스마트카드를 이용한 효율적인 키보드 해킹 방지 및 인증 시스템 구현

*황선태, 박종선
대전대학교 정보통신공학과
e-mail : *hwang@dju.ac.kr, jspark@ice.dju.ac.kr

Implementation of Efficient Keyboard-hacking prevention and Authentication Systems using a Smart Card

Suntae Hwang, Jong-Sun Park
Dept. of Information & Communications Engineering, Daejeon University

Abstract

In this paper, we describe the effective way of keyboard-hacking prevention and authentication system using a Smart Card. These days the securing information matters for pc-users are becoming more important as the internet business grows rapidly, and the ubiquitous computing environment is open for everyone. Therefore, PC authentication is necessary to handle the access control to the target PC. Also, the keyboard-inputting information is necessary to be protected properly against the malicious attack.

In this paper, we propose the keyboard-hacking protect systems and authentication system using a Smart Card, and show the conveniency and efficiency in the results.

I. 서론

인터넷의 활성화에 따라 스마트카드의 사용이 전세계적으로 급증하고 있으며, 이와 관련한 기술 개발이 활발히 이루어지고 있다. 개인용 컴퓨터나, 금융망, 행정망 및 의료망, 전자상거래 등에서 스마트카드의 사용이 필수적으로 대두되고 있다[8].

본 논문의 가장 큰 목적은 스마트카드를 사용하여 최근 개인정보 노출의 큰 문제점으로 대두된 키보드 해킹으로부터 PC사용자의 정보를 보호하고, PC인증을 통한 제삼자의 PC사용을 막기 위한 시스템을 자바카드 플랫폼 상에 구현하는데 있다. 또한 유비쿼터스(ubiquitous) 컴퓨팅환경에 쉽게 이용가능한 시스템을 제안 한다.

키보드 해킹은 키보드를 통해 PC로 입력되는 모든 정보 즉, ID, 패스워드, 신용카드번호 등을 키보드 버퍼로부터 빼 내가는 것을 말한다. 이러한 경우 PC사용자의 정보는 해커로부터 완전히 노출된 상태이며, PC사용자는 이것을 보호할 방법이 없다. 따라서 본 논문에서는 키보드로부터 입력되는 모든 정보를 자바카드 플랫폼 상에서 암호화함으로써, 해킹으로부터 정보를 보호하고 접근 권한을 가진 PC소유자만이 PC를 사용할 수 있는 PC인증 시스템을 구현한다.

서론에 이어 2장에서는 스마트카드의 특징과 자바카드에 대해 설명하고, 3장에서는 본 논문에서 구현한 시스템에 대한 기능을 설명하며, 4장에서 결론을 맺는다.

II. 스마트카드의 특징

2.1 스마트카드의 H/W 구조

스마트카드 H/W 구조는 그림 1과 같으며, 5개의 활성화된 접점이 존재한다. CLK는 단말기로부터 제공되는 Clock 신호이고, RST는 Reset 신호이며, Vcc와 GND는 각각 공급되는 전압과 접지를 나타내고, I/O는 데이터 입출력이다. 스마트카드 H/W를 구성하는 주요 요소로는 CPU와 기억장치인 16Kbytes의 ROM, 16Kbytes의 EEPROM, 1Kbytes 미만의 RAM, 그리고 그 외 Logic 회로들과 Charge Pump 등이 있다[7].

*종신회원 : 대전대학교 정보통신공학과 교수

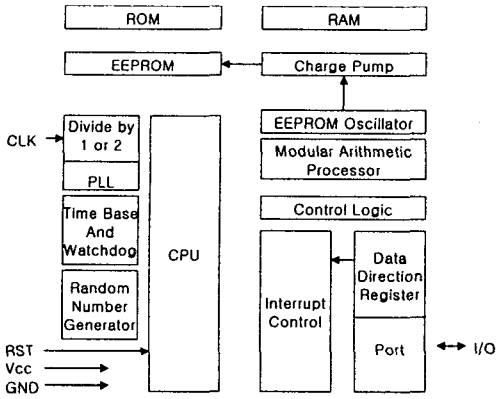


그림 1. 스마트카드 H/W 구조

2.2 스마트카드 명령어 구조

스마트카드 운영체제는 명령어와 응답 메시지를 사용하여 단말기와 스마트카드 사이에 통신을 한다. 스마트카드와 단말기 사이에 송신되는 명령어와 응답 메시지는 APDU(Application Protocol Data Unit)의 구조를 따르고, 그림 2와 같다[4, 9].

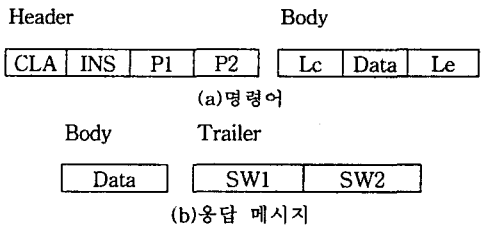


그림 2. 명령어와 응답메시지 구조

CLA는 1byte이고, Class byte이다. INS는 1byte이고, 명령어 구분코드이다. P1, P2는 1byte씩 이고, 명령어에서 사용되는 변수 1과 변수 2이다. Lc는 1byte 또는 3byte이고, 송신 데이터 바이트 수를 나타낸다. Le는 3byte이하이고, 수신 데이터 바이트 수를 나타낸다. Data는 송/수신 데이터를 나타낸다. SW1, SW2는 1byte이고, 응답 메시지에서 사용하는 상황 표시 1, 상황 표시 2를 나타낸다[9].

2.3 자바카드

자바카드란 스마트카드 기술을 기반으로 하여 자바의 기술을 접목시킨 것으로 그림 3과 같이 COS(Card Operating System)위에 JCVM(Java Card Virtual Machine)이 Wrapping되어 있는 구조의 IC카드를 말한다[5, 8].

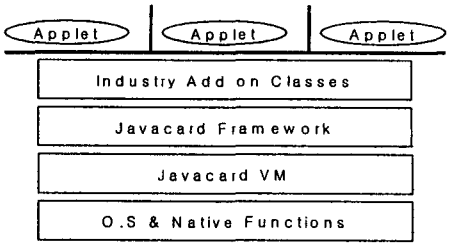


그림 3. 자바카드 구조

자바카드 Applet은 자바카드 상에서 실행될 수 있는 자바 프로그램이다. Applet과 호스트간의 통신은 그림 4에서 나타낸 바와 같이 명령, 응답 APDU의 교환을 통해서 이루어진다. Applet과 CAD(Card Access Device)또는 호스트간의 직접적인 통신은 불가능하며, JCRE(Java Card Runtime Environment)를 통한 통신만이 가능하다[8].

그림 4. Applet과 호스트 응용프로그램간의 통신

III. 시스템 구현

3.1 시스템 구현

본 장에서는 구현할 시스템에 대한 기능에 대하여 기술한다. 시스템 구현은 크게 다음과 같은 3부분으로 구분할 수 있다.

첫째, 데이터 암복호화 과정
둘째, PC사용자 인증 과정
셋째, Windows Control 과정

3.2 개발환경 및 시스템 흐름도

시스템 구현을 위한 개발 환경은 표 1과 같고, 시스템 흐름도는 그림 5와 같다.

표 1. 시스템 개발환경

운영체제	Windows 2000 Advance Server	
하드웨어	CPU	Pentium IV 1.7 MHz
	RAM	256 MB
개발도구	JDK 1.3	
	JCOP Tools 2.2(IBM), VC++	
	JCOP 21id Card(자바카드)	
	CHIPDRIVE micro 100 v4.30(단말기)	

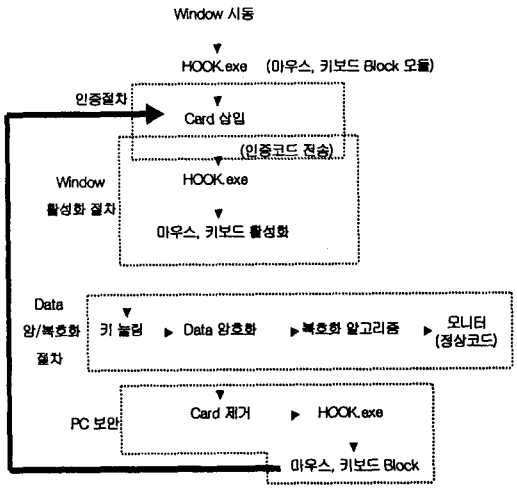


그림 5. 시스템 흐름도

그림 5에서 최초 윈도우가 구동되면 키보드와 마우스는 Block상태에 있기 때문에 PC를 사용할 수가 없다. 이 상태에서 카드를 삽입하면 카드내의 해쉬함수를 통한 인증코드가 전송이 되고, PC에서는 수신된 인증코드에 대한 인증 작업을 수행한다. 인증이 확인되면 키보드와 마우스는 Active 상태로 되어 PC를 사용할 수가 있게 된다. 또한 인증이 확인됨과 동시에 카드에서는 암복호화 수행을 위해 공개키를 PC로 전송한다. 그 다음부터 키보드를 통해 발생되는 스캔코드를 카드 내에서 개인키로 암호화하고, PC에서는 전송받은 공개키를 이용해 복호화를 수행된다. 카드를 제거하면 다시 키보드와 마우스는 Block상태로 전환된다. 이러한 과정을 반복함으로써 본 시스템은 효율적인 PC인증과 데이터 암복호화를 수행하게 된다.

3.3 데이터 암복호화

데이터 암복호화의 주 목적은 키보드 해킹을 방지하기 위함이다. 이를 위해 키보드에서 입력되는 데이터가 키보드 버퍼에 저장되기 전 과정에 카드에서의 암호화 처리를 하게 된다. 암복호화 알고리즘은 공개키 암호기법 중 대표적인 RSA_PKCS#1을 기반으로 한다.

결과적으로, 데이터 암복호화 기능은 키보드에서 발생되는 스캔코드를 카드내의 암호화 알고리즘을 통해 개인키로써 암호화를 수행하고, 암호화된 데이터는 키보드버퍼에 입력되며, PC에서의 인터럽트처리에 의해 PC로 전송되어, 복호화 알고리즘을 통해 공개키로써 복호화가 이루어져 화면에 정상적인 데이터로 보이게 된다.

3.4 PC사용자 인증

PC사용자 인증은 접근 권한을 가진 사용자만이 사용 권한을 받기 위한 절차이다. PIN(Personal Identification Number)코드로 사용될 카드의 Unique한 Serial number를 SHA 해쉬함수를 통해 해쉬코드로 바꾸어 PC로 전송하면, 안전성확보를 위해 해쉬코드로 사전에 PC에 저장되어 있는 PIN코드에 대한 해쉬코드와 비교 검증함으로써 정당한 사용자임을 확인하게 된다[6]. 불법접근에 대한 로그파일을 생성하여 차후 불법접근 확인 정보로도 이용할 수 있다.

3.5 Windows Control

Windows Control은 PC사용자의 PC사용에 대한 유연성을 갖고 제삼자로 하여금 PC접근 권한을 방지하기 위한 것이다.

최초 Windows가 구동되면 카드의 삽입과 PIN코드에 대한 인증 없이는 키보드와 마우스가 Block상태에 있어 PC를 사용할 수가 없으며, 카드의 삽입과 동시에 PIN코드 인증이 확인되면 키보드와 마우스의 동작이 가능케 되어 PC사용이 가능하다. 이러한 기능은 키보드 후킹 처리를 통해 컨트롤 된다. PC사용자가 작업 중 자리 이탈 시 카드를 제거하게 되면, 키보드와 마우스는 다시 Block상태로 전환된다.

본 시스템의 장점 중 하나는 작업 중 카드 제거 시 키보드와 마우스의 동작만을 Block시킴으로써, PC의 종료 혹은 재부팅 없이 카드 재 삽입을 통해PC작업을 계속할 수 있는 유연성을 갖고 있다.

3.6 시스템 시뮬레이션 결과 및 분석

구현된 시스템은 결과로써 데이터 암복호화와 PC인증 수행에 대한 검증이 확인 되었다. 그림 6은 PC인증 수행에 대한 결과이다. 카드를 삽입과 동시에 PIN코드에 대한 해쉬코드가 전송이 된 후, PC에서 PIN코드에 대한 정당성이 검증되어 PC사용이 가능하게 된 결과를 나타낸다.

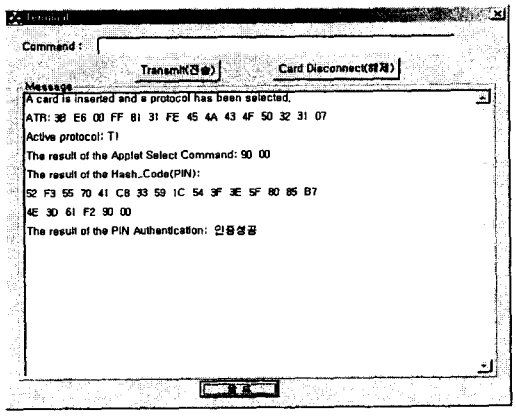
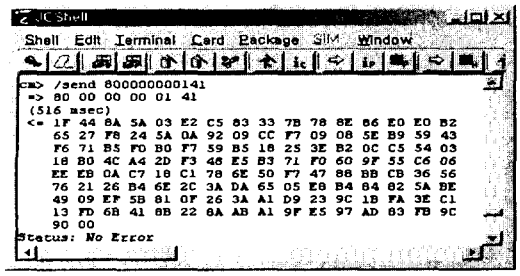
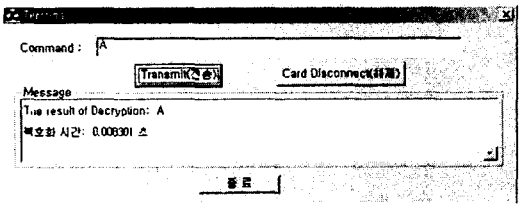


그림 6. PC인증 결과

그림 7은 키보드를 통해 입력된 스캔코드를 카드에서 개인키를 통한 암호화 수행 결과에 따른 128byte 암호화 코드와 PC상에서 공개키를 통해 복호화 한 결과를 나타내며, 암복호화에 따른 시간을 나타낸다.



(a)암호화 데이터와 암호화 시간



(b)복호화 데이터와 복호화 시간

그림 7. 데이터 암복호화 결과

Ⅳ. 결론

본 논문에서는 스마트카드를 이용한 효율적인 키보드 해킹 방지 및 인증 시스템을 자바카드 플랫폼 상에 구현하였다. 특히 키보드 해킹 방지를 위한 시스템 구현을 주안점으로 두었으며, 유비쿼터스(ubiquitous) 컴퓨팅환경에 쉽게 이용 가능한 이점을 제시하였다.

PC인증을 위해 SHA 해쉬함수를 사용하여 보다 정당성 있는 인증을 수행 할 수 있었고, 키보드에서 발생되는 스캔코드에 대해 바로 암호화를 수행하여 키보드 버퍼로 전송함으로써 키보드 해킹을 방지하게 되었다. 키보드와 마우스의 동작만을 Block시킴으로써 PC의 종료 혹은 재부팅 없이 카드 재 삽입을 통한 PC작업에 대한 유연성과 암복호화 시간에 따른 키보드 타이핑 딜레이에 영향을 받지 않음을 확인하였다. 또한 암복호화 기법에 있어서 공개키 암호화 기법인 RSA를 사용함으로써 여러 다른 응용분야로의 활용가능성을 기대할 수 있다.

참 고 문 헌

[1] ISO/IEC 7816-1, *Identification cards-Integrated circuit(s) cards with contact-Part 1: Phyical haracteristics*, 1998.

[2] ISO/IEC 7816-2, *Identification cards-Integrated circuit(s) cards with contact-Part 2: Dimensions and location of the contacts*, 1999.

[3] ISO/IEC 7816-3, *Identification cards-Integrated circuit(s) cards with contact-Part 3: Electronic signals and transmission protocols*, 1997.

[4] ISO/IEC 7816-4, *Identification cards-Integrated circuit(s) cards with contact-Part 4: Interindustry commands for interchange*, 1995.

[5] "Java CardTM 2.1.2 Development Kit User's Guide", Sun MicroSystem, Inc. 2001.

[6] "Java CardTM 2.2 Application Programming Interface", Sun MicroSystem, Inc. 2002

[7] 황선태, 이형, "스마트카드 모델의 기준에 관한 연구",한국 전자거래 학회 연구논문, 제4권 2-3호, pp197-212, 1999.

[8] 김성준, 이주영, "이재광 자바카드 기반 RSA 알고리즘 구현", 한국정보처리학회 추계 학술발표논문집 Vol.8, No.2, pp839-842.

[9] 김증섭, 조병호, 김효철, 이종국, 유기영, "다양한 응용을 위한 스마트카드 운영체제", 정보 과학회지 논문지 제8권 제3호.