JAVA CARD기반의 사용자 인증 및 파일 접근권한 Applet 설계

구은희° 신인철
단국대학교 전자컴퓨터공학과
단국대학교 전기전자컴퓨터공학부
{koohee°, char}@dankook.ac.kr

Applet Design of File Access Control and User Authentication based on Java Card

Eunhee Gu° Inchul Shin
Dept of Electronics & Computer Engineering, Dankook University
School of Electrical & Electronics & Computer Engineering, Dankook University

요 약

최근 개인자료의 유출 및 불법적인 사용이 사회적으로 큰 이슈가 되고 있어 개인의 정보보호 및 신분확인에 대한 요구가 증가하게 되었다. 이로 인하여 최근 안전한 데이터 전송과 거래를 위해 스마트카드의 이용이 증대되고 있는 추세이다. 특히 자바카드는 스마트카드 플랫폼에 자바의 기술을 접목시킨 것으로 양방향 통신, 정보의 보호기능 등을 수행할 수 있으며, 개인을 확인할 수 있고 이동성이 뛰어나며 복제가 어렵고 암호 알고리즘을 카드 내부에서 수행하여 보안상 매우 좋은 이점을 지니고 있어 스마트카드에서 필요로 하고 있는 다양한 서비스의 내용을 충분히 안정적으로 제공하고 있다.

본 논문에서는 이런 다양한 응용분야에 이용되는 자바카드의 보안성을 높이기 위하여 기존의 단순한 사용자 인증에 사용되는 PIN정보와 생체정보인 사인데이터를 함께 이용한다. 또한 개인에 따른 정보를 저장하는 방법과 이 정보를 접근하기 위하여 데이터를 사용하는 사용자간의 접근을 제한하기 위한 사용자의 접근권한을 설계하였다. 이와 같은 Applet을 설계함으로써 개인정보의 보다 안전하고 신뢰성을 보장하고 개인의 불법적인 유출 및 도용의 완벽한 제어가 될 것으로 기대된다.

1. 서 론

오늘날 통신 분야의 급속한 발달로 이를 이용한 다양한 서비스가 확산됨에 따라, 인증과 보안은 아주 중요한 분야로 대두되고 있다. 이로 인해 실용적이고 효과적인 정보보호 서비스를 제공하기 위해서 스마트카드의 사용이 급증하고 있으며, 이와 관련한 기술개발이 활발히 이루어지고 있다. 이러한 발전으로 기존의 메모리 및 CPU 처리 속도 등의 제약된 자원의 스마트카드를 겨냥하여 보다 사용이 편리하고 처리능력이 뛰어난 개념이 도입되고 있다[1],[2].

기존의 스마트카드에 Java Card platform을 내장한 즉, 모든 표준을 따르는 전형적인 스마트카드인데 하위의 운영체제 위에 존재하는 Java Card 가상 기계(Java Card Virtual Machine : JCVM)가 Java Card Applet의 바이트 코드를 수행하는 Java Card를 사용하게 되었다. Java Card 기술은 플랫폼간의 이진 코드의 이식성이 뛰어나고 악의적 코드에 대한 보안성을 지닌 Java 언어를 사용함으로써 정보보호 특성을 그대로 보존할 뿐만 아니라, 쉽게 응용프로그램을 작성하여 응용할 수 있다[3],[4],[6].

자바 카드는 응용 프로그램과 운영체제를 분리하는 개방형 운영체제를 가져오며 카드가 최종 사용자에게 발급된 이후에도 필요한 응용서비스에 따른 응용 프로그램을 카드에 적재할 수 있다[3],[4],[5],[7]. 따라서 다양한 다수의 응용 프로그램을 수용할 수 있고, 다수의 사용자가 하나의 시스템에 접근하는 형태를 가지는 형태를 띤다. 이런 시스템의 형태 때문에 카드를 사용하기 위해서는 사용자 인증이 필요하다. 기존의 인증방법은 PIN(Personal Identification Number)을 이용하여 이루어지고 있다.

본 논문에서는 기존의 인증방법인 PIN을 이용한 사용자 인증과 보다 높은 보안성과 편리성을 제공하기 위해 사람의 신체특징을 이용한 생체 정보를 이용하여 사용자 인증을 제공한다.

또한 다수의 사용자가 시스템을 사용하는 경우 개인의 정보자원 등을 부당한 사용자로부터 사용되거나, 수정, 노출, 파괴와 같은 비합법적인 행위로부터의 보안이 필수적인 요소가 되었다.

본 논문에서는 이러한 정보시스템의 저장, 관리되는 기술 중의 하나인 접근통제방법을 이용하여 관리자와 사용자들 간의 접근권한이 다르게 부여되는 시스템을 설계하였다.

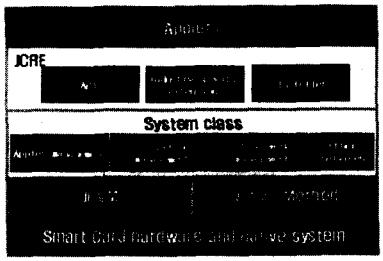
2. 시스템의 개요

2.1 자바카드(Java Card)의 개요

자바카드는 일반적인 스마트카드에 장애요소를 보안하기 위한 카드인데 하위의 운영체제인 COS(Card Operating System)위에 자바카드 가상기계인 JCVM이 있는 구조 즉, Open Platform 형식의 개발 환경이다.

하드웨어 플랫폼에 독립적이고 보안성이 우수하며 개발 시간 및 비용이 절감되고 다중 어플리케이션을 할 수 있는 장점을 가지고 있다[4],[5],[7].

자바카드는 [그림1]에서 보는 것처럼, 자바카드 API(Application Programming Interface)와 JCVM으로 이루어진 자바카드 수행환경(Java Card Runtime Environment : JCRE), COS, H/W 및 응용 프로그램인 애플릿으로 구성된다[3].



[그림1] 자바카드시스템 구조

2.2 제안한 시스템의 개요

자바카드에 필수적인 보안기능은 사용자 인증과 접근제어 이다. 다수의 사용자가 하나의 시스템에 접근하는 형태에서는 사용자 인증을 위해 시스템에 접근자의 신원을 확인하는 방법으로써 사용자가 알고 있는 것, 사용자가 가진 것 또는 사용자의 물리적, 행동적 특성으로 사용자를 확인한다. 이중 사용자 인증을 강화하기 위하여 인증에 활용할 수 있는 하드웨어를 사용하여 복잡성을 높임으로써 인증의 강화효과를 가지는 수단을 가져온다. 자바카드는 저장 내용을 임의로 수정하기 어려운 메모리를 가지고 있고, 프로세서를 포함하고 있어 내부 연산이 가능하다는 장점을 제공한다.

일반적으로 이용되는 인증 방법으로 가장 간단한 방법은 PIN 기반의 인증 방법이다. 이러한 인증 방식은 카드상에서 PIN 매칭을 수행함으로 이루어진다. 단말기에서 전송된 값과 카드의 PIN값을 비교하여 일치하면 카드는 단말기를 인증하여 타당한 단말기로서 인식한다. 또 카드의 어플리케이션이 많아지면서, 사람들은 갈수록 여러 개의 PIN 번호를 기억하도록 요구한다. 그러나 이러한 간단한 기법은 카드의 분실이나 사용자가 PIN을 잃어버리는 문제점이 있기 때문에 최근에는 개인을 식별하기 위한 방법으로 생체측정 기법들이 강조되고 있다.

생체측정법은 개인을 명백히 식별하기 위하여 인간의 생체적 특징을 측정하는 즉, 실제 사람자체를 식별하는 것이다. 따라서 각 개인에 유일무이 하면서 측정될 수 있는 생체학적 기법 중 서명(signature)을 이용하여 PIN 코드와 함께 동시에 사용하여 카드 어플리케이션의 운영자에게 트랜잭션의 조건/조항에 동의함을 표시하는 행위로 사용하였다.

시스템의 자원과 정보에 접근하기 위해서는 접근제어 시스템의 허가를 얻어야만 한다. 즉, 관련된 모든 시스템 호출은 접근제어 시스템을 통해서 허가된 경우에만 처리된다. 사용자는 접근제어 사용자 인터페이스를 통해 시스템 자원에 설정된 접근제어 관련 정보를 설정하거나 확인할 수 있다.

3. 제안한 시스템 구조

파일은 카드에 Application 데이터를 저장하는 단위로서 MF, DF, EF에 의해 3레벨의 파일구조를 가진다. 파일의 종류는 DF(Dedicated File), EF(Elementary File)로 나뉘며, DF는 파일의 디렉터리 구조를 나타낸다. DF는 다시 2종류로 나뉘어 지는데 DF들 중 루트 디렉터리에 해당하는 파일은 MF(Master File)라고 하고 이외의 파일들을 DF라고 한다. EF는 실제로 데이터가 저장되는 파일을 나타낸다. EF도 2종류로 나뉘어 지는데 카드의 운영체제가 사용하는 IEF(Internal Elementary File)와 응용 서비스의 정보를 저장하는데 사용하는 EF이다.

본 논문에서는 관리자, 일반 사용자, 보조 관리자로 나뉘어 카드가 사용된다. 관리자의 파일시스템은 일반 사용자의 개인정보 DF와 그 아래의 각종 데이터 EF와 보조 관리자의 신분 확인을 위한 DF와 그 아래 처리 EF가 있고 관리를 위한 DF와 신분 정보 및 확인을 위한 EF로 구성되어 있다. 일반 사용자의 파일 시스템은 MF 아래 개인 정보에 대한 DF와 각종 데이터를 담고 있는 EF들로 구성되어 있고, 보조 관리자의 파일 시스템은 MF 아래 신분 확인을 위한 DF와 그 아래 처리 데이터 EF들이 있다.

각각의 사용자에게 접근 권한을 정의는 접근권한 주체인 사용자를 정의하고, 인증 프로토콜을 설계하고, 접근권한 유형을 설정한다. 인증 프로토콜은 관리자는 개인식별데이터(signature), 일반 사용자 개인식별데이터(signature), 보조 관리자 개인식별번호(PIN)로 나뉘어진다. 각 사용자의 DF, EF의 권한 유형은 DF, EF를 접근하는 제어 목적으로 불리언 식의 규칙을 가지고 나눈다. 관리자는 모든 권한을 주고, 보조 관리자는 보조 관리자 DF 및 EF의 모든 권한과 일반 사용자 일부 EF 일부 권한을 부여하고, 일반 사용자는 자신의 일부 EF의 모든 권한과 나머지 EF 및 DF의 일부 권한만을 부여한다. [표1]은 본 논문에서 제안한 파일권한을 나타내었다.

		관리자(A)					일반사용자(U)					보조사용자(S)				
사용자 인증 Type		개인식별데이터 (signature)					개인식별데이터 (signature)					개인식별번호 (PIN)				
		a	r	w	e	d	a	r	w	e	d	a	r	w	e	d
DF 권한 유형	A	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o
	U	x	x	x	x	x	o	o	x	x	x	x	x	x	x	x
	S	x	x	x	x	x	x	x	x	x	x	o	o	x	x	x
EF 권한 유형	A	o	o	o	o	o	o	o	o	o	o	o	o	o	o	o
	U	x	x	x	x	x	o	o	o	o	o	o	o	x	x	x
	S	x	x	x	x	x	o	o	o	o	x	o	o	o	o	o
A : 관리자, U : 일반사용자, S : 보조사용자																
a: Access, r: Read, w: Write, e: Edit, d: Delete																

[표1] 제안 시스템의 접근권한

4. 제안 시스템의 Applet 구현

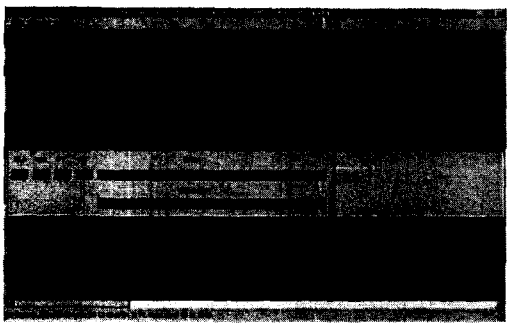
본 논문에서 제안한 시스템의 Applet을 구현하기 위하여 [표2]와 같은 환경을 이용하여 테스트 하였다.

종류	세부사항
운영체제	Window 2000 Server
개발도구	J2se verson 1.2.2 Java(TM) Communications API specification2.0 Java_card_kit_2_2_1
개발언어	Java
카드	Jcop 2.0, Smartcafelife(G&D)
단말기	SCRx31 CCID, PCT2000(G&D)

[표2] 시스템 구현 환경

카드와 단말기 사이의 통신을 위하여 APDU를 사용하였다. 카드와 단말기 사이의 접속 시에는 항상 인증 단계가 요구되게 하였으며 각각의 사용자는 임의로 정하여 애플릿으로 구현하였다. 또한 통신 프로토콜을 본 논문에서 제안한 프로토콜을 이용하여 시스템과 통신을 하였다.

자바카드 상에서 프로그램이 진행되는 과정을 위해서는 APDU의 command와 response명령을 주고받으며 통신을 하며 response명령어가 '9000'이란 값을 지니면 그 과정이 성공 했다는 것을 의미한다. [그림2]에서 보여지는 것은 카드에 있는 PIN값과 입력한 PIN 값이 동일한지를 비교하여 사용자를 판별하여 승인된 사용자를 보여주는 것이다.



[그림2] 접근권한 및 사용자인증 성공

6. 결 론

본 논문에서 구현한 시스템은 사회전반에 걸쳐 사용자의 정보를 좀 더 안전하게 사용하려고 스마트카드의 업계 표준으로 자리 잡고 있는 Java Card를 중심으로 접근권한을 두는 Applet을 설계하였다.

본 연구에서 카드는 개인만이 쓰는 것이 아니라 다수의 사용자가 접근하는 카드 이므로 개인의 정보를 개인의 승낙 없이 활용하거나 유출하는 것을 방지하기위하여 카드의 접속 시에는 항상 PIN과 생체인식 정보인 서명데이터를 이용하여 사용자 인증을 하였다. 또한 사용자에 따라 보안등급이 다른 정보와 서비스를 제공할 수 있도록 구성되었다. 이러한 Applet를 설계함으로써 사용자와 시스템간의 신뢰를 제공하여 개인정보의 안전성과 신뢰성을 보장하는 것을 확인하였다. 하지만 이러한 안전성과 신뢰성에도 불구하고 기존의 PIN으로 사용자 인증을 하는 시스템보다 처리속도가 조금 떨어진다. 하지만 계속되는 Java Card의 발전과 생체정보의 데이터사이즈의 축소로 이러한 약점은 충분히 극복될 것으로 보인다.

향후 현재까지 사용되고 있는 사용자 패스워드 또는 PIN데이터를 모두 다양한 생체인식정보와 결합하여 사용되어질 것이고, 이 또한 여러 응용분야로 발전할 수 있을 것이다.

참고문헌

[1] Jose Luis Zoreda Jose Manuel Oton, "Smart cards", Artech House Boston Sondon, 1994.

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

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

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

[5] Patrice Peyret, "JavaCard Technology for Smart Cards Architecture and Programmer's Guide", Apri 2000.

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

[7] Zhiqun Chen, "Java Card Technology for Smart Cards", Addison-Wesley, 2000.

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

[9] Eric Vetillard, "Java Card 2.1 general presentation", Gemplus Developer Conference, 1999.

[10] Gemplus, "GemXpresso 2.4 PK User Guide, Getting Started", October 1999.

[11] J.Bigun, "Multi-modal Person Authentication", Face recognition, Sringer-Verlag, 1997.

[12] C. Schnorr, "Efficient Signature Generation by Smart Cards", Journal of Cryptology, Vol.4, No.3, 1991.

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

[14] 임영이, 이윤철, 강회일, 이동일, "스마트카드 시스템의 보안 기술", 전자통신동향분석, Vol.14, No.5, 1999.

[15] 김연선, 이창욱, "자바카드 애플릿 설계 및 검증에 관한 연구", 한국통신정보보호학회 종합학술발표회 논문집, Vol.10, No.1, 2000.

[16] 황선명, 염희균, "자바 카드 애플릿의 검증 방법", 한국정보처리학회 소프트웨어공학연구회지, Vol.5, No.1, 2002.