2002년 한국정보처리학회 춘계학술발표논문집 제9권 제1호

MMORPG 게임에서의 스마트카드 활용 시스템 설계

권기달 김성찬 장인걸 신동규 신동일
세종대학교 컴퓨터공학과
e-mail : knight1976, kimschan, ig8961, shindk, dshin@gce.sejong.ac.kr

Design of System Using Smart-Card in MMORPG Game

Ki-dal Kwon Seong-chan Kim In-gaul Jang Dong-kyoo Shin Dong-il Shin
Dept. of Computer Engineering, Sejong University

요 약

본 논문에서는 MMORPG 게임에서 스마트카드를 이용한 시스템을 설계하였다. 스마트카드가 갖고 있는 기능적 특성들을 이용하여 MMORPG 게임에서 시스템 유해 코드 차단 및 개인 사용자의 정보 보호, 서비스 이용에 대한 과금 시스템 구축 등을 위해 기존의 서버-클라이언트 시스템상의 소프트웨어 설치를 통해 이루어졌던 사용자들이 신뢰할 수 없는 과금 체계나 보안 기능이 아닌 하드웨어적인 접근을 통하여 보안적으로 좀더 견고하고 안정적인 시스템을 구축할 수 있도록 하였다.

1. 서론

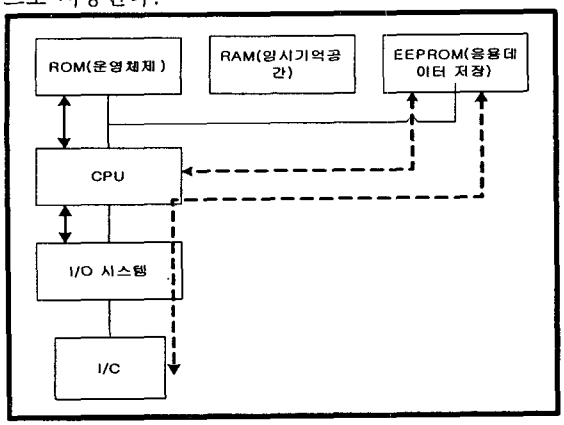
MMORPG(Massively Multi-Player Online Role-Playing Game) 게임[1] 시장은 해외에서뿐만 아니라 국내에서도 굉장히 활성화되고 있는 추세이다. 과거에 컴퓨터 네트워크가 대중적으로 보급되기 전까지는 영세적인 수준에서 벗어날 수 없었으나 ADSL, 케이블 모뎀[2]등과 같은 대중적인 컴퓨터 네트워크 사업을 주도하는 거대 ISP[2]업체들이 등장을 하였고 현재는 이러한 ISP 업체들에 의한 네트워크 보급이 활성화 됨에 따라 기존의 MMORPG 게임 개발사들은 게임 컨텐츠를 새롭게 개발하여 사용자들의 관심을 집중시켰고 이 관심을 바탕으로 MMORPG 게임은 전성기를 맞이하게 되었다. 국내에서는 NC 소프트의 리니지[3]가 그 단적인 예라고 할 수 있다. MMORPG 게임은 일반적인 패키지 게임시장에 비해 제작에 들어가는 초기비용 부담이 적을 뿐만 아니라 효율적인 사용자 관리 및 컨텐츠의 유지보수를 통해 지속적인 사용자 확보가 가능하고 이는 안정적인 수익구조 및 기반 사용자의 확보로 이어져오고 있다. 현재 이러한 게임 컨텐츠 및 서비스 중심으로 흘러가는 MMORPG 게임산업의 성장이면에는 사용자들의 정보보호에 대한 인식 부족과 미약한 서버 보안 기술 및 하위레벨 코드 취약성으로 인하여 개인 정보 도용 및 ID 해킹 사례가 빈번히 발생하고 시스템 유해코드로 인한 건전한 게임 문화의 파괴 및 컨텐츠의 존립위기를 가져왔다. 더욱이 이러한 문제점들이 사회적 문제로까지 번져가고 있다. 그리고 게임사들간의 과도한 경쟁으로 인한 과금 체계의 영세성은 지속적인 성장을 하고 있는 MMORPG 게임산업의 발전을 가로막고 있는 것이다.

이에 본 논문에서는 스마트 카드[4]를 이용하여 과금 체계, 개인정보보호 및 유해코드 차단을 위한 시스템을 설계하였다. 2 장 관련연구에서는 사용자 정보 보호 및 과금 시스템 구현을 위해 이용되는 스마트 카드에 대한 내용을 다루었으며 3 장에서는 스마트카드를 이용한 시스템 설계에 대한 내용을 언급하고 4 장에서는 결론 및 향후 전망에 대해서 논하겠다.

2. 관련연구

스마트카드는 내장된 마이크로 프로세서와 메모리를 이용하여 데이터의 저장과 처리가 가능한 플라스틱 재질의 카드를 말한다. 그리고 [그림 1]과 같이 기능성 측면에서 더 뛰어난 마이크로 프로세서 카드는

CPU, ROM, RAM, I/O 포트, 그리고 데이터의 저장을 위해 EEPROM 을 가지고 있으며 ROM 은 보통 운영체제의 저장을 위해, RAM 은 CPU 처리를 위한 임시기억공간으로, 그리고 EEPROM 은 어플리케이션의 기억 공간으로 사용된다.



[그림 1] 스마트 카드의 구조

스마트 카드의 크기는 일반 신용카드 정도이며 통합 회로 카드(ICC) 방식[5]을 이용하여 인증서와 개인키를 저장할 수 있고, 인증, 디지털 서명, 키 교환 등과 같은 공개키 암호화 작업[6]을 수행 기능을 한다. 스마트 카드의 보안 기능은 개인키나 다른 형태의 개인 ID 에 대한 변경을 허용하지 않는 스토리지(tamper-resistant storage)를 제공하고 인증, 디지털 서명 및 키 교환과 관련된 중요한 보안 계산 방식 및 그 결과를 해당 데이터가 필요하지 않은 시스템영역으로부터 분리 시키며 자격 정보 및 다른 개인적 정보를 회사의 컴퓨터에서 집이나 원격지 컴퓨터로 이동하는 것과 같은 작업 등을 할 수 있다. 또한 스마트카드의 사용목적에 따라 필요한 프로그램을 다운로드 받아 기능을 변경해서 사용할 수 있다. 따라서 다양한 목적에 따라 유연하고 유용하게 사용이 가능하다. 이러한 것들을 통하여 보안을 강화시킬 수 있으며 응용분야로는 금융, 신분확인, 그리고 접근통제 등이 있다[6].

현재 스마트카드는 그 사용 목적이 상거래상에서 이루어지는 지불행위로 쓰는 것이 개인의 신분증명 및 개인의 비밀 정보, 비밀키 등을 저장하는 용도로의 일반화가 되고 있다.

스마트 카드는 PC 와 연결하여 사용이 가능하며 현재 스마트 카드를 지원하는 운영체제로는 윈도우 2000 시스템이 있다.

윈도우 2000 시스템은 PC/SC(PersonalComputer/Smart Card)[7]를 수용하는 산업 표준형 스마트 카드를 지원하고 또한 PC/SC 작업 그룹이 개발한 사양을 준수하는 플러그 앤 플레이 스마트카드 판독기[8]를 지원한다. 윈도우 2000 서버 및 윈도우 XP 프로페셔널에서 작동이 가능하기 위해서 스마트카드는 ISO 7816-1, 7816-2 및 7816-3 표준[9]을 물리적, 전자적으로 모두 준수해야 한다.

스마트카드 판독기는 RS-232[10], PC Card 및 범용 직렬 버스(USB)와 같은 표준형 PC 주변기기 인터페이스에 부착되며 일부 RS-232 판독기는 판독기용 전원 공급을 위한 PS/2 포트를 통하여 통신하지 않는다. 판독기는 표준형 윈도우 장치로 보안 설명자(Security Descriptor) 및 플러그 앤 플레이 식별자(Plug and Play Identifier)를 갖고 있다. 스마트 카드 판독기는 표준형 윈도우 장치 드라이버에 의하여 제어되며 하드웨어 마법사를 사용하여 설치 및 제거가 가능하다.

3. MMORPG 게임에서의 스마트카드 활용 시스템 설계 및 동작 원리

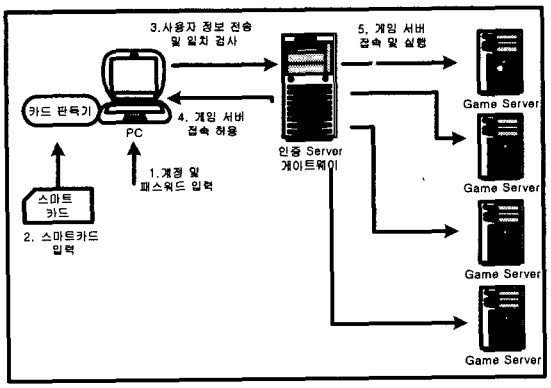
본 논문에서는 MMOPRG 게임에서 스마트 카드를 이용하여 효과적이고 안전한 과금 체계 시스템을 구축하고 유해코드 및 해킹과 같은 불법적인 행위로부터 게임 컨텐츠를 보호하며 MMORPG 게임 개인 사용자들의 정보보호를 위한 시스템을 설계하였다.

다음은 본 논문에서 설계한 시스템의 구조이다.

3.1. 사용자 인증 시스템 설계 및 동작 원리

3.1.1 사용자 인증 시스템 설계

스마트카드를 이용한 MMORPG 게임에서 사용자 인증 시스템은 사용자가 게임을 실행하기 위해 게임서버에 접속할 때 사용자 인증을 위해 사용되며
사용자에 대한 인증을 하기 위한 시스템의 구성요소는 [그림 1]에서와 같이 사용자 클라이언트에 속해 있는 스마트카드 판독 모듈과 스마트카드를 온라인 상에서 인증하기 위한 온라인 인증 서버 게이트웨이 모듈로 나눈다.



[그림 2] 사용자 인증 시스템 및 동작 구조

스마트 카드 판독모듈에서는 사용자가 판독기에 삽입한 스마트카드의 PIN(Personal Identification Number)[11]의 코드와 사용자 계정에 관련된 비밀키를 이용하여 복합적인 암호화 코드를 생성한다. 여기서 스마트카드 내의 PIN 코드는 카드내의 개인정보나 기타 데이터와 기능들을 접근할 때 검증을 위해 사용

되는 코드이다. 이렇게 생성된 암호화 코드는 인증서버를 통해 사용자 인증을 받아야 하며 또한 클라이언트는 인증 서버에서의 인증이 생성되기 전까지는 게임의 실행이 불가능하다. 그리고 항상 인증 및 게임 실행을 위해서는 스마트 카드와 판독기가 PC 에 부착되어 있어야 한다. 인증 서버 게이트웨이 모듈에서는 클라이언트로부터 전달된 코드의 유해성 및 안전성을 검사하고 이 코드에 대한 인증작업을 시작한다. 인증 작업이 완료가 되면 인증 서버 게이트웨이는 클라이언트에게 인증코드를 전송한다. 또한 인증 서버 게이트웨이는 게임의 진행 중에도 클라이언트로 인증확인 작업을 주기적으로 실행하여 스마트 카드의 무결성을 검사한다. 이 시스템의 장점은 기존의 게임 서버 시스템에 추가적인 장비의 설치 없이 좀 더 견고한 보안체계를 유지할 수 있다는 것이다.

3.1.2 사용자 인증 시스템의 동작 원리

스마트카드의 PIN 코드를 이용해 클라이언트와 게임 서버 간의 사용자 인증을 하는 과정은 [그림 2]와 같다. 사용자는 최초에 온라인 게임 클라이언트 프로그램에 접속하고 스마트카드를 판독기에 삽입하여 사용자 인증코드를 생성하고 이를 인증 서버 게이트웨이로 전송한다. 인증 서버 게이트웨이에서는 클라이언트로부터 전달 받은 인증코드에 대해 무결성 검사를 한 후 인증코드를 생성하여 클라이언트에게 전송한다. 클라이언트의 스마트카드 판독 모듈에서 이 인증코드를 받음으로써 게임이 실행된다.

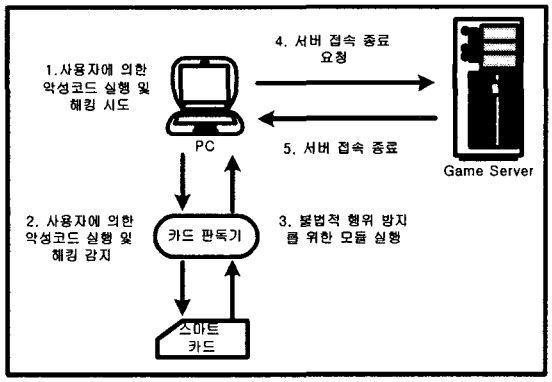
3.2 유해 코드 침입 방지 시스템 및 동작 원리

3.2.1 유해 코드 침입 방지 시스템 설계

유해코드 침입 방지 시스템은 기존의 MMORPG 게임에서 발생했던 해킹등과 같은 불법적인 행위를 클라이언트상에서 사전에 차단하기 위한 방법이다. 이를 위해 유해코드 침입 방지 시스템에서는 스마트카드 내부에 유해코드의 탐지 모듈이 데몬의 형태로 클라이언트가 게임서버에 접속하는 순간부터 종료할 때까지 탐지를 수행한다. 이 모듈의 역할은 유해코드로 인하여 클라이언트에서 서버로 패킷을 전송할 때 오류 코드가 전송되는 것을 차단하고 서버에 부하를 발생시키는 유해 코드를 사전에 탐지하여 유해 코드의 동작으로 인한 클라이언트와 서버간의 부하를 감소시키며 또한 MMORPG 게임상에서 발생하는 아이템 해킹과 같은 불법행위를 사전에 차단할 수 있다.

이 탐지 데몬 시스템의 동기화는 클라이언트에서 서버로의 사용자 인증 작업에 의해 동기화가 발생하고 일정기간 sleep 단계를 유지하다가 다시 인증 서버로부터 동기화가 발생하면 재동작을 한다. 그리고 유해 코드 탐지 모듈은 계속적으로 발생하는 유해코드들에 대한 탐지를 위해 패치 과정을 통해 업데이터가 가능하다.

3.2.2 유해코드 침입 방지 시스템의 동작 원리



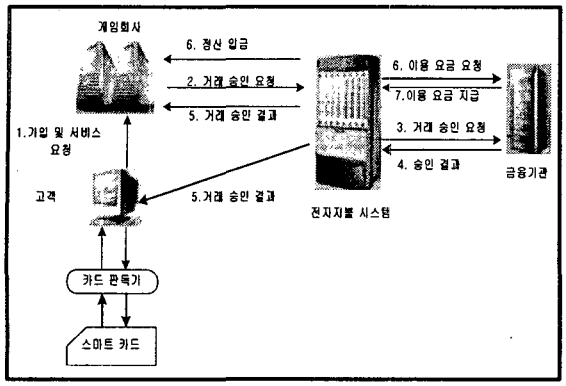
[그림 3] 유해코드 방지 시스템의 동작원리

유해코드 침입 방지 시스템의 동작 원리는 [그림 2]와 같다. [그림 2]에서 탐지 데몬 시스템은 사용자 인증 작업과 함께 로드 된다. 사용자가 유해코드를 통한 클라이언트 데이터의 정보 변경 및 게임상에서 발생할 수 있는 불법적인 행위를 시도하면 탐지 데몬 시스템이 탐지를 하여 클라이언트에게 경고메시지를 전송하고 서버에 접속 종료 요청을 보낸다. 게임서버는 요청을 승낙하고 클라이언트를 서버로부터 접속 종료 시킨다. 종료 후 게임 서버에 재 접속을 하기 위해서는 재 인증 과정이 필요하다.

3.3 과금 시스템 설계

스마트카드는 이미 실생활에서 온라인과 오프라인을 통한 전자상거래의 수단으로 검증이 된 인프라이다. 스마트 카드가 활용되는 환경 자체는 구조적 보안 취약성 때문에 거래내용, 신용카드번호, 계좌번호, 또 는 관련 비밀번호들의 거래 절차상 전달되는 개인 비 밀 정보들이 쉽게 누출될 수 있는 취약점을 가지고 있다. 이러한 환경하에서 보다 안전하고 신뢰성 있는 전자 상거래를 위해서는 데이터의 기밀성, 인증, 무결성, 부인 방지등과 같은 네 가지 특성이 요구 된다.

이러한 보안 취약성을 위해 전자 지불 시스템을 구축함으로서 서로 다른 특정 보안 알고리즘이나 지불 프로토콜 등을 사용하게 된다. 현재 스마트 카드를 이용한 전자지불 시스템 구축은 스마트카드 업체와 전자 상거래 업체 그리고 금융, 카드 업체들에 의하여 신용, 직불 카드를 위한 스마트카드 규격인 EMV 규격과 인터넷 전자상거래에 있어서의 신용카드 기반의 전자지불프로토콜인 SET[2]를 접목한 스마트카드 기반의 신용카드 전자지불 시스템을 구축하고 있다. 또한 신용 카드 기반의 전자지불 시스템에 더하여 전자지갑(스마트카드 형 전자화폐)[2]서비스도 추가함으로써 소액지불에 따른 지급결제수단으로도 사용이 가능하다.



[그림 4] 스마트카드를 이용한 과금 시스템

스마트카드를 이용한 과금 시스템은 [그림 3] 과 같다. [그림 3]에서는 전자상거래와 다른 다양한 분야에 널리 사용되고 있는 스마트 카드를 이용한 MMORPG 게임에서의 과금 시스템으로 설계한 것이다.

과금 시스템에서는 각 게임회사에서 발행하는 인증된 스마트 카드를 이용한 서비스 이용료에 대한 선불 정액제 형태로 과금이 가능하다.

현재 각 게임 서비스업체가 적용하고 있는 과금 체계를 전자 지불 시스템을 구축함으로써 간편하고 안전한 과금 지급 체계로의 전환이 가능하다.

4. 결론 및 향후 과제

본 논문에서는 MMORPG 게임의 보안상 취약점 및 과금 체계와 게임 컨텐츠 보호를 효과적으로 해결하기 위해 스마트 카드를 활용하는 시스템을 설계하였다. 기존 MMORPG 게임에서 갖고 있는 해킹과 유해코드의 실행을 통한 불법적인 행위를 방지하고 MMORPG 게임 서비스 제공에 대한 과금 시스템을 간편화함으로써 사용자와 게임사들에게 보안 취약에 대한 부담을 해결할 수 있고 과금에 대해 편의성을 제공한다. 우선적으로 스마트카드의 활용 시스템이 구현되려면 현재 게임 보안에 대한 일반사용자들이나 업체들의 관심이 집중되어야 하며 그 이후에 미흡한 관련 기술들의 개발이 이루어져야 한다.

5. 참고문헌

[1]Todd Barron, Multiplayer Game Programming, MIN Press, 2001, http://www.minpress.co.kr

[2] Steve McQuerry, Interconnecting Cisco Network Devices, 피어슨 에듀케이션 코리아, 2001

[3]리니지, NC 소프트, http://www.lineage.co.kr

[4]이강수, 고정호, 전은아, 최용준, "스마트카드 평가기준 해설서", 한국정보보호센터, 2000

[5] Microsoft Corp., 스마트 카드 백서, Microsoft Corp., 2000, http://www.microsoft.com/korea/technet/win2000/smtcard.asp

[6] 송유진, 영홍열, 이임영, 이만영, 김지홍, 류재철, 전자상거래 보안 기술, 생능출판사, 1999

[7] Windows 2000, Microsoft, http://www.microsoft.com

[8] 제페트로닉스, http://www.zepe.co.kr/

[9]Integrated circuit(s) cards with contacts, International Standards Organization, http://www.iso.ch/, 1997

[10] RS-232c 통신을 위한 교재, 무한 테크놀로지, http://www.moohantec.com

[11] 임영이, 이윤철, 강희일, 이동일, "스마트 카드시스템의 보안 기술", 전자통신동향분석 제 14 권 제 5 호, 1999