Java를 이용한 전자 경매 시스템 설계

윤두식, 이종후, 이만호, 류재철
충남대학교 컴퓨터과학과

Design of Electronic Auction System with Java

Doo-shik Yoon, Jong-hu Lee, Mann-ho Lee, Jae-cheol Ryou
Dept. Of Computer Science Chungnam National Univ.

요 약

인터넷의 급속한 성장과 함께 전자상거래에 대한 연구 및 개발이 활발하게 진행되고 있다. 본 논문에서는 전자상거래의 응용 분야의 하나인 전자 경매 시스템을 인터넷 환경에 가장 적합한 언어인 Java와 Java 암호화 모듈을 이용하여 설계하였다.

1. 서론

이제 인터넷은 현대를 살아가는 우리들에게는 없어서는 안될 중요한 통신 수단이다. 초기의 인터넷은 정보의 빠른 교환 및 공유에 초점이 맞추어졌으나, 지금에 와서는 인터넷을 여러 분야에서 상업적 수단으로 이용하려는 시도를 하고 있다. 이러한 시도 중 가장 눈에 띄는 것이 바로 전자상거래(Electronic Commerce)이다. 그러나 인터넷을 상업적인 수단으로 이용하는데 있어서 인터넷에 대한 보안 문제가 가장 큰 걸림돌로 지적이 되고 있으며, 이 문제가 완전하게 해결이 되지 않는 한 전자상거래의 성공은 결코 이루어 질 수 없다. 하지만 인터넷 보안 문제의 해결을 위한 많은 연구가 활발하게 진행중이며, 빠른 발전을 거듭하고 있어 전자상거래는 더욱 활성화 될 것으로 기대된다.

전자상거래의 한 분야가 전자 경매이다. 경매는 물품을 제공하는 측과 이 물품을 구입하려는 측으로 나뉘는데, 물품을 구입하려는 측에서 서로 더 높은 경매가를 제시하여 가장 높은 경매가를 제시한 사람이 물품을 획득하는 방법이다. 그러나 실세계의 경매는 직접 경매 장소에 가야하는 불편함과 공간의 제약성, 시간의 제약성이 따른다. 지구촌 저편에서 일어나고 있는 경매에는 자신이 참가할 수 없기 때문에, 정말로 필요로 하는 물품을 구입할 수 없을 뿐 아니라, 그러한 경매가 있는지 조차 알지 못하는 경우가 있다. 이러한 문제를 해결할 수 있는 것이 바로 인터넷을 이용한 전자 경매이다.

2. 기존 시스템

전자 경매 시스템은 현재에도 국내외에 몇 군데 존재하고 있다. 국내의 경우 인터넷 경매(http://www.auction.co.kr), 국외의 경우 Electronic Auction (http://www.auction.net) 등이 대표적인 전자 경매를 실시하고 있는 사이트이다. 그러나, 이러한 경매 사이트들은 경매기간이 너무 길거나 (1주일~2주일), 실시간 경매를 한다하더라도, 인터넷 보안 기술이 전무하거나 매우 미약하여, 경매를 하는 동안 경매에 관련된 각종 정보가 유출/변조될 수 있는 가능성이 매우 크다. 또한 일반적으로 브라우져에서 보안 기술을 이용하는 방법 중 대표적인 것이 plug-in인데, 이 방법의 가장 큰 단점은 각 암호화 통신을 이용하여 물품을 판매하려는 사이트가 여러 군데 존재한다면 사용자는 각각의 사이트에서 제공하는 plug-in을 모두 설치해야 한다는 것이다. 따라서 본 논문에서는 plug-in을 사용하지

않고, 사용자는 단순히 브라우저만을 가지고 충분히 안전한 암호화 통신을 할 수 있도록 Java를 이용하는 방법을 제시한다. Java를 이용한다면 일반 사용자는 별도의 Plug-in이나 암호화 모듈이 필요하지 않고, 단지 서버에서 제공하는 Java applet을 자동으로 사용하게 되므로, 별도의 프로그램(Plug-in)에 대한 사전 지식이 없어도 되고, 서로 다른 암호화 방식을 사용하는 사이트를 전혀 부담없이 사용할 수 있다는 장점이 있다.

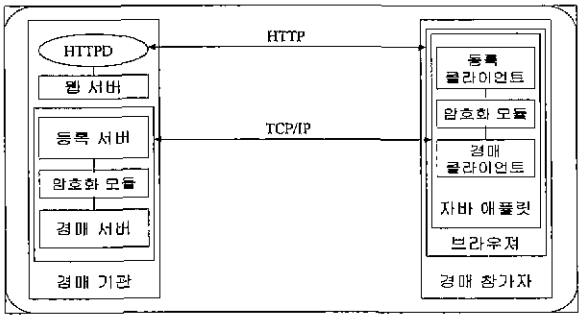
Java용 암호화 모듈은 여러 가지가 있는데, 대표적으로 Sun사의 JCE (Java Cryptography Extension)과 Systemics사의 Cryptix가 있다. 이 모듈을 JDK에 import 해서 사용함으로써 안전한 암호화 통신을 제공한다.

3. 전자 경매 시스템

본 장에서는 자바를 이용한 안전한 경매 프로토콜을 제시한다. 서버와 클라이언트 모두 사전에 상대방의 공개키를 자신의 시스템에 저장하고 있는 것으로 가정하고 구성된 것이다.

3.1. 시스템 구성

본 시스템의 전체 구성은 <그림 1> 과 같다.



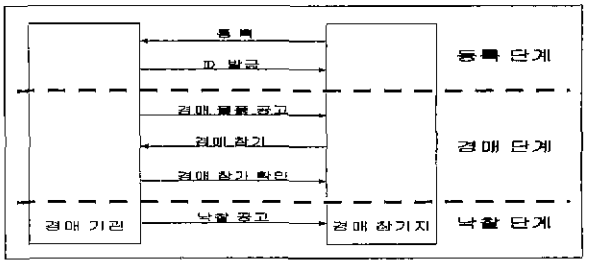
<그림 1> 시스템 구성

본 시스템에서 각 구성요소는 다음과 같은 역할을 한다.

1) 웹 서버 (Web Server)
   → 경매 물품을 공고한다.
2) 등록 서버 (Registration Server)
   → 등록을 희망하는 자들로부터 등록 접수를 받는다.
   → 등록 희망자들의 정보를 데이터베이스에 유지하고 관리한다.
   → 등록 희망자에게 유일한 ID를 발급한다.
3) 경매 서버 (Auction Server)
   → 기 등록자들로부터 경매 참가 신청을 접수한다.
   → 경매 참가자 데이터베이스를 유지하고 관리한다.
   → 참가자들이 제출한 경매가를 이용해서 낙찰자를 결정한다.
4) 등록 클라이언트 (Registration Client)
   → 등록 신청서의 데이터를 암호화하여 등록 서버에 전송한다.
   → 등록 서버가 보내온 ID를 Local machine에 저장한다.
5) 경매 클라이언트 (Auction Client)
   → 경매 참가자로부터 경매 서버로 전송하는 데이터를 암호화한다.
   → 현재 제시되고 있는 모든 경매 상황을 경매 참가자에게 알려준다.

3.2. 경매 프로토콜

본 시스템은 <그림 2>와 같이 크게 등록 , 경매 참가, 낙찰자 선정/공고 단계로 이루어진다.



<그림 2> 경매 프로토콜

3.2.1. 등록 단계

1) 등록 : 경매에 참가를 희망하는 자가 경매에 이를 위해 미리 서버에 등록하는 단계이다. 경매 참가자는 Applet의 form에 자신의 인적사항을 입력한 후 인증서(공개키)와 같이 참가자가 생성한 관용키로 암호화한 후 제출한다. 참가자의 관용키는 서버의 공개키를 이용하여 암호화하여 같이 보낸다. 내용은 다음과 같다.

$$E_{KS참가자}[\text{인적사항} \| \text{인증서}] \| E_{KU서버}[KS참가자] \quad 1)$$

2) ID 발급 : 경매 기관은 등록을 요청한 경매 참가자의 자격을 심사한 후, 경매 참가자에게 유일한 ID를 부여한다. 이때 ID는 서버의 전자 서명을 붙여 전달한다. 내용은 다음과 같다.

---

1) E_X : X로 암호화
KS참가자 : 참가자의 관용키, KU서버 : 서버의 공개키

$E_{KS서버}[ID \| E_{KR서버}[H(ID)]] \| E_{KU참가자}[KS서버]$ 2)

3.2.2. 경매 단계

1) 경매 물품 공고 : 서버는 경매 물품을 공고하고, 경매 시작 시간을 공고한다. 참가자는 경매 시작 시간 안에 경매 서버에 접속해야 한다. 이때 등록자는 자신의 ID와 전자서명을 이용해서 경매 서버에 접속할 수 있다. 이것은 비등록자들에게 경매 내용이 누출되지 않도록 하기 위함이다. 접속시 내용은 다음과 같다.

$E_{KS참가자}[ID \| E_{KR참가자}[ID]] \| E_{KU서버}[KS참가자]$

2) 경매 참가 : 경매 참가자는 applet이 제공하는 form에 의해 경매에 참가할 수 있다. 경매 참가자가 경매 내용을 서버에 전송하는 경우에는 경매 내용의 해쉬값을 구한 뒤 참가자의 서명을 붙임으로써 메시지의 무결성을 보장할 수 있고, 송신 부인 방지가 가능하다. 또한 전송되는 경매 내용은 경매 참가자가 생성한 관용키로 암호화되기 때문에, 제출한 참가자 이외에는 누구도 그 내용을 볼 수 없다. 또한, 참가자가 생성한 관용키는 서버의 공개키로 암호화되기 때문에, 안전하게 서버에게 전송된다.

$E_{KS참가자}[TimeStamp \| ID \| 경매정보 \| E_{KR참가자}[H(경매정보)]] \| E_{KU서버}[KS참가자]$

3) 경매 참가 확인 : 서버는 경매 참가자A가 제출한 경매내용을 복호화한 후 , 그 내용을 현재 경매에 참가하고 있는 모든 참가자에게 공고를 한다. 참가자는 현재 경매가를 보고 자신이 더 높은 가격에 물품을 구입하고 싶은 경우, 현재 경매가보다 더 높은 가격을 서버에 제시하면 된다. 만일 제시한 경매가가 현재 경매가보다 낮거나 같은 경우, 제시된 경매가는 받아들여지지 않고 다시 입력할 것을 요구한다. 이때 서버가 참가자A의 경매내용을 조작, 변조하는 것을 방지하기 위하여 참가자A가 보낸 경매 내용과 참가자A의 공개키를 모든 참가자에게 보낸다. 각 참가자는 경매 내용 중 참가자A의 전자서명을 참가자A의 공개키로 풀어 경매내용과 일치하는지 확인함으로써 경매내용의 조작/변조가 없음을 확인할 수 있다. 또한 보낸 모든 메시지는 서버의 log 데이터베이스에 저장/관리된다. 경매 확인 과정의 내용은 다음과 같다.

$E_{KS서버}[TimeStamp \| 경매정보 \| KU참가자A \| E_{KR참가자A}[경매정보]] \| E_{KU참가자}[KS서버]$ 3)

3.2.3. 낙찰 단계

1) 일정 시간동안 경매가가 올라가지 않으면 서버는 자동으로 낙찰자를 정하게 되며, 낙찰에 관한 정보는 최종 낙찰가와 함께 모든 참가자에게 알려지게 된다. 이 역시 최종 낙찰자로 선택된 참가자의 낙찰가와 낙찰자의 공개키를 모든 참가자에게 보냄으로써 낙찰가가 조작/변조되지 않았음을 확인시킬 수 있다.

2) 경매와 낙찰에 대한 모든 단계에서 참가자가 제시한 경매 정보는 각 확인 단계에서 참가자가 제시한 정보와 참가자의 공개키를 이용해서 확인하므로 낙찰에 대한 이의를 막을 수 있다.

4. 결 론

본 논문에서 제안한 실시간 전자 경매 시스템은 경매 물품에 대한 보다 안전하고 빠른 경매를 가능하게 한다. 기존의 plug-in을 이용하지 않고 Java를 이용함으로써 별도의 프로그램을 설치해야 하는 부담이 전혀 없이, 실시간으로 전자 경매에 참가를 할 수 있도록 한다. Java를 이용할 경우 처리속도와 applet만이 가지고 있는 보안 문제 때문에 현재는 여러 가지 단점이 지적되고 있으나, 처리속도는 실시간 처리에 중점을 두어 암호화에 사용되는 Key 길이를 줄이는 방법을 생각할 수 있고, applet이 갖는 보안 문제는 applet에 서버의 전자서명을 붙이는 방법(signed applet)을 사용하면 충분히 해결할 수 있을 것으로 본다. 본 논문에서 제시한 시스템은 전자 경매뿐 아니라 전자 입찰로도 확장하여 활용할 수 있을 것으로 본다

참고 문헌

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

[2] William Stallings, "Network and Internetwork Security", Prentice Hall International Edition

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

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

[5] http://java.sun.com/security

2) KR서버(서버의 비밀키)를 이용하여 전자서명 한다

3) KR참가자A : 경매가를 제시한 참가자A의 비밀키,
KU참가자A : 경매가를 제시한 참가자A의 공개키,
KU참가자 : 경매 참가자 개개인의 공개키,
KS서버 : 서버의 관용키