자바카드에서 다중 사용자 인증 및 파일 접근제어 구현

신상준°, 송영상, 신인철
단국대학교 전자컴퓨터공학과
{domx°, imagesys, char}@dku.edu

Implementation Multi-Users authentication and file Access control on Java Card

Sangjun Shin°, Youngsang Song, Inchul Shin
School of Electronics, and Computer Engineering, Dankook University

요 약

정보 통신의 발달로 인한 개인정보의 도용과 유출 및 불법적인 데이터의 사용을 차단하기 위한 많은 연구가 진행 되고 있다. 개인정보의 불법적인 유출을 막기 위해 스마트카드의 사용이 급증하고 있으며 현재 스마트카드보다 확장성 및 시스템 설계가 용이한 자바카드가 빠르게 보급되고 있는 추세이다. 본 논문에서는 정보보호 및 다양한 응용분야에 이용되는 자바카드의 기술규격(APDU)을 사용하여 다중사용자 인증과 사용자별 파일접근권한 시스템을 설계 및 구현하였다. 설계 구현한 시스템의 목적은 다수의 사용자 인증이 필요한 시스템에서 불법적인 정보의 유출을 방지하는 것이며 의료 분야 등 다양한 응용 프로그램에 적용이 가능하다.

1. 서 론

인터넷 및 정보 통신의 발달로 빠르고 다양한 정보의 혜택과 더불어 정보의 도용, 유출, 불법적인 데이터의 사용 또한 증가하고 있다. 따라서 개인 정보 보호와 인증에 관한 기술이 발달하고 있고 개인정보의 저장 및 인증을 담당해주는 스마트카드, USB토큰 등의 사용이 급증하고 있으며 관련 기술개발 또한 활발히 이루어지고 있다[1][2][3].

기존 사용되고 있는 인증 시스템은 개인 사용자를 목적으로 설계돼 있다. 그러나 정보 통신의 발달로 인한 다양한 서비스가 제공되고 있고 다중 사용자가 하나의 시스템에 접속 하게 된다는 가정을 할 수 있게 된다. 그래서 기존의 인증 시스템과는 다른 다중사용자인증 시스템의 구축을 필요로 하게 되었다.

스마트카드는 마이크로프로세서와 메모리를 내장하고 있는 칩을 가지고 있으며 개인 식별번호(PIN: personal identification number)가 저장돼 있어 타인의 사용이 불가능하고, 카드 발급자의 암호 키와 알고리즘이 카드에 내장되어 있어 외부의 침입 가능성이 없다. 스마트카드의 보안성, 휴대성, 편리한 사용법등의 특성을 이용하여 현재 통신, 금융, 교통, 신분확인, 전자화폐 등의 여러 응용 서비스에서 널리 사용되고 있으며 점차 그 용도가 확대되어 가고 있다[4][5][6]. 그러나 스마트카드는 칩 카드 제조사 마다 각각 상이한 COS(chip operating system)를 가지고 있어 다양한 어플리케이션의 접목이 어렵고 스마트카드의 업데이트를 통한 확장성이 떨어지며, 응용프로그램 작성이 어렵다는데 그 단점이 있다. 이것을 보안하기 위해 스마트카드 내에 자바 플랫폼을 내장한 자바 카드가 각광 받고 있는 추세이다[7][8].

자바카드는 자바 언어로 프로그램 되어 동작하는 스마트카드를 말하는데 객체지향언어인 자바를 사용 하여 카드 제조사에 관계없이 자바카드 가상 기계(JCVM: java card virtual machine)을 탑재하고 있어 서로 다른 플랫폼에서도 동작이 가능하며 다중 어플리케이션을 지원하고 애플릿의 추가 혹은 업데이트를 통해 어플리케이션의 추가가 가능하다[9][10][11].

본 논문에서는 부당한 정보의 사용을 차단하기 위해 자바카드를 이용하여 시스템을 설계한다. 스마트카드에서는 개인 사용자위주의 시스템을 구축 하였으나 애플릿의 추가를 통해 응용프로그램의 업데이트가 가능한 자바카드에서는 의료, 스포츠센터등 한 장의 카드에 다중 사용자 가 이용할 수 있는 시스템 구축이 필요하다. 따라서 다중 사용자 인증 시스템을 설계 하였다. 또한 다중사용자가 하나의 시스템을 이용할 경우 발생되는 정보의 부당한 수정, 노출, 파괴 등과 같은 보안상의 문제점을 해결하기 위하여 각 사용자마다 접근권한을 다르게 부여하여 불법적인 정보 유출을 방지할 수 있게 설계하였다. 애플릿 설계에서는 다중 사용자 인증과정을 실험할 수 있도록 3개의 PIN을 자바카드 애플릿에 이식 시켜 결과를 확인 하였고 또한 다수의 인증을 요구하는 시스템에서의 응용이 가능하도록 어플리케이션 프로그램을 설계하여 사용자별 PIN에 따른 파일 접근 제어 시스템을 구현하였다.

2. 자바카드

자바카드는 기존의 스마트카드에 자바 환경을 이식한 것으로 자바 기술을 스마트카드에 대해 최적화하여 구현하고 있으며 일반적인 스마트카드에 적용되는 모든 표준을 따르며 하위의 운영체제 위에 존재하는 자바카드 가상 기계가 자바카드 애플릿의 바이트 코드(byte code)를 수행하고 메모리, I/O 같은 카

드내의 모든 자원에 대한 접근을 제어한다는 점에서 스마트카드와 차이가 있다[9][12][13][14].

자바카드 기술은 플랫폼 간에 이진 코드의 이식성(portability) 즉 상호 운용성(interoperability)이 뛰어 나고 타입 검사 등에 대한 보안성을 가지고 있다. 또한 자바 가상기계가 내장되어있어 응용프로그램과 운영체제를 분리하는 개방형 운영체제를 가져오며 하드웨어 의존적인 어셈블리 코드가 아닌 상위 언어인 자바 언어로 쉽게 어플리케이션 프로그램을 작성 및 수행할 수 있게 되어 카드가 최종 사용자에게 발급된 이후에도 필요한 응용 서비스에 따른 응용 프로그램을 카드에 적재할 수 있다는 것이다. 자바카드는 자바카드 가상기계, 자바카드 수행 환경(JCRE: java card runtime environment), API(application programming interface), 애플릿으로 구성된다[15][16].

3. 시스템의 설계

자바카드는 여러 개의 애플릿을 장착하여 응용프로그램을 동작시키고 서로 다른 애플릿을 구분하기 위하여 AID(application identifier)를 생성시켜 주어야 하며 T=1인 메시지 전송 프로토콜에 따라 카드와 단말기 간에 전송이 이루어진다. T=1 프로토콜은 블록전송 프로토콜이라고 하며 T=0인 바이트 전송 프로토콜에 비해 보안성이 다소 개선된 프로토콜이다. 응용프로그램의 수행을 위해서는 APDU를 통해 카드에 명령어 전송, 카드에서의 명령어 처리 및 명령어에 대한 카드 응답으로 구성된다. APDU는 명령, 응답 APDU로 구분되는데 구조는 그림 1에서 나타내었다[9].

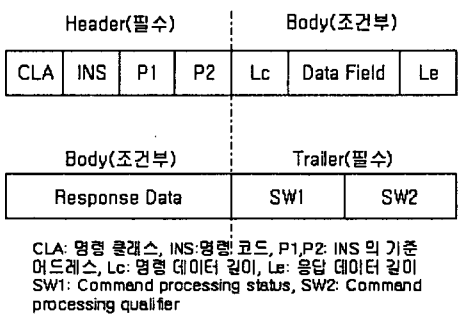

그림 1 명령, 응답 APDU

본 논문에서는 명령 APDU를 기반으로 하여 다중사용자 및 파일 접근제어 시스템을 구현한다. 따라서 각각의 사용자 접근권한 정의와 인증 프로토콜의 설계가 필요하다. 인증 프로토콜 설계는 관리자, 일반 사용자, 보조사용자 로 나뉘고 사용자별 개인 식별번호(PIN)와 파일 접근권한은 각각 다르게 주어지게 되고 카드에 접근할 때 개인별 접근 기록을 남기게 설계하여 사용자별 인증을 하게 된다. 자바카드 메모리에 저장된 각 파일들은 고유의 식별자와 파일 형식, 보안 변수, 파일에 대한 접근 조건에 대한 내용을 포함한 각종 정보를 갖는다. 사용자별 분류에 따라 접근 조건이 차별화 되며, 보안 변수는 파일이 요구하는 전자서명의 사용여부, 검증을 위한 보안모드 값들을 갖게 된다. 위와 같은 파일 접근 시스템과 보안 알고리즘을 구현하여 의료 시스템의 적용시켜보면 표1과 같은 파일 접근 시스템을 구현하게 된다.

기록 \ 권한	관리자 (의사)	일반 사용자 (약사)	보조사용자 (환자)
개인정보	N	N	R
주소정보	N	N	R
의료보험 카드번호	R	R	R
과거 병적기록	R	R	R
환자의 처방전	R, W	R	R
N: Not Access, R/W: Read, Write			

표 1 파일 접근 권한의 제어

애플릿은 사용자 인증과 파일 저장할 수 있도록 설계되어지며 어플리케이션 프로그램에서는 다중사용자의 접근 시 우려되는 정보의 수정, 노출, 파괴 등의 보안상의 문제점을 고려하여 각 파일마다 접근 권한을 다르게 부여하여 파일별 접근 권한과 보안 유형이 상이하게 설계되어 인증 받지 않은 사용자의 파일 접근을 불허 하도록 설계하였다.

4. 시스템의 구현

본 논문의 시스템 개발환경으로는 윈도우2003 서버에서 자바카드 2.1.2 기술버전을 사용했으며 애플릿의 설계는 자바관련 통합 개발 환경을 제공하는 Eclipse와 JCOP Tool3.0을 사용하였고, 사용된 자바 카드는 T=1 프로토콜에서 동작하는 IBM사의 JCOP카드이며 카드리더기로는 삼성전자의 SCR 331을 사용하여 구현하였다. 사용자 인증을 담당하는 테스트 애플릿의 구현은 APDU관련 명령어의 정의와 각 메소드를 정의 한다. 그림2에서는 사용자인증 애플릿 설계부분을 보여주고 있다.

```
protected TestA(byte[] Data, short Offset, byte Length)
{
pin1= new OwnerPIN(PIN_TRY_LIMIT,    MAX_PIN_SIZE);
pin1.update(mypin1, (short)0, (byte)mypin1.length);
pin2 = new OwnerPIN(PIN_TRY_LIMIT,    MAX_PIN_SIZE);
pin2.update(mypin2, (short)0, (byte)mypin2.length);
pin3 = new OwnerPIN(PIN_TRY_LIMIT,    MAX_PIN_SIZE);
pin3.update(mypin3, (short)0, (byte)mypin3.length);
ID_File = new byte[80];
Temp_Name=JCSystem.makeTransientByteArray((short)10,
JCSystem.CLEAR_ON_DESELECT);
register();
}
```

그림 2 사용자 인증 애플릿 구현

설계된 애플릿 AID는 "00112233445501"이며 그림2에서는 자바카드상의 애플릿을 확인할 수 있는 Cardman.exe 프로그램을 이용하여 자바카드에 실제 로딩된 애플릿을 보여주고 있다.

본 논문에서는 Boland C++ Bulider 6.0을 사용하여 사용자별 파일 접근 제어 어플리케이션 프로그램을 설계하였다.

구현된 시스템은 사용자의 PIN제출이 이루어지면 자바카드 내에서 PIN값을 비교하여 사용자 인증이 이루어지며, 어플리케이션에서는 사용자별 권한이 주어지게 된다. 각각 분할된 아스키코드 형식의 파일을 헥사파일 형식으로 변환하여 자바카드에 업로드 시키게 된다. 카드에 저장된 정보는 주어진 권한에 따라 읽거나 쓸 수 있게 된다. 그림3에서는 사용자별 접근 권한 시스템을 보여주고 있다.

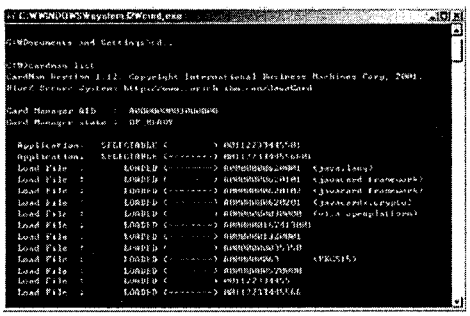

그림 3 자바카드의 내용

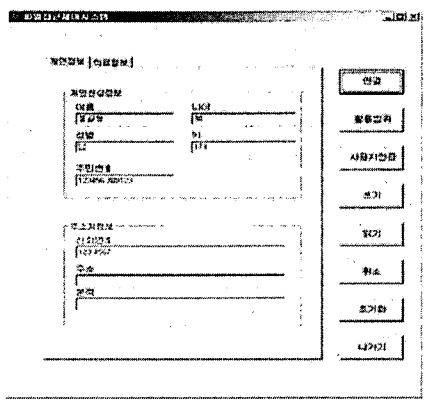

그림 4 파일접근제어 프로그램

5. 결론 및 향후 과제

현재 스마트카드는 보안성, 휴대성, 편리한 사용법등의 장점을 바탕으로 다양하게 응용되어 널리 사용되어지고 있고 개인 사용자 위주의 시스템으로 개발 되어 오고 있다.

본 논문에서는 기존의 시스템과는 달리 여러 명의 사용자가 한 장의 카드를 사용한다는 가정 하에 사용자별 인증 및 파일 접근 권한 시스템을 설계하였고, 다중사용자 인증을 위한 애플릿을 설계하였으며 어플리케이션 프로그램을 이용 관리자, 일반 사용자, 보조 사용자의 등급을 구분하여 인증과 파일 접근 통제가 동작되는 것을 확인하였다. 또한 사용자와 시스템간의 신뢰도를 제공하고 개인정보의 안전성과 신뢰성을 보장하게 된다. 따라서 본 논문에서 설계된 시스템은 의료, 스포츠 센터 등 다중사용자 인증을 필요로 하는 시스템에 적용 가능하다.

향후 연구과제로는 제한된 하드웨어를 가지고 있는 자바카드 효율적인 자원관리를 위해 애플릿 간에 최적화된 파일 공유 시스템을 구축하여 자바카드 내에서 파일 접근 시스템을 구현하는 것이 필요하다. 또한 자바카드 기반의 어플리케이션 프로그램에서 파일의 이동시 암호화 과정을 거친다면 보다 더 신뢰성 있는 시스템의 설계가 될 것이다.

참고문헌

[1] Walczowski, L.T, Deravi, F. "Training in the use of Java smart cards for embedded applications" The 8th IEEE International Conference on Volume 2, 2-5 Sept. 2001

[2] Zhang Jianjie, Li Feihui, Ge Yuanqing, Yue Zhenwu, Yang Zhilian, "A Java processor suitable for applications of smart card" 4th International Conference on 23-25 Oct. 2001

[3] B.Nichael, B.Peter, E.Thomas, H.Frank, O.Marcus, "Java Card -Form Hype to Realty", IEEE Concurrency, Oct.-Dec, 1999

[4] Java Card™ 2.2 Virtual Machine Specification, Sun Microsystems, Inc., Early Access, 2001

[5] Lodovic Casset, "Formal Development of an Embedded Verifier for Java Card Byte Code" International Conference on Dependable System and Networks, 2002

[6] Patrice Peyret, "Java Card Technology for Smart Card Architecture and Programmer's Guide", April 2000

[7] 황성명, 엄희균, " 자바카드 애플릿의 검증 방법", 한국정보처리학회 소프트웨어공학연구회지. Vol.5, No.1, 2002

[8] 강세나, 이기한 "IC 카드에 의한 원외 전자처방전 보안을 위한 시스템 구축", 정보처리학회 논문지, Vol.c,No.3, 2003

[9] Zhiqun Chen, "Java Card Technology for Smart Cards: Architecture and Programmer's Guide Foreword by Patrice Peyret", Addison Wesley, 2000

[10] Uwe Hansmann, "Smart Card Application Developement Using Java", Springer, 2002

[11] Wolfgang Effing and Wolfgang Rankl, "Smart Card Handbood", Jahn Wiley & Sons, 2000

[12] Vesna Hassler, "Java Card for E-Payment Application", Artech House, 2002

[13] Sun Microsystems, "Java Card™ 2.1.1 Application Programming Interface", May 2000

[14] Jose Luis Zoreda jose Manuel Oton, "SmartCards", Artech House Boston Sondon, 1994

[15] E.Vetillard, "Tools for Integrating the Java Card™ API into Jini™ Connection Technology", javaoneconf., 2000

[16] 탁승호, "Let's Smart Card", 성안당, 2004