情 報 保 護 學 會 誌
第 13 券 第 4 號, 2003. 8

IC카드의 안전성 관련 기능 및 공격기법

주 학 수*, 현 진 수*, 성 재 철*, 임 선 간*

요 약

인터넷과 전자상거래의 발전에 따라 전자적 수단으로 화폐 가치를 이전하는 수단이 마그네틱 카드에서 IC카드로 대체될 것으로 기대되고 있다. IC카드는 마그네틱 카드보다 많은 데이터를 저장할 수 있고, 물리적인 보안(Tamper-resistance)과 암호기법(Cryptographic Technique)을 통해 외부와의 통신을 업격히 통제 및 보호할 수 있는 장점이 있다. 본 고에서는 IC카드의 안전성에 대해 알아보기 위해 먼저 IC카드를 정의하고 분류한다. 그리고, IC카드의 안전성 관련기능으로 카드에서의 사용자 인증, 카드와 카드단말사이의 실체인증, 접근통제 및 데이터의 기밀성/무결성, 키관리에 대해 알아보고, IC카드와 관련된 공격모델 및 공격기법들을 조사하여 정리하고자 한다.

Ⅰ. 서 론

1974년 프랑스의 Roland Moreno가 IC카드에 대한 특허를 출원한 후, 세계 여러 나라에서는 마그네틱 카드보다 보안 및 저장공간이 더 좋은 IC카드 이용 및 개발을 진행하고 있다. 세계 각 국은 현재 다양한 환경에서의 호환성을 달성하기 위해 ISO/IEC, MULTOS, Global Platform 등 다양한 표준화 작업들을 진행하고 있으며, 전자상거래, 전자주민증, 공과금 납부, 병원 업무, 전자지갑 등 일상적인 생활의 다방면에서 IC카드를 안전한 도구로 사용하고 있다.

IC카드는 이미 10억 개 이상 사용되고 있으며, 현재 유럽 지역에 가장 많이 보급되어 있다. 독립적 시장 조사기관인 오붐 리서치(Ovum Research : www.ovum.com)는 2003년까지 매년 27억 개의 스마트카드가 발급될 것으로 예측하고 있으며, 또 다른 조사기관에서는 IC카드의 충전과 관련한 시장이 2005년까지 265억 달러 정도의 규모에 이를 것으로 보고 있다[1]. 컴팩과 휴렛패커드는 은행 신용카드처럼 읽을 수 있도록 IC카드 판독용 슬롯이 포함된 키보드를 연구 중에 있다고 밝혔다. 현재 Schlumberger, Gemplus 및 ORGA 등의 회사가 IC카드를 제작하고, 또 읽을 수 있는 하드웨어 장치를 만들고 있다.

그러나, IC카드가 갖는 물리적 안전성에 대한 위협 및 최근에 대두된 부채널 공격(Side Channel Attack)등으로 인해 IC카드에 저장된 비밀키에 대한 정보를 알아 낼 수 있는 다양한 공격기법들이 나타나고 있다. 이에 본 고에서는 IC카드를 정의하고 분류하며 IC카드 관련 안전성 관련기능 및 공격모델 및 공격기법들에 알아본다.

Ⅱ. IC카드의 기술개요

IC카드 혹은 스마트 카드(Smart Card)라는 용어는 그 적용 범위에 따라 다양하게 사용되고 있다. ISO 표준에서는 IC(Integrated Circuit)가 하나 이상 삽입되어 있는 카드의 총칭으로 IC카드란 용어를, 스마트 카드 포럼(Smart Card Forum)에서는 "Smart Card"란 용어를, 이밖에도 "Chip Card", "Microprocessor Card", "CPU Card" 등 연산기능을 강조하는 용어들이 사용되기도 하고, "Super Smart Card", "Crypto Card" 같은 용어가 쓰이기도 한다.

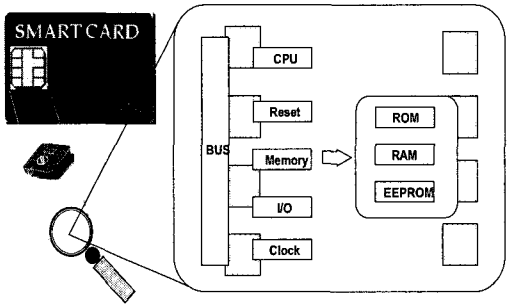
이외에, 메모리카드(Memory Card)'는 마이크로프로세서는 포함하지 않고 메모리만을 포함한 형태로서, 엄밀한 의미에서는 스마트 카드가 아니지만, 넓은 의미에서 포함시키기도 한다. 스마트 카드와

* 한국정보보호진흥원(KISA)({hsju,jshyun,sjames,seongan}@kisa.or.kr)

메모리 카드를 포함한 광의의 용어로서는 보통 '칩카드' 또는 'IC카드'를 사용하기 때문에 본 고에서는 용어를 IC카드로 통일하기로 한다.

2. IC카드의 구조

IC카드의 구조는 보통 그림 1과 같은 구조를 갖고 있다.



〔그림 1〕 IC카드의 전체적인 구조

- ROM(Read Only Memory) : 한 번 정보가 기록된 다음에는 영원히 앞으로 새로운 정보를 기록할 수 없는 기억 장치를 말함. 영구적인 방법에 의하여 정보를 기록하여 놓았기 때문에 전원공급이 중단되어도 기억 장소에 있는 내용이 사라지지 않는 특징이 있음. 이 메모리 안으로 COS(Card Operation System), 입력/출력, PIN 검증, 인증을 위한 기본 알고리즘과 같은 루틴이 들어감.
- RAM(Random Access Memory) : 임의접근 기억 장치로 데이터가 저장되어 있는 위치에 상관없이 같은 시간에 정보를 접근할 수 있는 기억 장치를 말함. 마이크로프로세서의 임시 저장용 기억장소(Scratch Pad)로 사용되며, RAM의 용량은 카드의 전반적인 수행속도에 많은 영향을 줌.
- EEPROM(Electrically Erasable and Programmable ROM) : 전기를 사용하여 기존에 저장되어 있던 내용을 지워버리고, 새로운 내용을 기록할 수 있는 ROM, EPROM과 달리, EEPROM은 메모리 셀이 전기적으로 지워질 수 있게 함으로써, 칩 카드에서 유용한 이점을 제공. 보통 어플리케이션 저장공간으로 사용됨.

3. IC카드의 분류

앞에서 언급한 것과 같이 IC카드는 프로세서 내장 형태에 따라 메모리카드와 스마트카드로 분류할 수 있으며, 외부인터페이스의 형태에 따라 〔표 1〕과 같이 분류할 수 있다.

〔표 1〕 외부인터페이스 형태에 따른 IC카드의 분류 및 특징

구분		정의	특성
접촉형 카드 (Contact Card)		• 수용하는 인터페이스 장치 (IFD: Interface Device)에 삽입되었을 때 카드의 접점이 IFD의 접점에 접촉됨으로써 카드가 활성화되는 형태의 카드	• 접점의 잦은 접촉으로 인하여 전기적 충격이나 손상이 있을 우려가 있음 • 고도의 보안을 요하며, 카드 내의 특정 암호화 알고리즘을 수행할 필요가 있는 분야에서 주로 사용
비접촉형 카드 (Contactless Card)		• 비접촉식 카드는 카드 판독기와 물리적으로 접촉하지 않는 것으로, 카드를 판독기 내에 삽입하는 대신 일정 거리 떨어져서 작동되는 카드	• 외부와의 직접적인 접촉이 없음으로 인하여 외부환경에 강하며, 접점에 유기되는 정전기에 의해 카드 내 칩이 파손될 확률이 작은 장점을 가짐 • 카드의 제조비용과 이를 수용하는 IFD가 접촉식보다 1.5~2.5배 정도 비싸 비용적인 측면에서 단점을 가짐
혼합카드	콤비카드 (Combi Card)	• 접촉식 카드와 비접촉식 카드의 형태를 모두 지원 • 접촉식 및 비접촉식 두 인터페이스가 연결되어 있으며, 마이크로프로세서나 로직 모듈을 통해 하나의 공유 데이터 영역을 액세스	• 내부 자원공유를 통한 이질적 어플리케이션(예:칩운영체제, 동일 키나 패스워드)의 통합 효과를 가져올 수 있음 • 공유되는 메모리 영역이 훼손당할 경우, 접촉/비접촉식 카드 기능이 모두 마비되는 경우가 존재할 수 있음
	하이브리드카드 (Hybrid Card)	• 접촉식 카드와 비접촉식 카드의 형태를 모두 지원 • 하나의 카드 내에 물리적으로 접촉식 카드와 비접촉식 카드가 독립된 형태로 존재	• 두 칩 사이에는 물리적인 연결이 없어서 메모리의 공유가 불가능 • 하드웨어 자원과 소프트웨어 자원 활용에 있어 비효율적이며, 제조단가 또한 다소 높음

4. IC카드의 응용분야

초기 IC카드는 금융권의 전자화폐와 같은 한정된 분야에 사용되었다. 그러나, 인터넷 기술과 전자상거래가 빠르게 발달함에 따라, IC카드는 안전한 가치저장 수단뿐 아니라 신원인증, 교통/통신 등의 용도로 그 사용이 빠르게 확산되고 있다. 또한, 비접촉형카드, 콤비카드 등의 새로운 형태의 외부인터페이스가 지원됨에 따라 IC카드의 용도도 다양해지게 되었다.

현재의 IC카드는 한가지 기능만을 지원하는 것이 아니라, 다양한 기능을 복합적으로 지원하기 때문에, 단순하게 IC카드의 응용분야를 구분하는 것은 어려운 일이나 [표 2]와 같이 6개의 분야로 구분할 수 있다.

[표 2] IC카드의 응용분야

응용분야	특징
전자지불	• 가장 기본적인 IC카드의 기능 • 은행의 현금카드나 신용카드 또는 전자화폐의 가치저장
보안 및 인증	• 블록암호알고리즘, 공개키 암호알고리즘 구현 • 암호화, 접근통제, 신원인증 • 전자상거래를 위한 인증서 저장
교통	• 비접촉형 카드 • 버스, 지하철 등의 교통카드 기능
통신	• 무선전화를 이용한 무선결제 • USIM 칩에 사용
건강	• 건강정보와 같은 중요한 개인정보의 안전한 가치저장
지적재산권	• 라이선스 정보 저장 • 디지털 콘텐츠에 대한 소유권 정보 저장

Ⅲ. IC카드의 안전성 관련 기능 및 공격기법

1. IC카드에서의 인증

IC카드에서의 인증방법은 크게 IC카드에 접근하려는 사용자의 신분을 증명하는 사용자(카드소유자) 인증, 카드와 카드단말간의 인증방식인 실체인증으로 분류할 수 있다.

1.1 IC카드에서의 사용자 인증

사용자 인증 기법이란 IC카드(혹은 카드단말)에 접근하려는 사용자의 신분을 증명하는 기능이며 식별된 사용자가 정당한 주체인지를 인증하는 것을 의미한다. 사용자 인증기법은 NIST의 FIPS-190[1]에 따르면, 다음과 같이 3가지 형태로 분류할 수 있으며, 현재 제시되고 있는 방법들을 정리하면 [표 3]과 같다.

[표 3] 사용자 인증기법 분류

구분	정의	종류
알고 있는 것 (Something you know)	사용자가 알고있는 지식을 이용하여 사용자를 인증하는 방법	패스워드 및 PIN 기반 인증
소유하고 있는 것 (Something you have)	사용자가 소유하고 있는 물리적인 매체에 저장되어 있는 인증데이터를 이용하여 인증하는 방법.	토큰(IC카드, 마그네틱 카드, 시도 응답 생성 기 등)기반 인증
개체의 특징 (Something you are)	사람의 생체적인 특징(Biometics)을 인증데이터로 사용하여 인증하는 방법	생체(Biometrics)(지문, 망막 패턴, 음성, 등)기반 인증

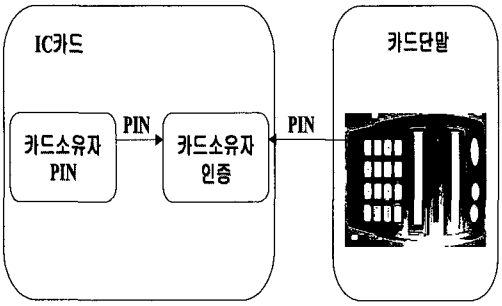
위에 제시된 방법들은 독립적 혹은 조합하여(다중인증) 사용되고 있다. 각각의 방법들이 모두 강력한 인증을 제공할 수 있는 반면, 각각의 방법들에 관련된 문제들 또한 존재한다. 컴퓨터 시스템 상에서 다른 사람으로 위장하길 원하는 사람은 다른 사람의 패스워드를 추측하거나, 알아낼 수 있으며 토큰을 훔치거나 위조할 수 있다. 또한 사용자는 패스워드를 잊어버리거나 토큰을 분실할 수 있고, 인증데이터와 토큰의 유지를 위한 관리상의 부담이 높다. 생체기반 인증 방식도 기술적 문제, 비용 등의 문제 등을 갖고 있다. 이 절에서는 IC카드에서의 사용자 인증방법에 대해 설명하고자 한다.

IC카드에서 사용자인증 방법으로 가장 많이 사용되는 방법은 PIN 혹은 패스워드를 이용하는 방법이다. PIN은 보통 4자리의 숫자(0~9)로 사용되는데, 그 이유는 현재 사용되는 카드 터미널에 숫자로 구성된 키패드(keypad)만이 장착되어 있으며 사용자들이 기억하기 쉽기 때문이다[17]. 보통 PIN이 터미널의 키패드 혹은 컴퓨터의 키보드를 통해 입력되면 그 정보는 카드로 보내어지게 되고 카드는 내부에 저장된 PIN정보와 비교해서 그 결과를 터미널에 알려주는 방식으로 사용자를 인증하게 된다.

보통 PIN의 입력 시, 공격자가 간섭(Tampering) 공격을 함으로써 PIN 정보를 알아낼 수 있기 때문에 PIN정보는 암호학적 보호기능을 갖춘 "PIN Pad[2]"에 의해 암호화되어 전송된다.

---

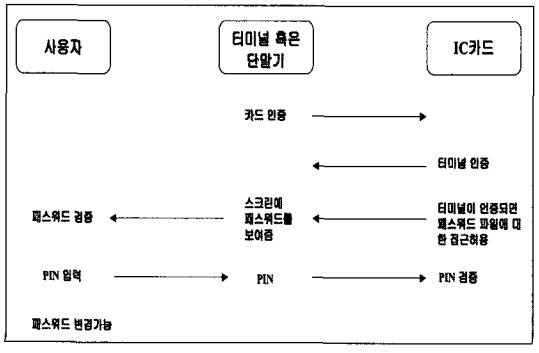
1) http://csrc.nist.gov/publications/fips/fips190/fip190.txt
2) EMV2000 표준에서는 PIN Pad를 Tamper-evident



〔그림 2〕 PIN을 이용한 사용자 인증

PIN을 이용한 방식은 터미널이 카드 소유자를 인증하는 방식으로 사용되지만, 카드소유자가 터미널을 인증하는 방법도 필요하다. 예를 들어, 공격자가 가짜 현금자동 지급기를 사용하는 경우를 생각해 보자. 공격자는 가짜 현금자동지급기를 사용하여 정당한 사용자들의 PIN정보를 모을 수 있다. 공격자가 사용자의 카드를 훔친 뒤, 모은 PIN정보를 이용하면 공격자는 정당한 사용자의 계좌로부터 돈을 인출할 수 있는 문제점이 발생한다. 이러한 문제점들은 카드소유자가 터미널을 인증하지 않기 때문에 발생한다. 이를 막기 위해 PIN방식과 함께, 사용자만이 아는 패스워드를 카드에 저장하는 방식이 결합되어 사용된다. IC카드 운영체제(OS)는 카드가 터미널을 인증한 후에만 터미널이 패스워드 파일을 읽을 수 있는 접근권한을 허락한다. 전체 방식은 〔그림 3〕처럼 구성된다.

사용자가 IC카드를 터미널(혹은 단말기)에 넣으면 카드와 터미널 사이의 상호인증이 가장 먼저 일어나고, 이 상호인증이 성공하면 카드는 터미널에게



〔그림 3〕 PIN과 패스워드를 이용한 사용자와 터미널의 상호인증

장치로 규정하고 있으며, PIN을 표준 ISO 9564-1에 따라 암호화하여 카드로 전송함

사용자의 비밀 패스워드 파일에 대한 읽기 권한을 허용한다. 터미널은 패스워드 파일을 스크린을 통해 사용자에게 보여주고 사용자는 자신의 패스워드가 맞는지를 검증함으로써, 터미널을 인증하게 된다. 이와 같은 과정이 성공하면, 사용자는 자신의 PIN 정보를 입력하여 사용자 인증과정을 수행한다.

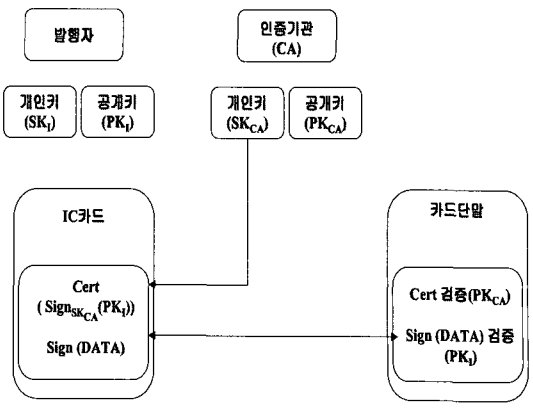
1.2 IC카드의 실체 인증

카드와 카드단말간의 인증(실체인증)방식으로는 공개키 암호알고리즘을 이용한 인증, 대칭형 암호 알고리즘을 이용한 인증 등이 있다.

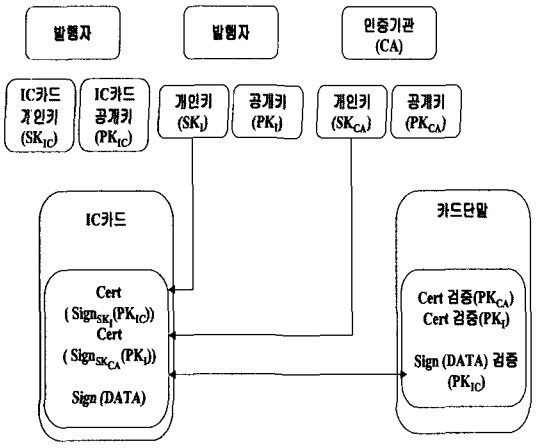
1.2.1 공개키 암호알고리즘을 이용한 인증

공개키 암호알고리즘을 이용한 인증방식은 인증기관(CA)으로부터 발급받는 공개키 인증서(Certificates)를 카드와 카드 단말에 설치하여 인증을 수행하는 방식으로 구성된다. 공개키 암호알고리즘을 이용하는 인증방식은 EMV 표준[10]에 따라, 정적(Static) 인증, 동적(Dynamic) 인증으로 분류할 수 있다.

정적인증 방식의 경우, 발급기관이 IC카드를 개인화(Personalization)할 때 카드에 전자서명 값이 카드번호, 사용자 이름, 주소 등과 같이 저장되게 된다. 카드가 단말기에 삽입된 후 발행자의 공개키에 대한 인증기관의 서명값과 데이터에 대한 발행자의 서명값이 단말기로 전송되면 단말기는 미리 분배되어 있는 CA와 발행자의 공개키를 사용하여 서명값들을 검증함으로써, 카드에 대한 인증을 하게되는 방식이다. 이 방식은 단지 저장된 값만을 이용하므로 IC 카드 내에서의 공개키 암호 연산이 필요없다는 장점이 있는 반면, 인증할 때마다 동일한 인



〔그림 4〕 IC카드의 정적(Static) 인증방식



〔그림 5〕 IC카드의 동적 인증 방식

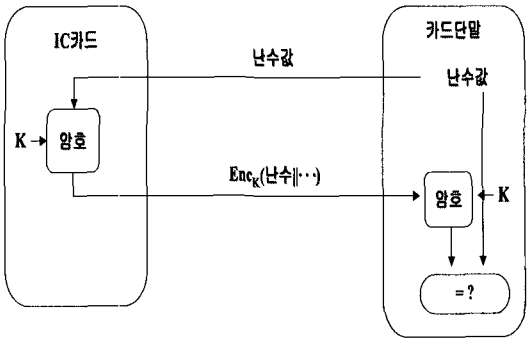
증 정보를 사용하여 replay attack에 취약한 단점이 있다.

동적 인증의 경우, 카드 자체의 공개키와 개인키를 갖고 있으며 거래 시 단말기가 생성한 난수값을 포함한 동적인 데이터가 단말기로부터 전송되는 것으로부터 시작된다. 카드는 이 동적인 데이터에 자신이 가지고 있는 개인키로 서명한 뒤 카드의 공개키에 대한 발행자의 서명값, 발행자에 대한 CA의 서명값을 단말기에 전송하면 단말기는 미리 분배되어 있는 공개키들로 서명들을 검증함으로써 카드에 대한 인증을 하게 된다. 이 방식은 카드에 암호(서명)연산을 수행할 수 있는 프로세서가 탑재되어 있어야 하며, 정적 인증과는 달리 매 인증마다 변하는 데이터를 사용하기 때문에 replay 공격에 안전하다는 장점이 있다.

현재는 IC카드의 메모리 크기, CPU의 조건, 성능 등 제약된 환경으로 정적인증만이 주로 사용되고 있으나, 향후 IC카드의 성능이 발달됨에 따라, 동적 인증방식이 주로 사용될 것으로 보인다.

1.2.2 대칭키 암호알고리즘을 이용한 인증

대칭형 암호알고리즘을 이용하는 인증방식은 단방향 인증과 상호 인증방식으로 분류할 수 있다. 단방향 인증의 경우, IC카드와 카드단말이 동일한 키를 갖고 있으며 단말기에서 난수를 생성하여 IC카드에 전송하면, IC카드는 난수값을 비밀키로 암호화(혹은 MAC)값을 계산하여 단말기에 전송한다. 단말기는 같은 비밀키로 암호화된 값을 복호화하여 난수값이 유효한지 검증함으로써 카드인증을 하는 방법이다.



〔그림 6〕 IC카드에서의 단방향 인증방식

상호 인증의 경우, 단방향 인증을 두 번 행함으로써 카드가 카드 단말기를 인증하듯이 카드가 카드 단말기를 인증하는 방법이다. 카드 단말은 카드 번호로부터 카드의 세션키를 계산하여야 하기 때문에 카드번호 및 난수값을 카드에 요청하고 자신도 난수값을 생성한다. 카드로부터 받은 난수값과 자신이 생성한 난수값을 세션키로 암호화하여 결과 값을 카드에게 보내고, 카드는 카드단말로부터 받은 결과값을 복호화하여 단말기의 난수값을 알아낸다. 이 때 카드는 카드단말의 인증이 끝나게 되고, 카드는 카드단말의 난수값과 자신의 난수값을 암호화하여 보내면 카드단말은 카드로부터 받은 결과 값을 복호화하여 자신의 난수값과 확인함으로써 카드를 인증하게 된다.

2. IC카드에서의 접근통제 및 데이터 기밀성/무결성

2.1 접근통제

IC카드의 보안기능 중 가치저장장치의 안전한 수단으로써 IC카드가 가져야 할 핵심기능은 접근통제(Access Control) 기능이며, 데이터를 보호하기 위한 메커니즘들 중의 하나이다.

접근통제는 주체가 컴퓨터 자원을 가지고 사용, 변경, 열람하려고 할 경우 접근통제 메커니즘에 의해 정의된 접근규칙에 따라 접근을 허가 또는 금지하는 보안기능을 의미한다. 즉, 허가되지 않은 접근이 발생한 경우 불법적인 자원의 사용, 노출, 수정, 파괴와 불법적인 명령어의 사용으로부터, 객체를 보호하는 것을 의미한다.

접근통제 규칙은 조직의 보안정책에 따라 신분기반 정책, 규칙기반 정책, 그리고 직무기반 정책으로 구분된다.

〔표 6〕 보안정책 분류

보안정책		설 명
신분기반정책	Individual-Based Policy	객체별로 접근통제 목록을 작성
	Group-Based Policy	그룹별로 접근통제 목록을 작성
규칙기반정책	Multi-Level Policy	기밀등급에 따라 분류된 환경에서 사용
	Compartment-based Policy	부서별로 구분된 접근허가 환경에서 사용
직무기반 정책		직무별로 접근통제 목록을 작성

IC카드에서 구현가능한 접근통제 모델로서 ISO/IEC 모델과 MPCOS-EMV 모델이 있다.

- ISO/IEC 7816-Part 9 : ISO 7816-Part 9 국제표준안에서는 객체별 접근통제 리스트(Access Control List) 모델을 이용하여 IC카드의 접근통제 모델을 제시한다. 객체별 접근통제 리스트는 객체를 접근할 수 있는 권한을 가진 주체들의 리스트를 유지하는 방법으로써, 접근행렬(Access Matrix)에서 각 열의 필드에 접근권한이 설정된 행의 주체들로 표현한다.
- MPCOS-EMV : MPCOS-EMV 카드는 파일 접근시 파일 보호를 위해 비밀 코드 또는 키들을 사용한다. 비밀코드는 요소파일에 저장되고 비밀코드 요소파일이라 불린다. 마스터파일과 각 전용파일은 하나의 비밀코드 요소파일을 가지고 있다. 터미널은 IC카드의 요소파일 내에 저장된 데이터에 접근하려 할 때, 카드는 요소파일 접근조건에 저장된 값과 인증 레지스터에 저장된 값을 비교한다.

2.2 데이터의 기밀성/무결성

기밀성(Confidentiality)/무결성(Integrity)은 데이터를 보호하기 위한 기능 뿐 아니라 앞에서 설명한 인증, 접근통제 등 다양한 기능에 필요한 기능이다.

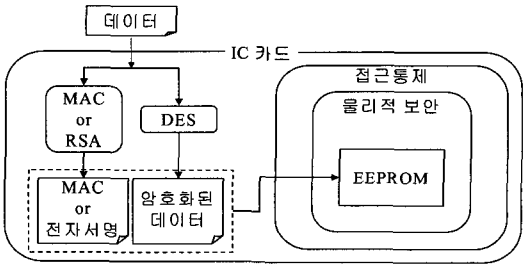
- 기밀성 : 기밀성이란, 정당한 권한이 부여된 사용자만이 데이터의 내용을 파악할 수 있게 하는 것으로서, DES, 3-DES 등의 블록암호알고리즘이 사용된다.
- 무결성 : 데이터가 불법적으로 위조 또는 변조되었는지를 검출하는 것으로, IC카드의 메모리에 저장된 가치(예, 교통카드의 잔액, 전자화폐)를 소유자가 임의로 변경할 수 없어야 한다. 무결성 기능을 위하여 메시지 인증 코드(Message Authentication Code)나 해쉬알고리즘 또는 전자서명이 사용된다.

IC카드에서 보호해야할 데이터는 메모리에 저장되어있는 저장 데이터와 단말기와의 통신에 사용되는 전송 데이터로 구분지을 수 있다. 각각의 데이터에서 기밀성/무결성 기능은 다음과 같이 사용된다.

2.2.1 저장 데이터

IC카드 내의 저장 데이터를 DES와 같은 블록암호알고리즘을 이용하여 암호화한 암호문을 데이터의 위·변조 여부를 확인하기 위해 데이터의 MAC 또는 전자서명과 같이 안전한 메모리에 저장한다.

IC카드에서는 기본적으로 하드웨어적으로 안전한 메모리에 데이터가 저장되기 때문에 저장 데이터에 대한 기밀성보다는 무결성에 초점이 맞추어져 있다. 그래서, 저장되는 데이터를 암호화하지 않고 데이터의 MAC과 함께 메모리에 저장하는 방식을 사용하기도 한다.



〔그림 7〕 저장 데이터의 인증

2.2.2 전송 데이터

IC카드의 전송데이터의 기밀성과 무결성 기능은 "Secure Messaging"기능이라고도 하며, 통신사에서 가해질 수 있는 각종 위협에 대한 방어수단이라고 생각할 수 있다.[3] IC카드와 터미널 사이의 데이터 전송은 IC카드의 I/O 접속단자를 통해 이루어진다. 그러나, 전송 중에 있는 데이터가 그대로 전송된다면, 공격자가 전송되는 데이터를 도청 또는 위·변조하는 것이 가능하고, 수신자는 이러한 사실을 알지 못할 것이다. 그러기 때문에, 안전한 전송을 위해서 전송되는 데이터의 일부 또는 전체에 대한 인증, 필요하다면 기밀성이 보장되어야 한다.

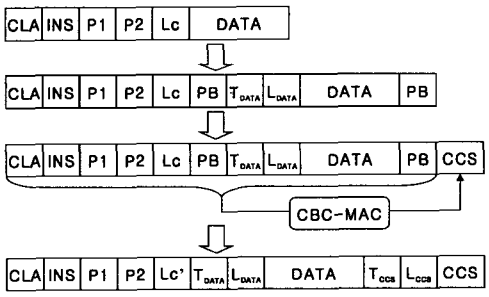
안전한 전송 프로토콜을 시작하기 전에 우선 IC 카드와 단말기 사이에 키 공유가 이루어져야 한다. 키 공유방법으로는 RSA, DH, ECDH 방식들이 사용되는데, 본 절에서는 구체적으로 언급하지 않고, IC카드와 단말기 사이에 키 공유가 이루어졌다고 가정하도록 하자.

데이터의 전송방법에 대하여는 ISO/IEC 7816-4에서 정의하고 있으며, 추가적인 기능은 ISO/IEC 7816-8에서 정의하고 있다.

가) 인증모드

인증모드는 초기 APDU(Application Protocol Data Unit)[3] 형식의 데이터에 인증을 위한 암호적 체크섬(CCS, Cryptographic Check Sum)을 추가하는 기본적인 전송 방법이다. 전송데이터는 평문상태 전송되기 때문에 위·변조를 막을 수는 있으나, 도청에 대하여는 취약하다.

단계 1 : 전송 데이터에 APDU 형식의 헤더 부분을 추가함
단계 2 : 데이터를 TLV[4] 코드화 데이터 형식으로 변환한 후, 8바이트의 정수배가 되도록 패딩함
단계 3 : DES를 이용한 CBC-MAC으로서 8바이트 CCS를 계산함
단계 4 : CCS 계산을 위해 사용한 패딩 바이트(PB : Padding Byte)를 제거한, 최종 전송 데이터



〔그림 8〕 전송 데이터 - 인증모드

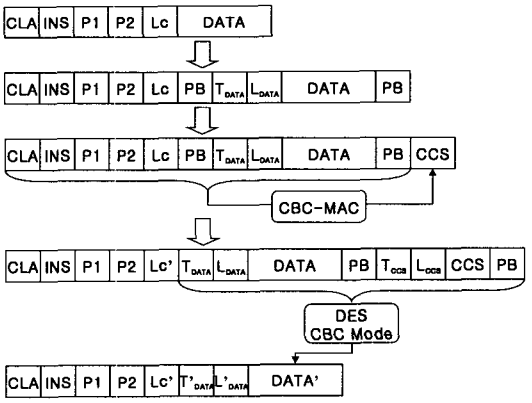
3) APDU란 Application protocol data unit의 약어로, OSI 모델 level 7인 어플리케이션 계층에서 사용되는 국제표준 데이터 유닛을 말함

4) TLV란 ASN.1에 따른 데이터 포맷으로 특정 데이터 객체(Object)를 표현해주기 위해 태그(tag)와 코드를 사용.

나) 결합모드

인증모드에 비하여 결합모드는 더 높은 수준의 보안 전송방법으로, 전송 데이터는 암호화하여 전송된다. 인증모드를 보완한 방법으로 CCS 뿐 아니라 암호화를 함으로 안전하게 전송할 수 있으나, 암호화/복호화 시간이 필요하기 때문에 효율성이 떨어진다는 단점이 있다.

단계 1 : 전송 데이터에 APDU 형식의 헤더 부분을 추가함
단계 2 : 데이터를 TLV 코드화 데이터 형식으로 변환한 후, 8바이트의 정수배가 되도록 PB(Padding Bytes)를 추가함
단계 3 : DES를 이용한 CBC-MAC으로서 8바이트 CCS를 계산함
단계 4 : 8바이트의 정수배가 되도록 PB(Padding Bytes)를 추가하고, CBC 모드의 DES로 초기 APDU 형식의 헤더를 제외하고 암호화
단계 5 : CCS 계산과 암호화에 사용된 PB를 제거한 암호화된 최종 전송 데이터

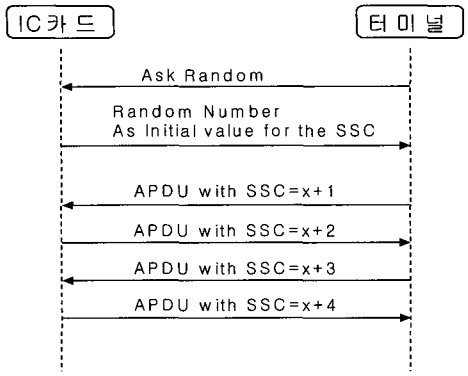


〔그림 9〕 전송 데이터 - 결합모드

다) 전송 수열 카운터 모드

전송 수열 카운터 모드는 전송되는 APDU에 전송시간과 관련된 수열을 추가하여 전송하는 방법이다. 전송 수열 카운터(SSC, Send Sequence Counter)만을 사용한 방법으로는 안전한 전송방법이 되지 못하기 때문에 반드시 인증모드 또는 결합모드와 같이 사용하여야만 한다.

SSC(Send Sequence Counter)를 전송 데이터에 추가하는 방법과 전송데이터와 XOR 연산을 하는 방법은 다음과 같다.

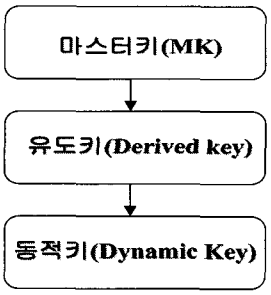


〔그림 10〕 전송 데이터 - 전송 수열 카운터 모드

3. IC카드에서의 키관리

IC카드에서의 키 관리란 IC카드의 보안기능을 이용할 때, 암호알고리즘에 사용되는 키들을 관리하기 위한 것으로, 키의 라이프 사이클 동안 키의 생성과 분배, 등록/취소 저장, 소멸 등의 전반적인 활동과 키 속성을 관리하는 기능을 말한다. 키관리의 요구사항은 대칭키와 공개키 알고리즘을 구현하는 모든 암호모듈에 의해 만족되는데, 대칭키와 개인키는 인가되지 않은 노출이나 수정으로부터 보호되어야 하며, 공개키는 인가되지 않은 수정과 치환에 대비하여 암호 모듈내에 보호되어야 한다.

IC카드 내부의 정보를 보호하기 위하여 사용되는 키는 마스터 키(Master Key), 유도키, 동적키(혹은 세션키(Session Key)라고도 함)로 분류될 수 있으며 다음과 같은 계층 구조를 갖는다.



〔그림 11〕 기본 키 계층 구조

○ 유도키(Derived Key) : 단말기와 달리 IC카드는 공격자가 가져가서 상당한 시간과 노력을 투자하여 다양한 공격들을 수행할 수 있다〔자세한 공격기법들은 4절을 참조〕. 따라서 카드가 마스터키를 가지고 있지 않다면, 인증되지 않은 접근으로부터의 영향을 최소화 할 수 있기 때문에 마스터키로부터 얻어진 유도키들만을 카드 내에 가지도록 한다[17]. 유도키는 암호 알고리즘에 의해 생성되어지며, 입력값은 마스터키와 카드의 식별정보를 사용하며 암호알고리즘으로는 보통 DES 혹은 3DES를 보통 사용한다.

유도키(derived key)=enc(master key; card number)

○ 동적키(Dynamic Key) : 일명 임시용 키(Temporary Key) 혹은 세션키로 언급되며, 안전한 데이터 전송을 위해 사용된다. 동적키(세션키)를 생성하기 위해서는 두 객체 중 한 객체가 먼저 특정 세션에 유일한 난수 값을 생성한 뒤 다른 객체에게 전달하는 과정으로 구성되는데, 대칭암호알고리즘을 사용하는 방식과 비대칭 암호알고리즘을 사용하는 방식으로 구분할 수 있다.

- 대칭 암호알고리즘 방식을 사용하여 동적키(세션키)를 교환하는 경우, 한 객체에 의해 난수가 생성되어 평문의 형태로 다른 객체에 전달된다. IC카드와 터미널은 유도키를 사용하여 난수값을 암호화하면 새로운 세션에 유일하게 사용될 동적키가 생성된다. 과정은 다음과 같다.

동적키(dynamic key)=enc(derived key; random number)

- 비대칭알고리즘 방식을 사용하여 동적키(세션키)를 교환하는 경우, 난수값으로부터 메시지 암호화에 사용될 동적키를 생성하고, 동적키의 교환을 RSA와 같은 비대칭암호알고리즘을 이용하여 상대방에게 전달하는 방식이다. 이 방식은 hybrid 방식으로 PGP 등과 같은 암호제품에서 많이 이용되고 있다.

동적키의 경우, 설정되는 매 세션마다 보안상의 안전성을 높이기 위하여 서로 다른 키를 사용해야 함에 따라, 사용기간이 비교적 짧고, 그 결과 상호간에 키를 갱신해야 하는 절차가 요구된다.

이 절에서는 유럽은행[7]의 키 관리 방법에 대한 가이드라인과 "스마트카드 핸드북[17]"을 참조하여 IC카드에서의 키 관리 시 유의점에 대해 정리하고자 한다.

- 키생성(Key Generation) : 마스터키, 키암호용키(KEK)[5]와 PIN 암호용 키는 최소 112비트(TDES) 정도의 안전도를 가져야 한다. 마스터키는 물리적 보호모듈(TRSM : Tamper Resistant Secure Module)안에서 생성되어야 하며 물리적 보호모듈를 벗어나는 경우, 평문의 형태로 존재해서는 안된다[7]. 암호시스템의 구현 시 부적절한 난수 혹은 의사난수를 사용함으로써, 시스템이 공격당할 수 있는 문제점들[15,12]이 있기 때문에 암호키를 생성하기 위해 사용되는 난수는 안전해야 한다.(안전한 난수, 의사난수 생성방법에 대해서는 [5]을 참조)
- 키백업 및 저장(Key Backup and Storage) : 마스터키가 물리적 보호장치를 벗어나서 백업될 때는 안전한 비밀분산기법(Secret Sharing Techniques)이 사용되어야 하며, 백업이 요구되지 않을 경우는 마스터키의 저장은 암호학적으로 안전한 하드웨어에 저장되어야 한다[7].
- 키의 사용 및 사용기간 제한: 파일 시스템을 사용하는 카드에서는 키들을 개인파일(Private File)에서 관리하는데, 키를 사용하기 위해 파일로 접근하는 것은 카드소유자의 신분을 증명하기 위해 입력된 PIN이나 생체정보를 검증한 후에야 제공되어야 한다[7,9]. 마스터키로 암호화된 세션키는 그와 같은 세션키로 암호화된 데이터와 같이 응용 프로그램들이 이용할 수 있다. 이 때, 마스터키가 세션키와 동일하게 취급되면 인가되지 않은 응용프로그램들이 마스터키로 암호화된 세션키의 평문을 획득할 수도 있다. 따라서, 키의 특성에 따라 키의 사용 방법을 제한하는 제어방식을 설치하는 것이 바람직하다. 키의 제어방식은 태그(Tag), 제어벡터(Key Control Vector)[3] 사용방식들이 있다[3].암호키는 암호분석으로 인하여 공격자가 키를 분석하거나 보관된 키를 알아낼 수 있는 문제점이 있기 때문에, 생성된 키는 정해진 기간만 사용된 후 소멸되어야 한다. 특히 세션키의 경우, 세션마다 다른 카들이 사용되어야 한다[17].
- 키의 다양성(Key Diversification) : 키가 손상되는 경우의 피해를 최소한으로 줄이기 위해서는 암호알고리즘에 따라 각각 다른 키들이 사용되어야 한다. 예를 들어 전자서명용, 데이터 전송용, 인증과 데이터 무결성을 위한 키들은 각 알고리즘 용도에 맞게 다르게 사용되어야 하며, 키들을 얻는데 사용되는 마스터키도 각각 달라야 한다.[17]
- 키 버전(Key versions) : 일반적으로 단 하나의 키를 생성해서 전체 카드의 사용기간동안 이용하는 것은 좋지 못하다. 만약 마스터키가 공격자의 공격에 의해 알려지게 되었다고 가정해보자. 이 경우 모든 어플리케이션 제공자들은 자신들의 시스템의 작동을 멈추어야 하고 카드 발행자들은 발행한 모든 카드를 바꾸어야만 한다. 그 결과의 손실은 엄청나다[17]. 따라서 현재 모든 시스템에서는 새로운 키를 생성하여 교환하는 것이 가능하도록 되어있다. 이 새로운 키의 생성은 키가 손상되거나 혹은 주기적인 간격으로 수행될 수 있다. 그러므로 카드를 회수하지 않고 시스템의 모든 키를 새로운 키로 교환하게 된다. 마스터키는 터미널과 시스템의 가장 안전한 레벨로 보관되어야 하기 때문에, 안전한 데이터 통신을 위해서는 아직 알려지지 않은 새로운 버전의 마스터키가 필요하다.

5) 세션키의 설정 또는 설정된 세션키의 저장에는 대칭키나 공개키 암호의 개인키가 적용될 수 있는데 이를 키암호화키(Key Encrypting Key)라고 한다. 키암호화키는 세션키보다는 사용기간이 비교적 길고 모든 클라이언트와 응용서버는 사전에 기밀성과 무결성이 보장되는 채널을 통해서 제공받게 되고, 매 세션마다 새롭게 생성되어야 하는 세션키의 설정에 사용된다.

4. IC카드에서의 공격방법

IC카드는 기존의 마그네틱 카드에 비하여 안전성 면에서 많은 장점이 있다. 이러한 IC카드는 현재 기술수준으로 가장 안전한 정보저장 수단으로 알려져 있다. 그러나, IC카드에서 정보를 안전하게 저장하는 기술이 발달함에 따라 이를 분석하는 기술 역시 발달하였기에 "과연 IC카드가 안전한가?"는 답하기 매우 어려운 질문이 되었다.

이에 따라, 이 절에서는 IC카드에 관련된 공격기법들을 알아보기 위해 IC카드와 응용환경에서의 객체들 사이에 일어날 수 있는 공격모델들[6]을 정의하고, 카드 자체에 대한 공격기법들을 조사하여 정리하고자 한다.

4.1 IC카드에서의 공격모델

IC카드의 공격주체란 IC카드 응용 시스템을 구성하는 모든 주체(즉, 카드원소유자, 카드취득자 등)

를 의미하며 이들은 카드에 대한 공격가능성을 가지고 있다.

먼저 IC카드의 참여자는 카드소유자(Cardholer), 터미널(Terminal), 데이터 소유자(Data owner), 카드발행자(Card Issuer), 카드제조업자(Card Manufacturer), 소프트웨어 제조업자(S/W Manufacturer) 등으로 분류할 수 있다.

- ㅇ 카드소유자 : IC카드를 소유하고 있는 참여자
- ㅇ 데이터 소유자 : 카드 안에 있는 데이터를 통제하는 참여자
  - ※ 디지털 인증서를 전달하는 도구로 카드를 사용하는 경우, 카드 소유자는 데이터 소유자임, 그러나, 카드가 전자-현금 카드라면 카드의 발행자가 데이터 소유자임
- ㅇ 터미널 : 사용자가 컴퓨터 시스템을 이용하는 위치로 최종 단말 위치에 연결되어 동작되는 장치로 IC카드와 사용자를 연결시켜줌. 터미널은 IC카드의 모든 입/출력(I/O)을 통제
- ㅇ 카드발행자 : IC카드를 발행하는 참여자, IC카드에 탑재되는 운영체제와 초기의 IC카드에 저장되는 데이터를 제어
- ㅇ 카드제조업자 : IC카드를 생산하는 참여자
- ㅇ 소프트웨어 제조업자 : IC카드에 들어가는 소프트웨어를 만드는 참여자

IC카드에 대한 공격 모델은 크게 시스템에 참여하는 참여자들에 의한 내부공격, 카드를 훔치는 공격자에 의한 외부공격으로 분류할 수 있으며, 이를 구체적으로 분류하여 정리하면 다음과 같다.

- ㅇ 카드소유자 혹은 데이터 소유자에 대한 터미널 공격 : 카드소유자가 자신의 카드를 터미널에 삽입하였을 때, 공격자가 ATM과 같은 터미널을 조작하여 공격하는 방법. 예를 들어 정직한 카드소유자는 $1의 지불을 하기를 원하지만, 조작된 터미널은 $1의 지불대신 $10의 지불을 명령하는 경우를 들 수 있음.

  이러한 공격을 방지하기 위해 IC카드에 탑재된 S/W로 하여금 위조된 터미널이 거래할 수 있는 거래량(한 번 거래시 최대 거래양을 $1로 제한[10])을 제한하는 방법이 사용되고 있음
- ㅇ 터미널에 대한 카드소유자의 공격 : 이 공격은 카드와 터미널 사이의 프로토콜을 공격할 목적으로 카드에 탑재된 소프트웨어 및 카드를 위조하는 공격을 말함. 이러한 공격을 막기 위해 카드의 물리적인 면을 위조하기 어렵게 만들고 있음[6]
- ㅇ 데이터 소유자에 대한 카드소유자의 공격 : 카드에 저장된 데이터에 대한 카드소유자의 공격을 말함. 현재까지 카드에 저장된 데이터를 알아내기 위한 공격방법으로는 Reverse-Engineering, Fault Analysis, Power 혹은 timing analysis와 같은 Side Channel attack 등이 있음
- ㅇ 발행자에 대한 카드소유자의 공격 : 이 공격은 발행자가 카드 안에 시스템의 사용을 인가하는 정보를 저장하였을 경우, 이 정보 혹은 프로그램의 무결성 혹은 인증에 대한 공격들을 말함
- ㅇ S/W 제조업자에 대한 카드소유자의 공격 : 악의적인 사용자가 자신에게 발행되는 카드에 새로운 S/W 프로그램을 설치하는 공격을 말함
- ㅇ 발행자에 대한 터미널 소유자의 공격 : 카드 발행자를 상대로 사기를 치거나 카드 발행자의 서비스 장애를 유발시키는 등, 카드와 카드발행자 사이의 모든 통신을 제어하는 터미널이 기록을 변조하거나 거래를 중단시키는 공격을 말함
- ㅇ 카드소유자에 대한 발행자의 공격 : 이 공격은 악의있는 발행자를 가정하는 것으로, 보통 카드소유자의 프라이버시를 침해하는 공격을 말함. 전자화폐를 위해 사용되는 IC 카드는 화폐처럼 익명성(Anonymity)과 불연계성(Unlinkability)을 제공하도록 설계되어야만 하는데 시스템의 잘못된 설계 및 공격은 사용자의 정보를 발행자가 모을 수 있게 하고있음
- ㅇ 데이터 소유자에 대한 제조업자의 공격 : 제조업자의 카드구현 시 데이터 정보(예를 들어, 어플리케이션 키 정보 등)를 알아내기 위한 의도된 공격방법으로, 난수생성기의 사용으로 인한 공격방법[15], Kleptographic Attacks[5,12], Subliminal Channels[10]등이 있음.
  - ※ Kleptographic 공격이란, 암호칩(블랙박스장치)의 설계자가 사용자의 정보를 알지 못하게 훔쳐낼 수 있게 하기 위한 기술임. 예를 들어, 설계자는 시스템이 사용자의 공개키/비밀키를 생성할 때, 사용자의 공개키를 ($n=pq, e=p^E \bmod N$)이 되면서 $(e, \phi(n))=1$이 되도록 설

6) VISA와 MasterCard사는 카드의 위조를 방지하기 위해 Hologram기술을 카드에 적용하고 있음

계한다. 사용자가 이렇게 조작된 시스템을 사용하여 공개키/비밀키를 생성하는 경우, 설계자는 공개키 디렉토리부터 얻은 사용자의 공개키 e로부터 사용자의 비밀정보인 $p = e^D \pmod N$을 계산할 수 있게되는 공격을 말함(단, N과 E는 설계자의 공개키, D는 설계자의 비밀키)

※ Subliminal Channel이란 통신하는 두 사용자들도 모르는 은밀한 통신경로를 말하는 것으로, 1983년 Simmons이 Schnorr 전자서명방식에서 은닉채널을 만들 수 있는 방법을 제안함[9]

o 이외에도 참여자들의 역할이 바뀌거나, 분할됨으로써 발생되는 공격법들이 있는데, 예를 들어 카드도난으로 인해 발생되는 공격, 공격자로 하여금 ActiveX 컨트롤을 사용하여 터미널 소유자가 되게 하는 공격기법 등이 있다.[8] 또한, 공격자는 카드와 단말기 사이의 거래를 모니터링 함으로써 거래에 대한 프라이버시를 침해할 수 있으며, PIN 혹은 비밀 데이터의 기밀성을 공격할 수 있음

4.2 IC카드자체에 대한 공격기법

IC카드를 이용한 위성 TV 채널의 유료 디지털 방송은 대부분 해킹되었다. 몇몇 유료 TV 해킹기술은 일반 PC와 IC카드 프로그램을 이용하여 간단하고 즉각적으로 적용할 수 있다[16]. 그러나, 만일 하나의 방송을 해킹하기 위해 수 시간의 준비과정이 필요하다면, 그 해킹기술이 아무리 간단하고 쉽다고 하더라도 이를 이용하는 사람은 거의 없을 것이다.

먼저 안전성을 분석하기 위해 IC카드자체를 공격하는 공격자의 레벨을 〔표 7〕과 같이 3단계로 구분하기로 한다.

GSM 무선 전화의 SIM 카드와 자동차의 원격 잠금 장치, 지불 토큰, pay-TV의 IC카드 등 IC카드를 이용한 응용프로그램의 수가 증가함에 따라, 공격자는 하나의 시도가 아닌 많은 시도를 거쳐 공격을 할 수 있다. 그래서, 모든 공격자들은 목표장비의 샘플을 얻을 수 있다고 가정되며, 제어 단계의 회로에서의 보안 장치는 무시하고, IC카드나 다른 칩 레벨의 보안 프로세서에 저장되어 있는 암호키를 복구하는데 공격을 집중하도록 공격모델을 설정하도록 하자.

IC카드를 분석하는 기술은 크게 침입형 공격(Invasive Attack), 준침입형 공격(Semi-Invasive Attack)과 비침입형 공격(Non-invasive Attack)으로 분류할 수 있다.

4.2.1 침입형 공격

침입형 공격은 IC카드를 H/W적으로 분해하고 분석하는 공격을 의미한다. 비침입형 공격이라고 할지라도 어느 정도는 침입형 공격이 요구된다. 일반적으로 침입형 공격은 특별한 연구실에서 수시간에서 수일에 이르는 긴 시간동안 이루어지기 때문에, 매우 높은 수준의 기술과 고가의 장비를 이용할 수 있는 공격자만 가능하다.

o 칩 분해단계 : IC카드의 칩은 1㎠ 크기로, 한쪽 면은 카드 리더기와 접속하기 위해 노출되어 있으며, 반대쪽은 실리콘물질과 에폭시 수지로 덮혀있다. 이러한 칩을 분해하는데 필요한 도구 및 재료는 주위에서 값싸고 손쉽게 구할 수 있으며, 과정 역시 어렵지 않다. 먼저 날카로운 칼을 이용하여 칩 모듈의 뒷면에 있는 플라스틱을 에폭시 합성수지가 보일 때까지 제거하고, 질산(NHO3) 몇 방울을 에폭시 합성수지 위에 떨어뜨리고, 칩의 일부가 보일 때까지 몇 분간 기다린다. 질산이

〔표 7〕 IC카드 자체에 대한 공격자 레벨

공격자 레벨	특 징
Class I clever outsiders	• 시스템에 대한 불충분한 지식을 가지고 있음 • 보통 수준의 장비를 분석에 이용함 • 시스템의 약점을 생성하기보다는 기존에 존재하는 약점을 이용함
Class II knowledgeable insiders	• 특별한 기술 교육과 경험이 있으며, 시스템에 대한 충분한 지식 보유 • 매우 정교한 장비와 도구를 분석에 이용함
Class III funded organizations	• 매우 큰 자본을 바탕으로 상호보완되는 기술을 가진 전문가 팀 • 정교한 공격을 설계하고 가장 최신 분석도구를 사용하여 시스템 분석 • 공격팀의 일부로 Class II의 공격자들을 이용함

제거한 에폭시 합성수지가 다시 단단해지기 전에 이것들을 아세톤에 씻어낸다. 이러한 과정을 몇 번 반복함으로 IC카드로부터 칩을 분리할 수 있다.

- 아키텍처 재구성 단계 : IC카드에 열과 화학처리로 칩을 분리한 뒤 고해상도 CCD 카메라와 연동된 광학현미경을 통해 칩 표면의 아키텍처 및 모듈 경계를 확대하여 재구성하는 단계이다. 공격자는 CMOS VLSI 설계기술과 마이크로프로세서 기술에 전문적인 지식을 가지고 있어야 하나, 이런 지식들은 많은 문서를 통해서 손쉽게 구할 수 있다.
  칩은 여러개의 층으로 구성되어 있는데, Hydroflouric Acid(HF)를 이용하여 하위층의 아키텍처를 재구성한다. 이러한 공격에 대응하기 위해 이미 잘 알려져 있는 표준 아키텍처 대신에 비표준 명령이나 "버스 스크램블링" 기술을 사용하여 카드를 제작하지만, EEPROM 메모리 셀의 전체 패스를 분석하면 다시 재구성할 수 있다. 또한, 암호알고리즘을 구현한 부분도 ASIC 설계기술을 응용한다면 공격이 가능하다. 또한, 공촛점 현미경, 전자현미경 및 이미지처리 기술을 이용하면 표준 ROM과 Dopant Selective Staniningrl 기술을 사용하여 ROM의 데이터도 읽을 수 있다.
- 보호막 제거 단계 : 대부분의 칩은 이온의 이동, 환경영향으로부터 보호하기 위해 실리콘 질화물 또는 산화물의 보호층을 가지고 있다. 실리콘 물질은 질산에 의해 영향을 받지 않기 때문에, 일반적으로 수소 불화물을 이용한 드라이 에칭으로 보호층을 제거한다. 보호층을 제거하는 다른 접근방법으로는 초음파 진동을 이용하여 보호층을 제거하는 마이크로프로빙(Microprobing) 방법과 레이저 절단기를 이용하는 방법이 있다.
  광학현미경, 시험패키지, Micropositioner 등이 포함된 "마이크로프로빙 워크스테이션"을 사용하여 보호막을 제거하기도 하나, 이를 사용하기 위해서는 많은 비용이 들기 때문에 Class I의 공격자가 하기에는 쉽지 않다.
- 입자빔 기술 : 초점이온빔 워크스테이션(FIB, Focused Ion Beam Workstation)은 갈륨 입자총 및 스캔 전자현미경(Scanning Electron Microscope)으로 구성되어있으며, 금속층 아래의 신호라인까지 작은 구멍을 뚫어 백금으로 그 안을 채움으로서 표면에서 금속층 내부로 접속이 가능하게 하여, 칩상의 두꺼운 메탈층과 폴리 실리콘 라인으로 구성된 보호층을 해독 할 수 있다.
  전자빔 테스터(EBT, Electronic Beam Tester)는 전압 조정 기능을 갖는 전자현미경이라 할 수 있다. 칩의 버스라인을 실시간으로 기록을 위해 칩의 클럭을 100kHz이하로 감소시킬수록 유용하며, 주기적인 시그널을 생성할 수 있을 때 유용한 공격도구이다.

4.2.2 준침입형 공격

침입형 공격은 칩을 완전히 분해하는데 반하여 준침입형 공격은 칩의 보호층을 제거하지 않고 칩의 표면에서 공격을 시행한다. 트렌지스터에 빛을 비춤으로서 오류를 유발시키는 공격이 가능하다. 소요되는 비용이 저렴한 것이 특징이다. UV-라이트, X-레이, 이온화 장비를 이용하여, 칩의 보호층을 제거하지 않고 비밀정보가 저장되어있는 EEPROM에 접근하는 공격은 칩의 구조와 기능이 잘 알려져있다면 EEPROM의 출력을 증폭하여 읽어낼 수 있다.

마지막으로, EEPROM이 정보를 읽고 쓰기 위해서 비교적 높은 전압이 필요하다는 점을 이용하여 EEPROM에 공급되는 전압을 조작함으로 공격을 할 수 있다. 초기 전화카드나 Pay-TV 카드 뿐 아니라 다른 많은 IC카드에 적용이 가능한 강력한 공격이다.

4.2.3 비침입형 공격

- Timing Attack : 암호화나 전자서명 등에서 입력되는 정보에 따른 연산 시간의 차이를 이용한 공격이다. 이 공격은 IC카드의 PIN이 알려져 있거나, 공격자가 원하는 입력을 IC카드에 넣을 수 있어야 가능하다.
- Power Analysis : 전력분석법은 IC카드의 전유소모량을 측정하여 공격에 이용하는 것이다. SPA (Simple Power Analysis)는 단순히 시스템의 전력소비를 측정하는 것이고, DPA(Differential Power Aanlysis)는 비트 "1"의 전력소모량이 비트 "0"보다 많음을 이용한다.
- Fault Generation Attack : IC카드의 프로세서가 동작하는 환경을 조절함으로 프로세서가 오작동을 하도록 하는 공격방법으로, 입력되는 전압의 크기 또는 주위의 온도를 조절하는 방법이다.
- Differential Fault Analysis : DFA는 IC

카드등이 열, 진동, 압력등의 영향으로 에러를 발생할 때, 이를 정상적인 결과와 비교하여 공격하는 방법이다. 주로 DES와 같은 암호알고리즘에서 오류를 이용해 이를 분석하는데 이용한다.

- 대응방법 : 비침입형 공격은 주로 프로세서의 오류를 유발시켜 이를 분석하거나, 프로세서의 동작중에 나타나는 현상을 분석에 이용한다. 그러므로, 오류가 발생하지 않도록 프로세서를 설계하고, 정상적인 환경이 아닐 경우 EEPROM의 정보를 초기화시키고, IC카드 연산 중에 나타나는 전자파나 전류의 소모량들을 일정하게 유지시키거나 랜덤화시키는 등의 과정으로 공격을 막을 수 있다.

Ⅵ. 결 론

IC카드가 화폐가치를 저장하기 위해 물리적 보안 및 암호기법 등을 사용함으로써 마그네틱 카드보다 훨씬 안전함에 따라, 화폐 가치를 이전하는 수단이 마그네틱 카드에서 IC카드로 대체될 것으로 기대되고 있다. 그러나, IC카드가 갖는 물리적 안전성에 대한 위협 및 최근에 대두된 부채널 공격 등으로 인해 IC카드에 저장된 비밀키에 대한 정보를 알아 낼 수 있는 다양한 공격기법들이 나타나고 있다. 이에 본 고에서는 IC카드의 안전성 관련기능으로 카드에서의 사용자 인증, 카드와 카드단말사이의 실체인증, 접근통제 및 데이터의 기밀성/무결성, 키관리에 대해 알아보고, IC카드와 관련된 공격모델 및 공격기법들을 조사하여 정리하였다.

참 고 문 헌

[1] 팀즈코리아, http://www.terms.co.kr

[2] 한국전자지불포럼, "국내 전자지불산업의 동향 및 전망", 2002.11.

[3] 한국정보보호진흥원, "스마트카드 제품 평가기준 해설서", 2000.11.

[4] 한국정보통신기술협회, "2001년도 정보통신표준화백서", 2001.12.

[5] A. J. MENEZES, P. C. VAN OORSCHOT and S. A. VANSTINE, "Handbook of applied cryptography", CRC Press, Boca Raton 1997.

[6] B. Schneier, A. Shostack, "Breaking Up Is Hard To Do : Modeling Security Threats for Smart Card", USENIX Workshop on Smartcard Technology, Chicago, Illiois, USA, May 10-11, 1999.

[7] ECBS, "Guideline on Algorithm Usage and Key Management", TR406, 2001.9.

[8] EMV2000, "Integrated Circuit Card Specification for Payment Systems Book2".

[9] GSA, Smart Access Common ID Card : Final Requirements Document, 2000.

[10] NIST, "Key Management Standard", http://www.csrc.nist.gov/encryption/kms

[11] O. Kommerling, M. G. Kuhn, Design Principles for Tamper-Resistant Smartcard Processors, In USENIX Workshop on Smartcard Technology, 1999.

[12] On cryptosystems untrustworthiness, Pavel V. Semjanov(Information Security center, St. Petersburg Technical University), 1996.

[13] R. Anderson, M. G. Kuhn, Low Cost Attacks on Tamper Resistant Devices, Security Protocols, 5th International Workshop, Paris, France, April 7-9, 1997

[14] R. Anderson, M. G. Kuhn, Tamper Rsistance - a Cautionary Note, Second USENIX Workshop on Electronic Commerce Proceedings, pp.1~11, Oakland, California, 18-21.11.1996.

[15] Snake Oil Warning Signs : Encryption Software to Avoid, 1998, Matt Curtin http://www.interhack.net/people/cmcurtir./ snake-oil-faq.ps.

[16] Stefano Zanero, Smart Card Content Security, http://securenetwork.it/szanero/scsecurity.pdf

[17] W. Rankl & W. Effing, "Smart Card Handbook : Second Edition", WILEY 2002.

〈著 者 紹 介〉

주 학 수 (Hak-Soo Ju)
정회원

1997년 8월 : 고려대학교 수학과 이학사
1999년 8월 : 고려대학교 수학과 이학석사
2001년 8월 : 고려대학교 수학과 박사과정 수료
2001년 9월~현재 : 한국정보보호진흥원(KISA) 연구원
관심분야 : 암호학, 공개키암호, 응용보안프로토콜

현 진 수 (Jinsu Hyun)
정회원

2000년 2월 : 한양대학교 수학과 이학사
2002년 2월 : 한양대학교 대학원 수학과 이학석사
2002년 1월~현재 : 한국정보보호진흥원 연구원
〈관심분야〉 암호학, 블록암호, 난수테스트

성 재 철 (Jaechul Sung)
정회원

1997년 8월 : 고려대학교 수학과 이학사
1999년 8월 : 고려대학교 대학원 수학과 이학석사
1997년 9월~2002년 7월 : 고려대학교 정보보호기술연구센터 연구원
2002년 8월 : 고려대학교 대학원 수학과 이학박사
2002년 7월~현재 : 한국정보보호진흥원 선임연구원
관심분야 : 암호학, 대칭키암호알고리즘 및 해쉬함수의 분석 및 설계

임 선 간 (Seongan Lim)
종신회원

1985년 : 동국대학교 수학과 학사
1987년 : 서울대학교 수학과 석사
1995년 : Purdue 대학교 수학과 박사
1999년~2002 : 한국정보보호진흥원 선임연구원
2003년~현재 : 한국정보보호진흥원 암호인증기술팀장
관심분야 : 암호프로토콜, 정보보호 등