 별도로 설치할 필요가 없다. 이는 사용자가 프로그램 업그레이드에 대해 신경을 쓸 부분이 없다는 것을 의미하므로, 서버에서 제공하는 프로그램을 믿고 사용하면 된다. 모든 프로그램은 서버측의 개발자가 개발하고 곧바로 이용이 가능하기 때문에 사용자는 최신 버전의 암호화 모듈과 경매 시스템을 이용할 수가 있다.

또한, 본 시스템은 사용자의 디렉토리에 공개키, 암호화된 비밀키, 서버의 공개키와 사용자의 ID를 모두 관리하고 있으므로, 이를 간단히 복사만 함으로써 이동성을 실현할 수 있기 때문에, 인터넷에 접속할 수 있는 곳이면 어디서든지 경매에 참여를 할 수 있다. 이때, Passphrase를 알지 못하면 서명을 위한 비밀키를 복호화할 수 없으므로 사용자의 비밀키에 대한 기

밀성이 보장된다. 현재 이 시스템은 인증서 발급과 지불 부분이 제외되어 있는데, 향후 두 부분이 개발된다면 보다 완벽한 경매시스템이 될 것으로 본다.

현재 경매는 일반인들에게는 익숙하지 않은 분야로 경매장소와 시간적 제약 때문에 많은 참여를 유도하지 못하고 있다. 하지만, 본 시스템은 인터넷상에서 쉽게 참여할 수 있으므로 많은 참여를 유도하여 경매를 보다 활성화 할 수 있는 가능성을 제공했다고 할 수 있다.

참 고 문 헌

[1] 실리콘밸리 뉴스, http://www.svnews.com.

[2] Bruce Schneier, "Applied Cryptography Second Edition," John Wiley & Sons Inc, 1996.

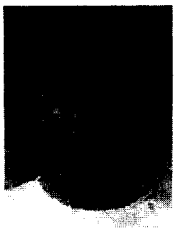
[3] William Stallings, "Network and Internetwork Security," Prentice Hall International Edition, 1995.

[4] Gary Cornell & Cay S. Horstmann., "core JAVA," Sunsoft Press, 1998.

[5] IAIK-JCE, http://jcewww.iaik.tu-graz.ac.at/.

[6] Scott Oaks, "Java Security," O'Reilly & Associates Inc, 1998.

[7] JCE, http://java.sun.com/security.



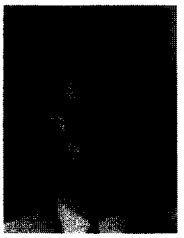
윤 두 식

e-mail : dsyoon@jiran.com

1998년 충남대학교 컴퓨터과학과 (학사)

1998년~현재 충남대학교 컴퓨터과학과 석사과정

관심분야 : 전자상거래, 네트워크 보안



박 현 동

e-mail : hdpark@esperosun.cnu.ac.kr

1995년 충남대학교 전산학과 졸업

1997년 충남대학교 대학원 컴퓨터과학과 (이학 석사)

1997년~현재 충남대학교 대학원 컴퓨터과학과 박사과정

관심분야 : 지불시스템, 전자상거래

이 종 후

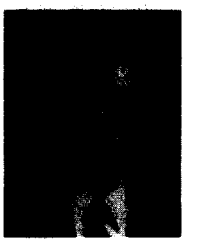
e-mail : jjongfu@ezisec.com

1997년 충남대학교 컴퓨터과학과 (학사)

1999년 충남대학교 대학원 컴퓨터과학과 (이학 석사)

1999년~현재 충남대학교 대학원 컴퓨터과학과 박사과정

관심분야 : 컴퓨터 및 통신보안체제, 전자상거래



이 만 호

e-mail : mhlee@cs.cnu.ac.kr

1975년 서울대학교 공과대학 응용수학과 (공학사)

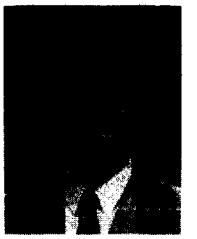
1977년 한국과학기술원 전산학과 (이학석사)

1991년 Indiana University, Dept. of Computer Science (PhD)

1977년~1980년 국방과학연구소, 연구원

1980년~현재 충남대학교, 컴퓨터과학과 교수, 교육대학원 컴퓨터과학교육전공 주임교수

관심분야 : Parallel Compiler, Parallel Processing, Programming Languages, Information Retrieval, Digital Library, Natural Language Processing



류 재 철

email : jcryou@esperosun.cnu.ac.kr

1985년 한양대학교 산업공학과 졸업

1988년 Iowa State University (전산학 석사)

1990년 Northwestern University (전산학 박사)

1991년~현재 충남대학교 컴퓨터과학과 부교수

관심분야 : 컴퓨터 및 통신보안체제, 전자상거래