스마트카드의 보안 기능 및 사용자 보안 모듈의 요구사항에 관한 연구

김수진*, 안기범*, 문종철**, 윤혁중**, 원동호*,

*성균관대학교, 정보통신공학부 정보통신보호연구실

Analysis of Security Function of Smart Card & Requirement of Security Module

Soo-jin Kim*, Gi-bum Ahn*, Jong-chul Moon**, Hyeg-jung Yun**, Dong-ho Won*,

*Department of Information & Communications Engineering Sungkyunkwan Univ.

** National Security Research Institute

요 약

스마트카드는 휴대하기에 간편하고 사용하기에 편리하다는 장점으로 인해 세계 각국에서 전자상거래를 비롯한 다양한 분야에서 그 이용범위가 급속히 확대되고 있다. 현재 사용되고 있는 스마트카드가 자체적으로 어느 정도의 보안과 인증기능을 갖추고 있기는 하지만 아직까지 사용자 보안 모듈로서의 기능은 미비한 실정이다. 본 논문에서는 스마트카드가 가지고 있는 자체적 보안 특징과 기능적 보안 특징을 분석한 후, 이를 이용하여 스마트카드가 사용자 보안 모듈로 사용되기 위해 필요한 요구사항을 제안하고자 한다.

Ⅰ. 서론

인터넷이 발전함에 따라 이를 이용한 인터넷 쇼핑몰 등의 전자상거래 또한 증가하고 있다. 이러한 전자상거래는 일반적인 상거래와는 달리 인터넷이라는 가상공간 내에서 행해지므로 사용자로 하여금 공간과 시간상의 제약을 받지 않아도 되는 편리성을 제공하지만, 판매자에게는 서비스나 상품에 대한 대가를 보장해야 하며 구매자에게는 안전한 지불 수단이 확보되어야 한다. 그러나, 현재 가장 많이 사용되고 있는 신용카드의 경우에는 지불 기능에만 국한이 되어 있기 때문에 모든 정보들이 공개되어 있는 개방형 네트워크에서 그대로 사용할 경우 위·변조의 위험이 따른다. 따라서 정보에 대한 암호화와 전자서명을 수행하여 위·변조 및 해킹을 방지할 수 있는 매체로서 스마트카드가 등장하게 되었다.

스마트카드란 마이크로 프로세서, 운영체제, 보안 모듈, 메모리 등을 갖추고, 특정 트랜잭션 처리능력의 집적회로 칩을 내장한 신용카드 크기의 플라스틱 카드이다. 스마트카드의 활용분야가 금융, 건강, 신분증, 통신, 보험, 로열티 분야 등으로 확장되면서 유선 인터넷 환경과 더불어 언제 어디서나 접속 가능한 무선 인터넷 환경으로까지 확대되고 있다. 이에 따라 스마트카드의 사용이 증가하고 있으나 스마트카드 내에 저장되는 개인의 신분증명서와 비밀키, 인증서 등의 보안 관련 문제에 대한 해결책은 아직까지 미비한 실정이다. 그러므로 이를 보완하기 위하여 스마트카드에 암호화 기능을 수행할 수 있는 보안모듈을 적용한다. 이는 사용자의 비밀키 관련 정보나 개인 아이디 등이 탑재되는 하드웨어 토큰을 의미하며, 단순히 메모리 기능만을 수행하는 것과 연산 능력이 있는 프로세서를 포함하는 것으로 나누어진다. 최근에는 보안 모듈 내에 암호 알고리즘의 연산을 수행할 수 있는 프로세스가 포함되어 무선 인터넷 환경에서도 공개키 연산의 수행이 가능하게 되었다. 그러나, 스마트 카드의 경우 카드 내에 칩의 용량과 카드 간의 호환문제 등으로 인하여 보안모듈로서 쓰이기보다 저장장치로 쓰이는 경우가 많다.

본 논문에서는 무선인터넷환경에서 스마트카드가 실질적인 보안모듈로서 사용되기 위해 필요한 요구사항을 제안한다. 본 논문의 구성은 다음과 같다. 2장에서는 스마트카드의 보안에 대해 간단히 소개하고, 3장에서는 보안 모듈로 사용되기 위해 필요한 요구사항들을 제안한다. 마지막으로 4

장에서는 결론과 향후 연구 방안에 대해 제시한다.

Ⅱ. 스마트 카드의 보안 기능

1. 스마트카드의 자체적 보안 기능

1) 가시적 보안 특징

스마트카드의 오용을 방지하기 위해서는 무엇보다도 일차적으로 육안으로 식별이 가능해야 한다. 그래서 스마트카드 내부에는 눈으로 식별 가능한 보안 식별자가 내장되어 있다. 이러한 보안 식별자는 눈으로는 식별 가능 하지만 내부에 저장되어 있는 데이터를 보호하지는 못한다.

[표 1] 가시적 보안의 종류

종류	설명
사진부착 (Photo lamination)	카드소지자의 사진을 카드에 부착함으로써 카드소지자의 신분 확인 가능
서명띠 (Signature strip)	제조시 카드에 부착되어 카드소지자가 이곳에 서명
홀로그램 (Holograms)	제조시 카드에 본딩되는 것으로 복제가 어렵고 이것을 떼내려 하면 기판이 손상됨
초미세 인쇄 (Microprinting)	하나의 선으로 보이지만 내용을 담고 있고 인쇄 자체가 복사하기 어려움
양각 (Embossing)	카드에 가압 성형되어 글자가 튀어 나오게 하는 것으로 홀로그램과 같이 사용하면 보안성을 높일 수 있음
보안패턴 (Guilloche)	아주 미세한, 새끼처럼 꼬인 모양의 선들을 카드 기판 위에 인쇄하는 것
레이저 그라비아 인쇄 (Laser gravure)	레이저를 이용하여 카드 기판 위에 이미지를 태우는 것으로 인쇄하는 것이 가능

[표 1]은 이러한 보안 식별자의 종류를 정리한 것이다.

2) 카드 운영체제의 보안 특징

스마트카드의 운영체제는 크게 전용 OS를 가지는 방식과 다양한 어플리케이션과 API를 추가할 수 있는 개방형 플랫폼을 가지는 방식으로 나뉘어 진다. 전용 OS는 고유의 파일 구조를 가진 각각의 어플리케이션으로, 카드 내의 동일한 수행코드를 공유한다. 그러나 전용 OS는 어플리케이션 간의 분리가 되지 않기 때문에 모든 어플리케이션이 하나의 단일 수행 프로그램을 공유하게 되며, 따라서 이로 인한 보안 문제가 발생하게 된다. 이러한 보안상의 문제점은 칩 상에서 EEPROM의 전용 파일(Dedicated File)을 논리적인 위치에 설계하거나 다양한 어플리케이션을 추가할 수 있는 개방형 플랫폼을 사용함으로써 해결할 수 있다.

또한 스마트 카드 내에 개인식별번호(PIN)나 암호화키를 저장함으로써 정보를 보호할 수도 있다. 예를 들어, 개인식별정보를 사용하는 경우, 사용자가 스마트 카드 내에 정해진 횟수를 초과하여 잘못된 개인식별정보를 입력하게 되면, 자동적으로 스마트 카드가 비활성화되어 접근이 금지됨으로써 정보를 보호한다. 암호화키를 사용하는 경우에는 암호화키로 데이터를 암호화시킴으로써 디렉토리 내의 정보를 보호한다.

3) 네트워크상의 보안 특징

지금의 카드 단말기는 컴퓨터들 사이의 통신 링크들로 이루어진 더 크고 복잡한 네트워크를 가지고 있기 때문에 네트워크상에서 보안문제를 고려해야만 한다. 네트워크상의 접속 예로는 카드와 판독기를 들 수 있는데, 예를 들어 스마트 카드가 판독기와 동작하여 데이터가 흐르는 경우 악의적인 카드 판독기에 의해 정보가 세어나가게 된다. 이와 같은 부정 조작을 보완하기 위한 방법으로는 트랜스포트 프로토콜을 설계하는 방법이 있다. 이외에도 네트워크 로그온을 하는 경우에는 인트라넷(Intranet)과 엑스트라넷(Extranet)의 인증을 하여 정보를 주고받음으로써 네트워크상의 보안문제를 해결할 수 있으며, 암호화키를 가지고 있는 경우에는 데이터를 암호화함으로써 외부의 공격으로부터 방어를 할 수 있다.

2. 스마트카드의 기능적 보안

카드와 카드 단말기사이의 문제뿐만 아니라 네트워크상에서 데이터를 안전하게 송수신하기 위해서는 소지하고 있는 키로 데이터를 암호화하여 네트워크를 통해서 암호화된 데이터를 보낸다. 수신측에서는 암호화된 데이터를 받아 암호화키와 쌍을 이루는 키로 데이터를 복호화해서 확인함으로써 데이터 보호할 수 있다. 이러한 과정을 통해서데이터의 기밀성, 무결성, 인증, 부인방지, 검증을 제공하게된다. 또한 다양한 암호화 알고리즘을 사용함과 더불어 데이터를 암·복호화하는 기술적인 정책을 지원함으로써 스마트 카드의 효율적인 보안을 제공한다.

[표 2]는 스마트 카드가 지원하는 보안 기능을 간략히 정리한 것이다.

[표 2] 스마트 카드가 지원하는 보안 기능

기능	설명
기밀성 (Confidentiality)	비 인가된 사람이 데이터를 볼수 없도록 보장 - 메시지 암호화를 위한 키 저장 - 암호화키를 위한 랜덤 수 생성
무결성 (Integrity)	데이터가 불법적으로 수정되지 못하도록 보장 - MAC계산을 위한 키 보유 - 전자 서명으로 무결성 확인
인증 (Authentication)	상호 간에 서로 믿을 수 있는 개체임을 보장 - PKI기반의 인증서 보유 - 전자 서명을 위한 비밀키 저장
부인방지 (Non-repudiation)	송신 부인 방지를 위한 전자 서명 - 전자서명을 위한 비밀키 저장 - 전자 서명 값 계산
검증 (Verification)	스마트 카드의 정당한 소유 및 시스템 접근 권한 확인 - PIN 확인을 위한 코드 저장

Ⅲ. 사용자 보안모듈의 요구사항

본 장에서는 스마트카드가 사용자 보안 모듈로써 사용되기 위해 필요한 요구사항을 제시한다. 먼저, 보안 모듈의 요구 사항을 칩에 대한 기능적·물리적 요구 사항으로 나누어 설명하고, 물리적 보안에서 보안 모듈에 대한 공격에 대한 해결책을 설명한다. 또한 사용자의 신원을 확인하기 위해 지원되어야 할 Two-factor 인증과 보안 모듈이 지원해야할 표준 알고리즘 및 호환성에 대해 기술한다.

1. 기능적 보안

보다 강화된 보안 특성을 만족하기 위해서는 칩 내부에서 암호 처리가 가능한 Co-processor의 필요성이 요구된다. Co-processor의 기능은 모듈 내부에 암호 알고리즘을 내장하여 이를 이용하여 데이터의 암호화와 모듈로부터 생성되는 메시지에 대한 인증을 수행하는 것이다. Co-processor의 메모리 접근 통제 측면에서 보면 모듈의 비밀번호, 즉 PIN을 알고 있는 정당한 모듈 소지자일지라도 보안 모듈내의 파일구조와 각 디렉토리·파일마다 서로 다르게 부여되어 있는 암호화된 코드(secret code)를 알 수 없기 때문에 사전에 한정된 범위 내에서 데이터를 조회할 수 있도록 한다. 암호기능 측면에서는 보안 모듈은 명령어 및 결과 값이 세션 키(session key)로 암호화되어 있기 때문에 결과 값을 중간에 가로챈다고 해도 그 내용을 해독하거나 재사용 할 수 없게 구현한다.

2. 물리적 보안

보안모듈이 RSA, 3DES등의 강력한 암호 알고리즘을 사용하고 있기 때문에 알고리즘 공격보다는 IC칩의 물리적 공격을 가해지는데 이를 보안하기 위해 다음과 같은 칩의 설계를 해야한다.

스마트 카드의 칩을 외부에서의 접근이 불가능하게 하도록 칩 공정에서 비가역적으로 전환을 시키거나 EEPROM 상의 위치를 임의적으로 수정하여 칩을 논리적으로 변경한다. 뿐만 아니라 내부 주소와 칩 상의 구성요소를 연결하는 주소 및 데이터 버스의 위치를 변경함으로써 접근과 노출을 방지한다. 또 다른 온칩(on chip) 보안 방법으로는 소자를 접근 불가능한 위치에 묻음으로써 분해공학에 의한 회로 노출을 방지하도록 설계하는 방법이 있다.

그 외에 메모리에 방출되는 전기적인 신호가 외부로부터 감지되는 것을 막기 위해서 EEPROM을 둘러싼 칩 영역을 금속 차폐물로 코팅하기도 한다. 이 차폐물을 제거하면 칩이 파괴되어 제 기능을 할 수 없게 된다. 또한 자외선이 칩 상의 메모리 내용을 지우는 것을 방지하기 위한 보호막 코팅막을 쓰기도 한다.

3. Two factor 인증

Two-factor 인증은 서로 다른 두 개의 요소로 사용자의 신원을 확인하는 것이다. 즉, 사용자가 소지하고 있는 것과 알고 있는 것을 이용함으로써 소지 기반의 인증과 지식 기반의 인증을 수행한다. 보안 모듈을 가지고 있다는 사실과 패스워드 또는 PIN(Personal Identification Number)을 알고 있다는 사실을 함께 이용하여 보다 안전하게 인증이 이루어지는 것이다.

이는 패스워드 모니터링, 사용자의 인적 정보에 대한 추측, 인증 수행중의 main-in-the-middle attacks, 네트워크 모니터링 등의 단일 요소에 대한 공격으로부터 안전하다. 또한, Two-factor 인증과정을 성공적으로 거친 사용자는 그 후에 수행한 모든 일에 대해 책임을 져야하기 때문에 부인 방지 기능도 있다.

4. 표준 알고리즘의 지원

보안 모듈에 프라이버시(Privacy), 부인방지(Non- repudiation), 인증(Authentication), 무결성(Integrity) 검증(Verification) 등과 같은 보안 원칙을 구현하기 위해서는 표준 암호화 알고리즘을 사용해야 한다. 보안 모듈에서 사용하기 적합한 대칭키 암호 알고리즘으로는 DES, 3DES, AES, SEED, IDEA 등이 있다. 이 중, 높은 수준의 보안성을 제공하기 위해서는 3DES를 사용하는 것이 적합하다. 또한, 공개키 암호 알고리즘으로는 RSA, ECC(Elliptic Curve Cryptosystem) 등이 있다. RSA의 경우 1024bit 또는 2048bit 길이의 키를 사용하고, ECC의 경우 160bit 길이의 키를 사용하므로, 메모리 등의 하드웨어적 사양이 부족한 환경에서는 ECC를 사용하는 것이 적합하다. 그리고 해쉬 알고리즘은 MD5, SHA-1, HAS-160 등을 사용하는 것이 적합하다.

5. 호환성

보안 모듈을 무선 인터넷과 멀티 응용 환경에서 보다 효율적이고 안전하게 사용하기 위해 내부적으로 호환이 이루어져야 하는데 이러한 요구사항으로 프로토콜 호환과 전압공급 레벨 호환이 있다.

프로토콜 경우, T=0 프로토콜과 T=1 프로토콜이 존재하는데, T=0 프로토콜은 단순한 byte-by-byte 전송기술을 사용하며, 요구되는 메모리의 크기가 작다는 장점을 지니고 있다. 반면에 T=1 프로토콜은 블록 단위의 데이터 전송을 수행하는데, 이는 보안성이 요구되는 메시지 전송이나 복잡한 인터페이스 소자에 적합한 특성을 지니고 있다. 현재의 보안 모듈 칩 내부에서 각각의 프로토콜을 지원하게 설계되어 있으나, 보안 모듈로서 수행되기 위해서는 T=0 프로토콜과 T=1 프로토콜 두 가지 모두를 지원해야 한다.

전압 공급레벨의 경우, 스마트카드 내에서 일반적으로 3V의 동작 전압이 일반화되어 있으나, 5V만을 지원하는 시스템이 생기면서 3V 동작 전압의 보안 모듈을 5V 동작전압에서 운용하는 경우 칩에 심각한 손상이 가해진다. 따라서 3V와 5V의 동작전압의 호환이 되기 위해선 보안 모듈 안의 동작전압이 2.7V에서 5.5 V사이의 공급 전압을 수용할 수 있도록 요구되어야 한다.

Ⅳ. 결론

인터넷을 비롯한 네트워크의 발달과 무선 통신의 발전으로 인해 암호학적 비밀키나 인증서와 같은 사용자의 비밀정보를 저장하고, 암호학적 연산을 수행하는 사용자 보안 모듈에 대한 관심이 증가되고 있다.

그중 대표적인 사용자 보안 모듈인 스마트 카드는 휴대하기 간편하고 사용이 편리하므로 금융, 의료, 전자상거래, 접근통제, 신분확인 등의 다양한 분야에서 사용되고 있다. 그러나 현재 사용되고 있는 대부분의 스마트 카드는 저장 장치로만 활용되고 있을 뿐 사용자 보안 모듈로써의 기능을 충분히 수행하고 있지는 않은 실정이다.

따라서, 본 논문에서는 스마트 카드가 사용자의 비밀키 관련 정보나 개인 아이디 등을 안전하게 탑재하고 사용자 보안 모듈로써 활용되기 위해 필요한 요구사항을 제시하였다. 스마트 카드가 사용자 보안모듈로써 사용되기 위해 갖추어야 할 요구사항으로는 기능적 보안, 물리적 보안, Two factor 인증, 표준 알고리즘의 지원 및 호환성 제공 등이 있다.

참고문헌

[1] William stallings, Cryptography and Network Security: principles and Practice-second edition, Prentice Hall International, Inc

[2] 스마트 카드 Technology& Market Analysis , 한국전자통신연구원

[3] 조소영, 스마트카드를 이용한 사용자 인증, 정보보호21c, 2002. 5 , p75

[4] Yoshiaki Isobe, Yoichi Seto, 생체인식, 스마트 카드, 그리고 PKI(하) 개인인증 기술의 체계 연구, 정보보호21c, 2002. 5 , p53-p57

[5] Jprge Ferrar. et al., Smart Cards LA Case Study, IBM, 1998, www.redbooks.ibm.com

[6] 성균관대 정보통신보호연구실, 무선 PKI환경에서 보안 모듈의 활용방안

[7] ISO/IEC 7816, identification cards-Integrated circuit(s) cards with contacts, International Organization for Standardization(ISO)

[8] Alfred J.Menezes, Paul C. van Oorschot, Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press

[9] 이만영, 김지홍, 류재철, 송유진, 염흥열, 이임영, 전자상거래 보안 기술, 생능출판사, 1999

[10] Smartcard and memory card IC data briefing-Databook 7th Edition, STMicroelectronics, NOV.1999