論文
7 - 5 - 4

자바카드기반 다중 사용자 파일접근에 대한 애플릿 설계 및 구현 (Design and Implementation of Applet for Multi-Users File Access based on Java Card)

김범식(Bum-Sik Kim)[1)]

요약

정보 통신의 발달로 인한 편리함과 동시에 정보의 유출 및 불법적인 데이터의 사용 또한 급증하고 있다. 따라서 불법적인 정보의 유출을 차단하기 위한 많은 연구가 진행 되고 있으며 개인정보의 보호를 위해 스마트카드의 사용이 급증하고 있다. 최근 자바카드는 스마트카드가 가지고 있는 기술적 문제점을 보완 할 수 있는 대안으로 빠르게 보급되고 있는 추세이다.

본 논문에서는 정보보호 및 다양한 응용분야에 이용되는 자바카드를 기반으로 다중사용자 인증과 사용자별 파일접근권한 시스템을 설계 구현하였다. 파일 접근 권한의 부여는 애플릿에 권한 테이블을 작성하여 사용자별 파일 접근 권한의 처리가 이루어진다. 따라서 하나의 자바카드 내에 있는 여러 개의 파일이 접근 권한에 따라 읽기/쓰기 등이 선별적으로 이루어진다. 이로서 다중 사용자접근 시 우려되는 불법적인 정보의 수정, 노출, 파괴 등을 방지할 수 있게 되며 다수의 인증을 요구하는 시스템에서 응용이 가능하다.

Abstract

Whereas conveniences deriving from the development of information and telecommunication technology increase, information outflow and illegal data use are also rapidly on the rise. Consequently, many studies to prevent illegal information outflow are currently under way, and the use of Smart Card is in steep jump. Recently, Java Card is diffused fast as an alternative to complement the technical problems of the Smart Card. This paper designed and Implementation the system for multi-users authentication and file access control by user through designing a Java Card applet that is used for information protection and in various application fields. For allowing a file access competence, each user's file access competence is processed via drawing up the access condition table in the applet. Therefore, illegal correction, exposure and destruction of information, which become the concerns when multi-users have an access, can be prevented. In addition, its application becomes possible in the system requiring multi-users certifications.

논문접수 : 2006. 9. 15.
심사완료 : 2006. 10. 9.

1) 정회원 : 여주대학

1. 서론

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

기존 스마트카드 시스템은 개인 사용자를 목적으로 설계 활용 되고 있다. 그러나 경제 활동의 다양화와 정보 통신의 발달로 인한 신종 서비스의 출연에 다중 사용자 가 하나의 시스템에 접근 한다는 가정을 할 수 있게 되었다. 따라서 기존의 인증 시스템과는 다른 다중 사용자 인증 시스템의 구축 또한 필요 하게 되었다.[3][4]

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 침입가능성이 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. 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.[5][6][7]

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.[8][9][10]

본 논문에서는 부당한 정보의 사용을 차단하기 위해 자바카드를 이용하여 시스템을 설계한다. 또한 자바카드를 이용 개인 사용자인증 시스템을 벗어난 다중 사용자 인증 시스템을 구축 하고 애플릿의 추가를 통해 금융, 의료, 스포츠 등의 서비스를 한 장의 카드로 통합 시킬 수 있는 시스템의 토대를 마련한다. 또한 다중 사용자가 하나의 시스템을 이용할 경우 발생되는 정보의 부당한 수정, 노출, 파괴 등과 같은 보안상의 문제점을 해결하기 위하여 각 사용자마다 파일 접근권한의 부여를 다르게 하여 불법적인 정보 유출을 방지할 수 있도록 설계하였다. 자바카드 내부에 기록된 각각의 파일은 사용자인증을 거친 뒤 파일 접근권한 테이블(access condition table)의 주어진 정보에 따라 권한의 부여가 이루어지게 된다. 파일 접근 권한 테이블은 자바 카드 내부에 이식 시켜 제출된 PIN에 따라 사용자의 파일 접근 권한이 주어지게 되도록 설계되어 부당한 사용자의 카드 내부의 정보 접근을 불허 하여 정보 유출 및 도용을 방지할 수 있도록 설계하였다.

본 논문에서는 다중 사용자 인증과 파일 접근 권한 테이블을 내장된 애플릿 설계를 통해 다수의 인증을 요구하는 시스템에서 응용이 가능하도록 설계하였다.

2. 자바카드 관련 기술

본 장에서는 자바카드의 기술적인 부분에 대해 기술 하였다. 자바카드는 스마트카드가 제공하는 보안, 기술규격을 제공하고 있으며 동시에 다양한 어플리케이션의 접목과 업데이트를 통한 확장 등의 장점을 가지고 있다. 이러한 자바카드의 보안 특성은 보안 메커니즘, 보안 블록과 개인 식별 번호를 통한 메모리 부분에 대한 접근 제어를 할 수 있게 되며 각종 정

보가 포함된 파일의 접근 권한을 다르게 두어 기밀성의 강화와 양방향 통신을 통한 사용자의 참여로 인한 부인봉쇄, 사용자가 직접 소지하여 직접 전송해준 데이터의 무결성 또한 검증받을 수 있는 시스템의 구축을 할 수 있다.

2.1 자바카드 보안 메커니즘

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 기계(Java Card Virtual Machine)가 자바카드 애플릿의 바이트 코드(byte code)를 수행하고 메모리, I/O 같은 카드내의 모든 자원에 대한 접근을 제어한다.[11][12]

자바카드에서의 가상기계를 이용에 의한 장점은 응용프로그램과 운영체제를 분리하는 개방형 운영체제를 가져오며 하드웨어 의존적인 어셈블리 코드가 아닌 상위 언어인 자바 언어로 쉽게 응용프로그램을 작성 및 수행할 수 있으며 카드가 최종 사용자에게 발급된 이후에도 필요한 응용 서비스에 따른 응용 프로그램을 카드에 적재할 수 있다는 것이다. 이에 따라 다양한 다수의 응용 프로그램을 수용할 수 있는 유연성을 가지게 된다. 또한, 자바카드에서는 자바 언어 자체의 보안 특성 이외에 응용프로그램간의 방화벽을 제공함으로써 엄격한 보안성을 보장하며 자바카드 플랫폼은 스마트카드의 기술을 충분히 안정적으로 제공하고 있다.[9][13]

2.2 파일 접근 제어

자바 카드는 16~32Kbyte 의 메모리(EEPROM)를 확보 하고 있으며 각 파일은 고유의 식별자와 파일 형식, 보안변수를 가지며 접근 조건에 대한 각종 정보를 가지게 된다. 보안 변수 값으로는 파일이 요구하는 개인 식별 번호와 파일에 저장돼 있는 파라미터 값 등이며 각 파일들은 저장하고 있는 정보의 내용에 따라 각기 다른 권한을 부여 받으며 보안 변수에 따라 접근 조건이 차별화 된다.[14][15]

3. 시스템 설계

자바카드는 여러 개의 애플릿을 장착하여 응용프로그램을 동작시키게 되며 서로 다른 애플릿을 구분하기 위하여 AID(application identifier)를 생성시켜 주어야 한다. 실험 및 구현에 사용된 JCOP 카드는 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.[9][16] APDU는 명령, 응답 APDU로 구분되는데 구조는 그림 1에서 나타내었다.

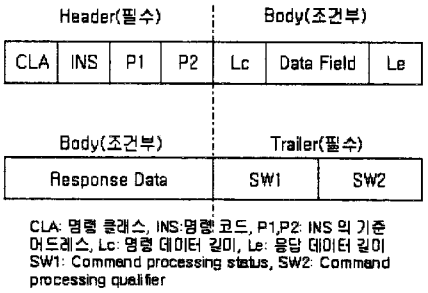

그림 51 명령, 응답 APDU

본 논문에서는 명령 APDU를 기반으로 하여 다중사용자 및 파일 접근제어 시스템을 구현한다. 따라서 각각의 사용자 접근 권한 정의와 인증 프로토콜의 설계가 필요하다. 프로토콜 설계에서는 다중 사용자 인증을 위해 4개의 PIN을 카드 내부에 이식 하였으며 각 사용자별 파일 접근 권한의 부여를 위해 애플릿에 사용자 권한 테이블을 장착하여 사용자의 보안 모드에 따라 파일 접근권한을 각각 다르게 주어지게 설계 하였다. 애플릿 테스트를 위해

APDU header 부분을 표1과 같이 정의 하였다.

Header	값	정의
CLA	0x90	인증, 쓰기, 읽기 클래스 정의
INS	0x24	데이터의 읽기
	0x26	데이터의 쓰기
P1	0x01~0x0A	P1값을 변화 하여 쓰거나 읽을 수 있는 파일을 나타낸다.
P2	0x00	사용하지 않음

표 1 APDU header 정의

본 논문에서 제안된 시스템의 프로토콜은 그림2와 같이 설계되었다.

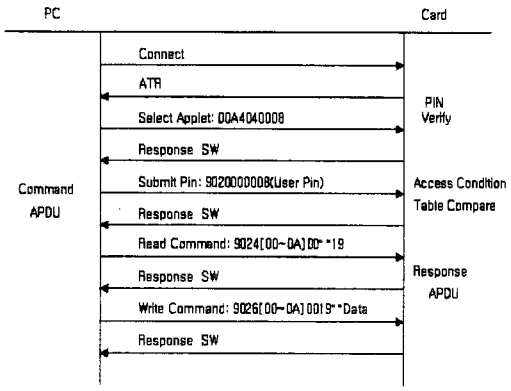

그림 52 제안 시스템의 프로토콜

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.

```
protected void cmdReadID(APDU apdu)
    short user_index = 0;
    byte[] buffer = apdu.getBuffer();
// User Check
if ( PIN1.isValidated() ) user_index = 0;
if ( PIN2.isValidated() ) user_index = 1;
if ( PIN3.isValidated() ) user_index = 2;
if ( PIN4.isValidated() ) user_index = 3;
// P1 = File Number
  byte FileNo = buffer[ISO7816.OFFSET_P1];
// Calculate Access Condition Table Offset
  short ACC_Offset = (short)( FileNo *
                              COUNT_USER );
// Auth Check
if((EF_ACC_TABLE[(short)(ACC_Offset+user_index)]
    != ACC_READONLY) &&
(EF_ACC_TABLE[(short)(ACC_Offset+user_index)]
    != ACC_READWRITE) )
ISOException.throwIt(SW_PIN_VERIFICATION_REQUIR
ED);      // Length Check (Le)
if (buffer[ISO7816.OFFSET_LC]
     != SIZE_ID_FILE )

ISOException.throwIt(ISO7816.SW_WRONG_LENGTH);

 // Calculate ID_File Offset
 short ID_Offset = (short)(FileNo *
                           SIZE_ID_FILE);
// Send Response Data

Util.arrayCopyNonAtomic(EF_ID,ID_Offset,buffer,(short
)0, SIZE_ID_FILE);
apdu.setOutgoingAndSend((short)0,
                           SIZE_ID_FILE);
}
```

그림 3 파일 접근 권한 애플릿 설계

그림3은 읽기 명령에서 파일 접근 권한에 대한 애플릿 설계부분을 보여주고 있다. 설계된 애플릿 AID는 "0011223344556601"이며 그림4에서는 자바카드상의 애플릿을 확인할 수 있는 Cardman.exe 프로그램을 이용하여 자바카드에 실제 로딩된 애플릿을 보여주고 있다.

다중 사용자 인증과 애플릿 내에 내장된 권한 테이블에 의한 파일 접근 시스템을 테스트 해보기 위해 카드 내부에 각각 25Byte의 파일 사이즈를 갖는 10개의 파일을 생성 하였고

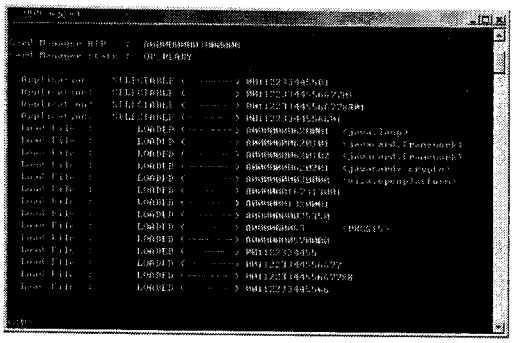

그림 4 자바 카드의 내용

Boland C++ Bulider 6.0을 사용하여 자바 카드의 정상 동작 여부를 확인하였다. 그림 5에서는 User2의 파일 읽기 권한을 보여주고 있다.

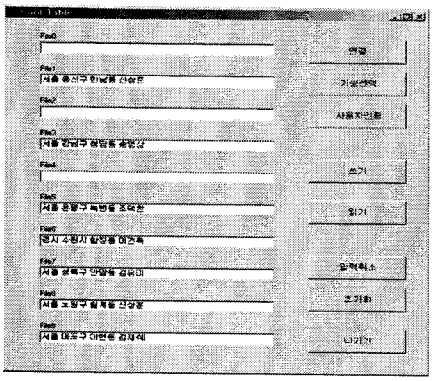

그림 5 User2의 파일 읽기 권한 테스트

5. 결론

현재 스마트카드는 보안성, 휴대성, 편리한 사용법등의 장점을 바탕으로 다양하게 응용되어 널리 사용되어
지고 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 인증 및 파일 접근 권한 애플릿을 설계하였다. 또한 응용프로그램을 설계 하여 카드에 내장된 권한 테이블에 따른 파일 접근 통제를 확인 하여 사용자와 시스템간의 신뢰도를 제공하고 개인정보의 안전성과 신뢰성을 보장함을 볼 수 있었다. 설계된 시스템은 의료, 스포츠 센터 등 다중사용자 인증을 필요로 하는 시스템에 적용 가능하다.

향후 연구과제로는 제한된 하드웨어를 가지고 있는 자바카드 효율적인 자원관리를 위해 파일 시스템 API를 적용하여 최적화된 파일의 관리와 파일의 생성 과 함께 애플릿 간에 파일 공유 시스템을 구축연구해 보고자 한다. 또한 자바카드 기반의 어플리케이션 프로그램에서 파일의 이동시 암호화 과정의 추가로 보다 더 신뢰성 있는 시스템의 설계가 필요 하다.

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