情報保護學會論文誌
第13券 第3號, 2003. 6

온라인 게임 아이템의 안전한 전자 거래 시스템

정 윤 경*, 기 준 백**, 천 정 희***

Secure Electronic Trading System for Online Game-Items

Yunkyoung Jeong*, Junbaek Ki**, Jung Hee Cheon***

요 약

본 논문에서는 현재 사이버 상에 존재하는 게임 아이템 거래 시스템과 그에 따른 문제점들을 분석하여, 온라인 게임 아이템의 안전한 거래가 가능한 전자 거래 시스템을 제안한다. 제안 시스템에서 게임 서버는 아이템 인증서를 사용자에게 발급하여, 서로 다른 온라인 게임간 아이템의 교환 및 거래를 가능하도록 한다. 또한 시스템의 문제 발생시 아이템의 복구를 가능하게 한다. 제안 시스템은 거래자들에게 신뢰할 수 있는 안전한 거래 방식을 제공하며, 거래 과정에서 어떤 오프라인 상의 작업도 필요로 하지 않는다.

ABSTRACT

In this paper, we analyze the current trading systems and suggest two secure electronic trading systems that make a fair exchange for online game items. The system is made up for the weak points in the current item trading system. In the proposed system, a game server issues a certificate for each item on the user's request. On the one hand, this certificate is used to recover the item when the system error is occured. On the other hand, the user may exchange it with another item or cyber money. The proposed system supports private and reliable trading. Further, the trading can be completed only by online processing.

Keyword : *Online game, Item, Exchanging, Electronic trading, Electronic contract*

Ⅰ. 서 론

인터넷의 보급과 컨텐츠 산업의 발전으로 온라인 게임이 급속도로 성장하게 되었고, 오락레저 분야 가운데 가장 핵심 부분으로 부상하였다. 이로 인해 온라인 게임은 21세기 엔터테인먼트 산업의 총아로 주목받게 되었다.

온라인 게임 중 하나인 RPG(Role Playing Game) 사용자들 사이에서는 게임 아이템의 교환이 급증하고 있으며, 현금을 지불하는 아이템 거래가 이루어지고 있다. 아이템 거래싸이트 중 하나인 아이템베이만 해도 지난 2001년 2월부터 중계 서비스를 시작, 지난해 500억원대 거래를 성사시키면서 총 85억원의 매출을 올렸다. 이 회사는 올들어 1일 평균 1억5000만원의 거래를 중계하고 있고, 연말까지 총 2000억원대의 거래 규모를 달성할 것으로 보고 있다[8,10,11]. 그러나 기존의 거래 시장은 여러 문제점들을 안고 있다. 첫째, 완전한 온라인 거래가 아니다. 사용자들은 안전한 아이템 교환을 위해 물리적인 장소인 거래소에 직접 방문하거나 게임방 등에서 직접 만나 아이템

* 한국정보통신대학원대학교 공학부(ykjeong@icu.ac.kr)
** 한국정보통신대학원대학교 공학부(kijun21@icu.ac.kr)
*** 서울대학교 수리과학부(jhcheon@math.snu.ac.kr)

교환을 하여야 한다. 둘째, 복제된 아이템의 거래를 방지하지 못한다[17]. 불법 복제되거나 또는 불법 취득한 아이템이 교환되었을 경우, 아이템 거래 중개 회사는 책임을 지지 않는다. 셋째, 거래 시 거래자에게 많은 절차를 요구한다. 거래 아이템을 판매 리스트에 올리고, 구매자가 생길 경우, 구매자는 판매자와 직접 연락을 취해야 하며, 물건과 현금이 오갈 때마다 아이템 중계 회사에 통보해야 한다.

우리가 제안하는 시스템에서는 이러한 문제점들을 해결한다. 이 시스템은 게임 서비스 제공 업체가 아이템 인증서(certificate)를 게임 사용자들에게 발행함으로써, 게임 사용자들에게 아이템에 대한 소유권 인정 및 아이템 판매를 정당화하였다. 사용자는 자신의 컴퓨터에 아이템을 저장하기 위해 게임 서버로부터 인증서를 발급받아 현재 발생하는 아이템 분실 등의 사고를 막을 수 있다[10,12]. 또한 거래 시에는 아이템의 복제 및 사기 사고를 막기 위해 사용할 수 있다[13].

본 논문에서 두 가지 모델을 제안한다. 첫 번째 모델에서 판·구매자들의 완전한 신뢰 속에서 판매자대신 그의 모든 역할을 수행하며 모든 것을 책임지는 마켓을 보여준다. 두 번째 모델에서의 마켓은 단지 판매 아이템의 리스트만을 제시하며, 판·구매 시 거래 당사자들 사이에 문제가 발생할 경우에만 거래 중재를 하는 형태를 띄고 있다. 이 두 모델의 모든 과정은 사이버 상에서 안전하게 이루어진다.

본 논문의 구성은 다음과 같이 이루어진다. 2장에서 현재 아이템 거래 시장에 대해 알아보고, 그에 대한 문제점을 논의한다. 3장에서는 아이템의 온라인 거래에 있어서의 요구 사항을 4장에서는 안전한 온라인 전자 거래 시스템의 두 가지 모델을 제안한다. 5장에서는 현존하는 모델과 제안된 두 모델을 비교 분석하며, 마지막으로 6장에서는 간단하게 결론을 내린다.

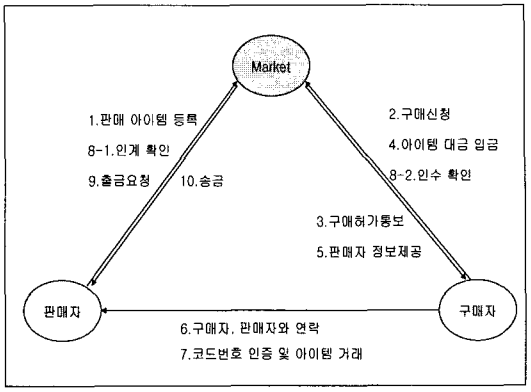
II. 현 온라인 게임 아이템 거래 시스템

현재 사이버 상에 존재하는 게임 아이템 거래 시스템을 분석하고, 그에 따른 문제점들을 파악한다.

2.1 현 시스템 분석 (예, itemXXX)

2.1.1 거래 절차

① 판매 아이템 등록 : 판매자는 판매하고자 하는 아이템의 정보를 마켓에 등록한다.



〔그림 1〕 itemXXX 거래 도표

② 구매 신청 : 구매자는 아이템 판매 리스트에서 구매하고자 하는 아이템을 마켓에 신청한다.

③ 구매 허가 통보 : 마켓은 구매자에게 아이템 구매가 허가되었음을 통보한다.

④ 아이템 대금 입금 : 구매자는 아이템의 대금을 마켓의 은행 계좌에 입금한다.

⑤ 판매자 정보 제공 : 구매자의 입금을 확인한 후 마켓은 구매자에게 판매자의 정보를 제공한다. (e-mail, 핸드폰 번호, 전화번호 등)

⑥ 구매자, 판매자와 연락 : 구매자는 마켓으로부터 제공받은 정보를 통해 판매자와 연락을 취하여 거래 방법, 시간, 장소 등을 정한다.

⑦ 코드번호 인증 및 아이템 거래 : 구매자와 판매자는 '지정점거래' 혹은 '자율거래'를 통하여 거래를 하며, 거래 시 아이템의 코드번호를 서로 확인한 후 거래를 실시한다.

⑧ 인수인계 확인 : 구매자와 판매자는 서로의 거래를 확인한 후 마켓에 아이템의 인수인계 확인 메시지를 보낸다.

⑨ 출금요청 : 아이템의 인수인계 확인 후 판매자는 마켓에 출금요청을 한다.

⑩ 입금 : 마켓은 모든 거래가 정상적으로 이루어 졌을 때, 판매자에게 아이템 판매에 대한 금액을 송금한다.

2.1.2 문제점

① 거래 당사자간 대면 거래(지정점 거래) : 대면하지 않은 상태에서의 거래는 서로 신뢰할 수 없기 때문에, 실제 거래 시에는 거래소와 같은 물리적인 장소에서 거래 당사자들이 대면한 상태에서의 거래를 권유하고 있다.

② 개인정보 유출 : 아이템 거래 시 마켓은 구매자에게 판매자의 e-mail, 핸드폰번호 등의 개인 정보를 제공한다.
③ 거래부인(자율 거래) : 구매자는 판매자로부터 아이템을 인수하고도 거래 사실을 부인할 수 있으며, 판매자는 아이템을 인계하지 않고도 허위로 아이템의 거래를 주장할 수 있다.
④ 아이템의 중복 등록 : 판매자는 동일한 아이템을 타마켓을 통해 이중으로 등록하여 마켓의 신뢰도를 실추시킬 수 있다.
⑤ 복제 아이템의 이중사용 : 아이템 거래 시 복제 아이템이 거래되고 있으나, 누구도 이를 분별할 수 있는 능력이 없다.
⑥ 아이템의 허위 등록 : 판매자는 아이템에 대한 허위 정보를 게시할 수 있다.
⑦ 구매자, 판매자와 연락 : 마켓이 거래 중개자로써의 역할을 담당함에도 불구하고, 판매자와 구매자가 직접 연락을 취하여 거래 방법, 장소와 시간 등을 정해야 한다.
⑧ 판매, 구매 지연에 따른 거래 중지 : 마켓은 아이템 인계인수 지연, 구매자의 입금 지연 등과 같은 거래 지연으로 인해 거래의 안정성을 부여하지 못하고, 판매 및 구매 지연 시에는 거래를 파기하는 상황이 발생한다.
⑨ 게임 서버 이상으로 인한 재거래 : 게임 서비스 제공 업체의 서버 이상으로 인해 거래된 아이템이 거래 이전의 상태로 되돌아갔을 때, 재 거래가 이루어져야 한다.
⑩ 과다한 거래 절차 : 거래를 위해서는 판매자와 구매자간 상호 연락 절차가 필요하며, 판매자는 아이템의 인계확인을 구매자는 아이템의 인수확인 사항을 마켓에 알려야 한다.

Ⅲ. 온라인 거래에 있어서의 요구 사항

앞장에서 제시한 현재 온라인 게임 아이템의 거래 시스템에 대한 문제점을 토대로 온라인 게임 아이템의 안전한 전자 거래를 위한 요구 사항을 제안한다.

3.1 일반 요구 사항

① 온라인 거래 : 아이템의 판·구매 시, 모든 거래가 온라인 상에서 이루어져야한다.
② 게임 서버 로드의 최소화 : 게임 서버는 게임 운용, 관리 외의 다른 업무를 수행하지 않는다.
③ 마켓의 로드를 최소화 : 마켓은 고객들과의 거래를 최소화하여 마켓의 로드를 최소화한다.
④ 비동시성 보장 : 네트웍 또는 PC 등의 오류로 인해 거래가 중지된다 할지라도, 거래가 유지·지속되어야 한다.
⑤ 판매 리스트에 대한 신뢰 : 마켓에 리스트 되어진 아이템은 유일한 것이며, 이를 모두가 신뢰할 수 있어야 한다.

3.2 보안 요구 사항

① 아이템 복제 및 이중 사용 방지 : 아이템의 복제 및 이중 사용이 불가능해야 한다.
② 거래 부인 방지 : 아이템을 주고 돈을 못 받거나, 돈을 주고 아이템을 받지 못하는 판·구매자의 거래 사실 부인 및 허위 아이템 거래 주장이 발생하지 않도록 한다. 즉, 거래는 안전하고 공정해야만 한다.
③ 아이템의 무결성 보장 : 아이템의 내용에 변질이 있어서는 안 된다.
④ 양도 가능 : 서버에 접속 없이 사용자들 간에 지속적인 아이템의 양도가 가능해야 한다.
⑤ 프라이버시 보장 : 마켓은 고객의 개인 정보, 거래 내역 등의 정보가 유출되지 않도록 보장해 줘야 한다.

Ⅳ. 온라인 게임 아이템의 안전한 전자거래시스템

모델을 제안하기 앞서 전자거래시스템을 위해 필요한 몇 가지 가정을 한 후, 온라인 게임 아이템의 안전한 전자거래시스템의 두 가지 모델을 제안한다.

4.1 가정

⊙ 온라인 게임 아이템은 PC 게임의 RPG[1]게임 아이템에 한정한다.
⊙ 게임 서비스 업체는 아이템에 대한 인증서를 발

1) Role playing, 즉 역할 놀이이다. 보통 전사, 마법사, 성직자, 도둑 등의 역할을 만들어서 자기의 역할에 맞는 일을 수행한다. 역할이 정해지면, 그 역할에 따라서 주어진 일을 수행해 나간다. 디아블로와 리니지 등의 게임이 이에 속한다.

행한다.

⊙ 대금 결제는 '사이버 머니[2](cyber money)'를 통해서만 이루어진다.

첫째, 이 시스템을 통하여 거래 가능한 아이템은 PC게임의 RPG 아이템에 한정한다. 현재 PC, PDA, 핸드폰 등을 통해 언제 어디서든, 단순한 보드 게임에서 복잡한 RPG까지 다양한 온라인 게임을 즐길 수 있다. 이 시스템에서 거래 가능한 아이템은 RPG에서 사용되는 칼과 방패 같은 아이템의 거래만을 가정한다. 시스템의 거래 변경을 통해서 보드 게임에서 사용되어지는 사이버 머니 또는 적립된 포인트의 교환 및 거래에서 사용되어질 수 있다.

둘째, 게임 서비스 업체는 아이템에 대한 인증서를 발행한다. 인증서의 발행은 이 시스템에서 가장 중요한 부분이다. 게임 아이템에 대한 인증서를 발행함으로써 개인에게 게임 아이템의 소유권[3]을 인정하며, 서버의 오류로 인한 아이템 분실 시, 소유 아이템에 대한 복구를 가능하게 한다. 또한 이러한 아이템 인증서의 발행으로 아이템을 물건처럼 매매 가능하게 하고, 게임 서버에 직접 연결할 필요 없이 게임 아이템의 거래가 가능하다.

셋째, 대금 결제는 '사이버 머니'를 통해서만 가능하다. 현실적으로 사이버 머니는 마켓에서 발행, 관리하며 인증서와 비슷하게 온라인으로 관리한다. 여기서 사용되는 사이버 머니는 양도가능하며, 이중사용이 불가한 것으로 가정되어지며, 완전한 전자 화폐가 개발되어진다면 이것으로 사이버 머니를 대체할 수 있다[1,5,7]. 현재 시스템에서는 아이템 거래 시에 신용카드 결제, 현금 결제 등이 이루어지고 있으나, 이러한 현금 결제는 많은 사회 문제를 일으키고 있다[9,14,15,16]. 이번 시스템에서는 '사이버 머니'를 통한 거래만을 가정한다. 이는 문제를 기술적인 측면으로 단순화 시켜 정보보호 기술에 초점을 맞출 수 있도록 하기 위함이다.

우리의 거래 시스템은 위 세 가지 가정 하에 설계되었으며, 위의 가정 사항은 온라인 게임의 발전과 온라인 게임 아이템 거래에 대한 사회 인식의 변화, 게임 기술의 발전, 기업의 정책 등에 따라 달라질 수 있다.

4.2 모델 1 (증권 거래 모델)

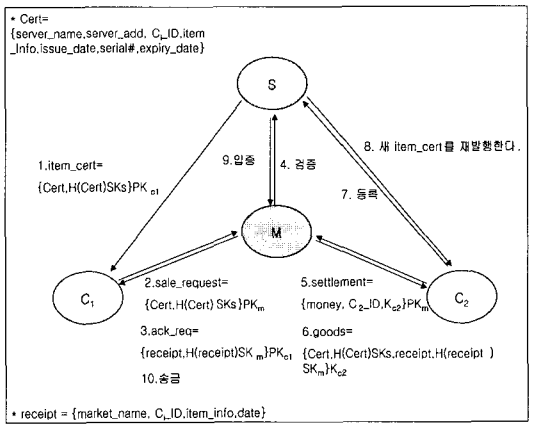
모델 1은 판매자가 마켓을 전적으로 신뢰하는 모델로써, 마켓이 판매자를 대신해 판매에 관한 모든 업무를 대리 수행한다. 이는 증권 회사를 응용한 모델이라 할 수 있겠다.

4.2.1 Parameter

⊙ S : 게임 서비스 제공 업체
⊙ M : 신뢰하는 마켓
⊙ C_1 : 마켓의 정회원, 판매자
⊙ C_2 : 마켓의 정회원 또는 비회원, 구매자
⊙ H : 해쉬 함수
⊙ SK_a, PK_a : a의 개인키, 공개키
⊙ K_a : a의 세션키
⊙ 인증서 : {server_name, server_add, C_a_ID, item_info, issue_date, serial#, Expiry_date}
⊙ 영수증 : {Market_name, C_a_ID, item_info, date}

4.2.2 거래 절차

S는 C_1에게 아이템 인증서를 발급한다. 인증서는 해쉬 함수를 사용하여 서버의 개인키로 서명하여 인증서에 대한 변형을 불가능하게 한다. 또한, 인증서에 C_1_ID를 포함시킴으로써 인증서 복제에 따른 이중사용을 방지한다. 만일 다른 게이머가 아이템 인증서를 불법 취득하거나 복제할지라도, 그의 ID와 인증서 필드에 내재된 ID와 다르기 때문에 사용할 수



〔그림 2〕 온라인 게임 아이템 거래 모델 1

2) 전자상거래 및 콘텐츠 제공업체들이 자사 회원에게 마일리지 형태로 제공하는 가상화폐

3) 이 소유권은 점포의 권리금과 같은 성격을 갖는다. 즉, 게임 서비스가 이루어지는 동안만 유효하며, 게임 서비스 중단 시 아이템에 관한 소유권은 사라지는 것으로 가정한다.

없게 된다.

item_cert = {Cert, H(Cert)SKs}PKc1
Cert = {server_name, server_add, C1_ID, item_info, issue_date, serial#, expiry_date}[4]

아이템 판매를 원하는 C_1은 거래하고자 하는 인증서를 M의 공개키로 암호화하여 마켓에 보낸다. C_1은 전적으로 신뢰하는 M에게 인증서를 보냄으로써 거래에 관한 모든 업무를 마켓에 전가시킨다.

sale_request = {Cert, H(Cert)SKs}PKm

C_1의 판매 요청을 받은 M은 C_1에게 C_1의 공개키로 암호화한 영수증(receipt)을 발송한다. 영수증은 M의 개인키로 서명되어 있으므로, M은 C_1에게 인증서를 받은 사실을 부인할 수 없다. 또한, 영수증의 변조를 방지하기 위해 거래자의 ID를 영수증에 명시하고, 해쉬 함수를 이용하여 영수증의 무결성을 보장한다.

ack_req = {receipt, H(receipt)SKm}PKc1

C_2가 구매를 요청할 경우, M은 S에 item_cert 검증을 요청한다. 이때, S는 검증에 따르는 로드를 줄이기 위해 revocation list를 사용한다. 구매 요청이 들어오면, 현 거래 이전에 이미 다른 마켓을 통하여 아이템 거래가 이루어졌을 수 있으므로, 거래 직전에 S에 연결하여 검증 절차를 밟는다[5]. 검증이 끝난 후 C_2는 자신의 정보, 세션키 그리고 '사이버 머니'를 M의 공개키로 암호화하여 M에게 보낸다.

settlement = {money, C2_ID, Kc2}PKm

M은 item_cert와 결제에 따른 인증서와 영수증을 C_2의 세션 키로 암호화하여 보낸다. M과 S의 서명으로써 인증서에 대한 확인과 부인 방지를 보장한다.

goods = {Cert, H(Cert)SKs, receipt, H(receipt)SKm}Kc2

C_2는 M으로부터 받은 인증서와 영수증을 S에 보냄으로써, C_2 자신의 아이템으로 등록하고, 새로운 item_cert를 발급받는다.

{Cert, H(Cert)SKs, receipt, H(receipt)SKm}PKs
Cert' = {server_name, server_add, C2_ID, item_info, issue_date', serial#', expiry_date'}

S는 아이템 소유가 이전되었음을 M에게 통보하며, M은 C_1에게 판매 대금을 송금한다.

이 모델은 마켓 M을 전적으로 신뢰하는 모델이다. 마켓은 판매자 C_1의 판매에 대한 모든 업무를 대리 수행하므로 판매자는 항상 마켓에 연결되어 있을 필요가 없다. 모든 거래를 마켓이 하며, 판매자는 최종적으로 거래에 따른 판매 대금만을 송금 받는다. 따라서, 이 모델은 고객들에게 가장 이상적인 모델이다. 그러나 모델 1은 마켓에 과다한 로드를 부여하고, 마켓을 전적으로 신뢰해야만 하는 단점을 가지고 있다.

4.3 모델 2 (부동산 거래 모델)

모델 2에서의 마켓은 거래 대금의 처리를 담당하며, 판매자와 구매자 사이에 문제가 발생하는 경우 중재하는 역할도 수행한다. 여기서는 판매자가 마켓을 완전히 신뢰하지 않는다는 가정에서 이뤄진다. 판매자는 단지 마켓에게 자신이 소유하고 있는 아이템에 대한 정보만을 제공하며, 그 외의 거래에 관한 모든 과정은 판매자와 구매자 사이에서만 이루어진다. 이는 부동산 중개 회사를 응용한 모델이라 할 수 있겠다.

4.3.1 Parameter

모델 2에서 사용되어지는 파라미터들은 2.1과 동일하다.

4.3.2 거래 절차

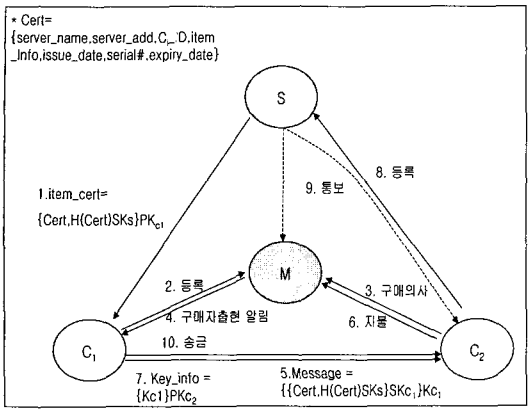
S는 C_1의 요청에 따른 아이템 인증서를 발급한다.

item_cert = {Cert, H(Cert)SKs}PKc1

M이 C_1이 판매하고자 하는 아이템 정보를 게시한

4) 여기서 *H(Cert)SKs*는 *H(Cert)*를 *s*의 비밀키 *SKs*로 서명한 값을 의미하며, *{XXX}PKc1*은 *C1*의 공개키로 암호화한 값이다. 앞으로 나오는 기호들도 이와 같다.

5) 검증 과정을 통하여 이미 거래된 아이템인지 확인하며, 이를 통하여 이중사용 및 인증서 불법 복제 거래를 막는다.



〔그림 3〕 온라인 게임 아이템 거래 모델 2

다. 이때, M은 C_1이 아이템에 대한 정보를 제공할 때, ZKIP(Zero Knowledge Interactive Proof)을 사용하여 실제 C_1이 아이템을 소유하고 있음을 확인한다. C_2는 M의 판매 리스트에서 구매하고자 하는 아이템에 대해 M에게 아이템 구매 신청을 한다. M은 C_1에게 구매자가 나타났음을 알리고, C_1은 인증서에 자신의 개인키로 서명하고, 자신이 생성한 세션 키로 암호화하여 C_2에게 보낸다.

$$Message = \{\{Cert,H(Cert)SKs\}SKc_1\}Kc_1$$

C_2는 M에 대금을 지불하고, M은 C_1에게 대금 지불 사실을 통보한다. 통보를 받은 C_1은 C_2에게 세션 키를 C_2의 공개키로 암호화하여 보낸다.

$$Key\_info = \{Kc_1\}PKc_2$$

C_2는 C_1으로부터 받은 세션 키로 인증서를 복호화한 후, 사실 여부를 확인하고 S에 등록한다. S는 C_2가 의뢰한 아이템에 대해서 등록 여부를 확인한 후, 이를 M과 C_2에게 통보한다. M이 S로부터 확인된 사실을 통보 받으면, C_2로부터 입금된 돈을 C_1에게 송금한다.

이 모델은 마켓 M이 판매 아이템 리스트 제공과 대금 지불 등의 일만을 수행하고, 실제적인 거래는 거래자들이 직접 수행한다. 이 모델은 모델 1에 비해 마켓의 로드를 현저히 줄일 수 있다는 장점이 있으나, ZKIP의 사용으로 인해 거래 시간의 지연이 일어나는 단점이 있다.

V. 모델의 비교 및 분석

지금까지 우리는 현존하는 온라인 아이템 거래 시스템에 대해 알아보았고, 두 개의 새로운 안전한 거래 시스템을 제안하였다. 이 장에서 현 시스템과 새로운 두 개의 시스템들이 3장에서 언급한 요구 사항들에 얼마나 만족하는 지를 비교 분석한다.

시스템의 비교, 분석 결과를 [표 1]에 정리해 보았다.

〔표 1〕 시스템의 비교 및 분석

(○:만족, △:중간, ×:불만족)

		현재 시스템	모델 1	모델 2
일반 요구 사항	1.온라인 거래	△	○	○
	2.게임서버 로드의 최소화	○	△	△
	3.마켓 로드의 최소화	○	×	○
	4.비동시성 보장	△	○	○
	5.판매 리스트의 신뢰도	△	△	△
보안 요구 사항	6.아이템(인증서) 복제 및 이중 사용 방지	×	○	○
	7.거래 부인방지	×	○	○
	8.아이템(인증서)의 무결성 보장	×	○	○
	9.양도성	×	×	×
	10.프라이버시 보장	×	○	△

① 온라인 거래 : 현재 시스템인 지정점 거래의 경우, 거래자들이 직접 만나 교환해야하므로 완전한 온라인 거래를 제공하지 못한다. 제안된 모델에서는 게임 아이템 인증서를 발급 받게 되므로 완전한 온라인 거래가 가능하다.

② 게임 서버 로드 최소화 : 현 모델의 게임 서버는 단지 게임만을 위한 서버가 운용되지만, 제안된 모델에서는 인증서 발행 및 검증 등의 업무 추가가 불가피 하다. 따라서 게임서버의 로드가 현재보다 증가한다.

③ 마켓 로드 최소화 : 현재 모델과 모델 2에서는 아이템 거래를 위한 아이템 구매 리스트 제공과 물품 대금 송금 이외에는 마켓이 하는 일이 거의 없으나, 모델 1에서는 마켓이 판매자 대신 모든 거래를 하게 되므로 마켓의 로드가 증가한다.

④ 비동시성 보장 : 어느 한쪽의 시스템 결함으로 인하여 거래가 중지되었을 경우, 현 모델에서는 더 이상 거래가 불가능 하나, 제안된 모델에서는 마

켓에서의 중재로 거래가 지속적으로 이루어 질 수 있다. 모델 2에서도 판매자와 구매자 사이의 거래 중 문제 발생 시 마켓의 중재로 거래를 완만히 성사시킬 수 있다.

⑤ 판매 리스트의 신뢰도 : 현 모델에서 판매자는 여러 마켓에 자신의 아이템을 등록할 수 있으며, 제안된 두 모델에서도 아이템 인증서를 복사하는 등의 방법으로 여러 마켓에 등록할 수 있다. 이는 복제라는 기술을 원천 봉쇄 할 수는 없기 때문이다. 이로 인해, 마켓에서 제공하는 판매 아이템 리스트는 현 모델이나 제안된 모델에서 동일하게 완전한 신뢰를 주지 못한다. 그러므로, 각각의 마켓들은 타 마켓과의 협력을 통해 거래 된 아이템에 대한 업그레이드를 함으로써 마켓 자신의 신뢰도를 높게 유지시켜야 한다.

⑥ 아이템(인증서)의 복제 및 이중 사용 방지 : 위에서 언급했듯이, 현 모델과 제안된 모델 모두 복제 아이템의 거래를 방지할 수 없다. 그러나 제안된 모델에서는 마켓이나 구매자가 인증서를 통해, 아이템 검증 및 등록여부를 서버에 확인하므로 복제된 인증서의 사용이 불가능하다. 만일 게이머가 다른 게이머의 아이템 인증서를 불법 취득하여 거래하고자 하여도, 마켓이 게임 서버에 검증 절차를 거치는 과정으로 인해 거래가 중단된다. 두 모델에 대한 자세한 설명은 다음과 같다.

-모델 1 : 판매자가 아이템 인증서를 복사하여 여러 마켓에 팔거나 또는 이미 팔아버린 인증서를 복사해서 이중 판매를 한다 할지라도, 구매자의 구매 요청 시 마켓은 서버에 연결하여 인증서에 대한 검증을 하게 되므로, 복사 및 이중 판매 방지가 가능하다.

-모델 2 : 판매자가 아이템 인증서를 이중 사용할 경우, 구매자가 마지막 등록 절차를 거치며 서버에 확인하는 과정에서 인증서에 대한 검증을 하게되어 이중 사용을 막는다. 만일 아이템 인증서가 복사본이거나 이중 사용된 것으로 서버에서 확인한다면, 이는 마켓과 구매자에게 통보되어지므로 마켓은 판매자에게 돈을 지불 하지 않고, 이 거래는 취소된다.

⑦ 거래 부인 방지 : 현 모델은 마켓이 중간에서 증인을 두어 거래 부인방지를 할 수 있으나, 제안된 모델에서는 영수증이나 세션키 등을 이용하여 판매자와 구매자의 거래 부인방지를 가능하게 한다. 만일 누구든 거래에 대한 거짓을 나타낼 경우, 세션키 등을 통해 마켓은 문제를 쉽게 해결할 수 있는 능력을 지니게 된다. 두 모델에 대한 자세한 설명은 다음과 같다.

- 모델 1 : 구매자가 마켓으로부터 아이템 인증서를 받고난 후 받지 않았다고 부인할 경우, 마켓은 구매자에게 구매자의 공개키로 암호화한 인증서와 영수증을 얼마든지 다시 주어 거래 부인을 방지한다. 또한 판매자가 돈을 받지 못했다고 부인을 할 경우에는 기존의 전자화폐 추적과 동일한 방법을 통하여 거짓을 밝혀낸다.
- 모델 2 : 문제가 발생할 경우, 모든 문제를 마켓이 중간에서 해결한다. 판매자로부터 암호화된 아이템 인증서를 건네받은 구매자가 이를 부인할 경우, 판매자는 인증서를 다시 보내거나 인증서를 복호화할 세션키를 보내지 않는다. 판매자가 인증서를 보낸 후에, 세션키를 보내지 않고서 보냈다고 거짓을 고할 경우, 마켓의 중재로 판매자에게 보냈다고 주장하는 세션키를 다시 보내도록 한다. 구매자가 세션키를 받았음에도 이를 부인할 경우, 판매자는 키를 얼마든지 다시 보낼 수 있다. 또한 판매자가 돈을 받지 못했다고 부인을 할 경우에는 모델 1과 마찬가지로 기존의 전자화폐 추적과 동일한 방법을 통하여 거짓을 밝혀낸다.

⑧ 아이템(인증서) 무결성 보장 : 인증서를 서버로부터 발급받을 때, 인증서와 함께 일방향 함수인 해쉬 함수를 사용한 인증서를 함께 발급받는다. 판매자는 이 인증서와 해쉬된 인증서를 함께 전달하여 악의적인 누군가가 인증서를 가로채서 내용을 바꾸었을 때, 인증서가 잘못되었음을 확인할 수 있게 한다. 또한 해쉬 함수와 함께 개인키등을 이용하여 암호화하므로, 악의적인 공격자가 인증서를 바꾸고, 이것을 가지고 해쉬한 잘못된 인증서를 보낸다하더라도 공격자는 개인키를 알 수 없으므로 아이템 인증서를 변경하여 전달할 수 없게 된다. 이는 인증서뿐만 아니라, 영수증 전달에도 적용되어 무결성을 보장한다.

⑨ 양도 가능 : 현 모델에서는 게임 서버에 직접 연결 후, 구매자에게 아이템을 양도하므로, 게임 서버 접속 없이 타인에게 아이템의 양도가 불가능하다. 제안된 모델 역시 인증서를 발급하지만, 구매자의 등록과 확인하는 절차 이후에 새로운 아이템 인증서를 발급받게 되므로, 게임 서버와 연결하는 절차 없이 타인에게 아이템 인증서의 양도가 불가

능하다.

⑩ 프라이버시 보장 : 현 모델은 아이템 교환을 위해 구매자에게 판매자의 개인 정보를 제공하며, 직접 대면하여 거래하기 때문에 서로의 프라이버시가 보장되지 못한다. 제안된 모델 1에서는 거래가 마켓을 통해 이루어지므로, 마켓만이 구매자와 판매자의 정보를 보유하고 거래할 뿐, 직접적으로 그들에게 서로의 개인 정보를 유출하지 않는다. 모델 2에서는 거래 당사자들끼리 거래가 이루어지므로, e-mail 등의 서로간의 개인 정보가 유출되어지나, 오프라인 상에서의 실제 상대가 누구인지는 알 수 없다.

위의 [표 1]의 비교·분석을 통해 알 수 있듯이 현 시스템은 게임 서버와 마켓의 로드를 최소화하는 것 외에는 다른 일반 요구 사항 및 보안 요구 사항을 거의 만족시키지 못한다. 이번 연구에서 제안한 두 모델은 아이템 온라인 거래에 대한 요구 사항을 대부분 만족시키고 있다. 모델 1의 경우 마켓의 업무에 대한 부하는 크나 마켓이 모든 업무를 수행함에 따라 개인 정보에 대한 유출을 막을 수 있으면, 고객들에게 최선의 서비스를 제공할 수 있다. 모델 2는 마켓의 로드를 최소화하면서 거래자들 간에 안전하고 공정한 거래를 제공한다.

Ⅵ. 결 론

현 온라인 게임 아이템의 거래에 있어 복제 아이템의 거래, 거래 부인 등의 사기 사고가 빈번하게 발생하고 있다. 그럼에도 불구하고, 아이템 거래 시장에서는 아직까지 이러한 문제들에 대한 특별한 해결안을 찾지 못하고 있다.

이번 연구에서는 이런 문제들을 해결하고자 거래 시스템에 간단한 암호기술을 적용하였다. 그 결과 온라인 게임 아이템 거래에 있어 안전하고 공정한 거래가 가능한 두 개의 모델이 착안되었고, 이 모델들을 통하여 온라인 게임 아이템의 안전한 전자 거래 시스템이 구현되었다. 그러나 아직까지 해결해야 할 몇 가지 문제들이 남아 있다.

⊙ 게임 서버와 마켓의 부담 축소 문제
⊙ 아이템에 대한 양도성 문제
⊙ 수익 모델인 마켓의 신뢰도 문제

첫 번째로 게임 아이템 인증서를 통해 거래가 이루어지므로 기존의 시스템에 비해 게임 서버와 마켓에 로드를 더하게 되었다.

두 번째는 게임 서버에 직접 연결하여 등록하는 절차 없이 아이템 인증서의 양도가 가능한 시스템을 설계해야 할 것이다.

마지막으로, 마켓의 신뢰도를 떨어뜨리지 않도록 해야 한다. 판매자가 다수의 마켓에 판매 등록을 함으로써 타 마켓의 신뢰도를 떨어트리는 행위에 대해, 현재는 판매자에게 벌점을 주는 것으로 문제를 해결하고 있으나, 앞으로는 기술적인 방법에 의한 해결 방안이 제시되어야 할 것이다.

온라인 게임이 발전함에 따라 온라인 게임 아이템의 거래 시장 또한 엄청난 규모로 성장하고 있다. 그에 따른 보안 또한 많은 연구와 기술적인 발전이 있어야 할 것이다.

참 고 문 헌

[1] Donald O'Mahony, Michael Peirce, "Hitesh Tewari, Electronic Payment System," Artech House, 1997

[2] Charles P. "Pfleeger, *Security in Computing*," pp.129~151, Prentice Hall ,1989

[3] Christian Cachin and Jan Camenisch, "Optimistic Fair Secure Computation," IBM Research, Zurich Research Laboratory

[4] Tatsuaki Okamoto, "Disposable Zero-Knowlodge Authentications and Their Applications to Untraceable Electronic Cash," NTT Communications and Information Processing Laboratories

[5] Mostafa Hashem Sherif, "Protocols for Secure Electronic Commerce," CRC Press, 2000

[6] Alfred J. Menezes, "Paul C. van Oorschot, Scott A. Vanstone," HANDBOOK of APPLIED CRYPTOGRAPHY, CRC Press, 1996

[7] N. Asokan and Victor Shoup, "Michael Waidner, Optimistic Fair Exchange of Digital Signature," IBM Research, Zurich Research Laboratory

[8] http://www.m-dream.com/gamenews_view.php?no=592

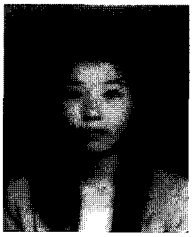
[9] http://www.sportschosun.com/news/entertainment/200208/20020814/28n19004.htm

[10] http://www.itembay.com

[11] http://www.khan.co.kr/nm/20021010/society/contents.

php3?id=3117
[12] Game조선, "게이머..우왕좌왕", 2003.01.27
[13] http://www.cyber118.or.kr/FAQ/hack1_13.html
[14] mbc뉴스, "머드 게임 아이템 사기 10대 구속", 2001.04.26
[15] mbc뉴스, "카드정보로 게임아이템 산 뒤 되팔아", 2003.01.09, http://news.imbc.com/asp/News/Society/detail.asp?News_ID=20030109015400**********
[16] mbc뉴스, "5천만원 게임아이템 사기 10대 구속", 2003.01.15, http://news.imbc.com/asp/News/Society/detail.asp?News_ID=20030115000500**********
[17] mbc뉴스, "리니지 아이템 해킹 판매 10대 구속", 2002.01.29, http://news.imbc.com/asp/News/Society/detail.asp?News_ID=20020129031500**********

〈著者紹介〉



정 윤 경 (Yunkyoung Jeong) 학생회원
1998년 3월~2002년 2월 : 전북대학교 정보통신공학과
2002년 2월~현재 : 한국정보통신대학원대학교 정보보호 트랙 석사과정
<관심분야> 정보보호, 휴먼 컴퓨팅 환경

기 준 백 (Junbaek Ki)
1992년 3월~1996년 2월 : 단국대학교 토목공학과
2001년 3월~2003년 2월 : 한국정보통신대학원대학교 전자상거래 정보보호
<관심분야> 온라인게임에서의 보안, 전자상거래 보안 기술(전자계약, 전자화폐)

천 정 희 (Jung Hee Cheon) 정회원
1997년 2월 : 한국과학기술원 수학과 박사
1997년 3월~2000년 1월 : 한국전자통신연구원 선임연구원
2000년 1월~2000년 12월 : Brown 대학 박사후 연구원
2000년 12월~2003년 2월 : 한국정보통신대학교 공학부 조교수
2003년 3월~현재 : 서울대학교 수리과학부 조교수
<관심분야> 응용정수론, 암호론, 응용암호론