通信情報保護學會誌
第 10 券 第 3 號, 2000. 9

스마트카드 데이터 보호를 위한 접근통제 모델 분석

권 현 조*, 원 동 호**

요 약

본 고에서는 최근 휴대용 보안장치로 이슈화되고 있는 스마트카드에 대하여 기술한다. 요즘 우리주변에서 쉽게 접할 수 있는 스마트카드는 교통카드이다. 1997년 스마트카드를 이용한 버스카드 시범 프로젝트가 성공적으로 이루어지면서 1999년부터는 지하철 패스와 버스카드를 통합하여 지금은 일반인들이 소유하고 있는 가장 보편화된 교통 지불 수단으로서 그 활용도가 높다고 볼 수 있다. 최근 스마트카드에 대한 인식이 제고되고 있는 이유는 스마트카드가 일반 사용자들의 실생활을 사이버세계를 연결해 줄 수 있는 다리역할을 할 수 있기 때문이다. 하지만 일반인들은 스마트카드가 보안 장치로서의 역할을 수행한다는 사실은 인지하지 못하고 있는 실정이다. 앞으로 실생활에 밀접하게 활용되게 될 스마트카드에 대한 보안 구조를 살펴보고 스마트카드에 저장되어 있는 사용자 데이터를 보호하기 위하여 스마트카드에 구현되는 접근통제 메커니즘을 분석한다.

Ⅰ. 서 론

스마트카드는 신용카드 크기의 플라스틱 카드로서 데이터를 가공·처리할 수 있는 칩을 내장하고 있다. 1974년 프랑스의 Roland Moreno가 IC 카드로 특허를 출원한 이후 Bull S&T사와 모토롤라사가 공동으로 칩 카드를 개발하였으며 1981년에 현재 상용화되고 있는 단일 칩으로 구성된 스마트카드가 개발되었다[1]. 정보통신 환경의 발달로 인하여 실생활의 많은 부분들이 사이버 세계에서도 이루어지면서 일반 사용자들은 자신들이 소유한 정보에 대한 가치를 인식해 가고 있다. 이에 수반하여 정보보호에 대한 인식도 점차 확산되어 가고 있다. 최근들어 전자상거래 환경이 구축되면서 실물경제가 사이버 세계에서 이루어지고 가치이전의 수단으로 스마트카드의 중요성이 부각되고 있다. 사이버 세계에서 스마트카드는 가치이전의 수단뿐만 아니라 전화카드, 이동 통신 보안수단, 신분증, 교통카드 등 그 활용분야가 아주 다양하기 때문에 정보통신망 환경에서 스마트카드가 중요한 보안장치로 수요나 활용면에서 급격한 증가율을 보이고 있는 실정이다.

스마트카드는 ID-1 형식의 신분확인 카드 계열 중에 가장 최근에 개발된 카드이며 기존의 카드보다도 많은 정보처리 능력을 가질 뿐만 아니라 보안특성도 가지고 있다. ID-1 형식의 신분확인 카드는 엠보싱 처리를 한 카드, 마그네틱 카드, 스마트카드 순으로 발전되어 왔으며 스마트카드는 마그네틱 카드와 비교하여 볼 때 많은 장점을 가지고 있다. 스마트카드는 20 Kbytes 정도의 저장용량을 가지고 있으며 특히 비인가된 접근 및 훼손공격으로부터 스마트카드에 저장된 데이터를 보호할 수 있는 기능을 가지고 있다. 스마트카드에 대한 접근은 스마트카드 운영체제 및 보안논리 회로를 통해서만 가능하도록 접근통제 메커니즘이 구현되어 있으며 스마트카드에 마이크로프로세서와 더불어 co-processor를 추가하여 복잡한 산술연산을 빠른 시간 내에 할 수 있도록 한다면 암호연산을 스마트카드 내에서 처리할 수 있다[1]. 스마트카드가 암호연산을 자체적으로 수행할 수 있으므로 휴대하기 편리한 가장 간단한 보안장치로 스마트카드에 대한 관심이 고조되어 가고 있다.

스마트카드의 기술이 발달함에 따라 여러 가지 보

* 성균관대학교 정보통신대학원 정보통신공학과(hckwon@kisa.or.kr).
** 성균관대학교 전기전자컴퓨터 공학부 (dhwon@simsan.skku.ac.kr)

안기능을 구현할 수 있지만 가치저장장치의 안전한 수단으로써 스마트카드가 가져야 할 보안기능은 접근통제 기능이다. 접근통제는 외부 실체가 스마트카드의 파일 및 데이터에 대한 접근을 시도할 경우 접근통제 메커니즘에서 정의한 접근규칙에 따라서 접근을 허가 또는 금지하는 보안기능이다. 즉 스마트카드의 파일 및 데이터에 대한 접근을 통제하여 스마트카드의 정보를 보호하는 수단을 제공한다. 스마트카드에 대한 연구는 학계에서보다는 스마트카드를 실제로 개발하고 상용화하는 유럽의 산업계에서 활발히 이루어져왔기 때문에 스마트카드에 대한 표준 개발도 이들이 주도로 이루어졌고 현재 스마트카드 개발자들은 스마트카드의 표준을 많이 준용하고 있다. 이 중에서도 ISO/IEC JTC 1 7816 IC 카드 표준은 스마트카드의 물리적 특성, 기본명령어, 보안구조, 데이터 객체 정의, 보안기능 명령어 및 접근통제를 위한 보안속성에 대해서 정의하고 있다.

본문에서는 이 표준을 중심으로 스마트카드의 보안구조를 분석하고 이 보안구조를 기반으로 이루어지는 접근통제 모델에 대하여 서술한다[2,3,4]. 또한 유럽에서 개발하여 상용화된 COS의 접근통제 메커니즘을 알아보고 스마트카드에서의 데이터 보호를 위한 접근통제 기능 구현을 이해한다[5].

II. 스마트카드의 보안구조

스마트카드의 보안구조는 세 가지로 구분하여 정의할 수 있다. 스마트카드가 어떠한 동작을 수행하고 나면 스마트카드 파일에 대한 보안 상태가 결정되는데 보안상태를 결정하기 전에, 파일에 대한 특성을 저장하고 있는 보안속성 값의 비교결과에 따라 보안상태가 결정된다. 보안 상태의 상태전이를 일으키게 하는 보안기능을 구현한 것이 보안 메커니즘이다. 본 절에서는 스마트카드의 보안구조를 결정하는 보안상태, 보안속성 및 보안 메커니즘에 대하여 서술하며 그림 1에서는 스마트카드의 전반적인 보안구조를 나타내고 있다.

1. 보안상태

보안상태(Security Status)는 스마트카드가 어떠한 동작을 수행하고 난 이후의 카드의 현재상태를 나타내는 것이며 명령어를 수행하거나 파일에 대한 접근을 시도할 경우 카드가 발행되기 이전에 정의된 객체에 대한 보안속성과 보안상태를 비교하여 수행조건 및 접근조건을 만족하는지를 검사한다. 스마트카드 초기 동작을 수행한 이후나 일련의 실체(entity) 인증 절차를 성공한 이후에 스마트카드의 보안상태가 결정된다. 스마트카드의 상태전이를 일으키는 동작은 다음과 같다[2].

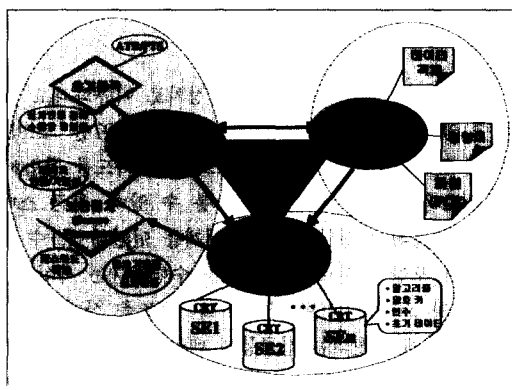


그림 1 스마트카드의 보안구조

- 보안상태를 결정하는 스마트카드 초기동작
  - ATR(answer to reset) : 카드의 동작특성에 대한 정보를 저장하고 있는 요소파일의 내용을 터미널로 전송
  - PTS(protocol to selection) : 터미널과 스마트카드 사이의 프로토콜을 설정
  - 인증 절차를 수행하기 이전에 스마트카드의 안전한 상태를 보장하기 위하여 수행하여야 하는 명령어 또는 일련의 순서를 가진 명령어들
- 보안상태를 결정하는 실체인증
  - 패스워드를 이용한 인증
  - 암호 키를 이용한 인증
  - 보안처리 메시지(SM : Secure messaging)

위와 같은 동작을 수행한 이후 스마트카드의 보안상태가 결정된다. 스마트카드의 보안상태는 스마트카드 내부에 구성되어 있는 파일종류에 따라서 다른 의미로 해석할 수 있다. 예를 들어 패스워드를 이용한 실체인증 기법을 수행하였다 하더라도 그 대상 파일의 종류가 어떤 것인가에 따라 스마트카드의 보안상태가 달라질 수 있다. 스마트카드의 대상 파일의 종류에 따른 보안상태는 다음과 같다.

- Global security status : 스마트카드의 기본

파일(MF)에 접근하기 위하여 요구되는 인증 절차를 성공적으로 수행한 이후에 결정되는 보안상태로서 카드의 동작을 안전하기 수행하기 위한 카드의 전반적인 보안상태를 나타낸다.

- File-specific security status : 전용파일에 대한 접근을 승인 받기 위하여 수행하여야 하는 인증 절차(예, 패스워드를 이용한 인증이나 경우에 따라서 암호 키를 이용한 인증을 성공한 뒤에 파일에 대한 접근허가가 가능)
- Command-specific security status : 명령어를 통해서 전송되는 데이터를 보호하기 위한 수단을 제공한 경우 명령어에 대한 보안상태를 나타낸다.

2. 보안속성

파일에 대한 오퍼레이션을 수행할 경우 적절한 보안조건을 만족시켜야 하며 보안속성(Security Attribute)은 이러한 보안조건을 나타내는 수단이다. 보안속성은 객체에 대하여 허용되는 오퍼레이션을 명시하며 이러한 오퍼레이션을 성공적으로 수행하기 위한 절차를 정의한다. 보안속성은 파일에 종속된 정보를 가지고 있으며 파일의 특성을 나타내는 파일 제어정보 템플릿을 통해 표현된다.

3. 보안 메커니즘(Security Mechanism)

3.1 보안기능

1) 패스워드를 이용한 인증 : 스마트카드는 카드 소지자를 인증하기 위하여 카드외부 실체에서 전송받은 데이터와 스마트카드 내부에 저장되어 있는 비밀정보를 비교하여 스마트카드의 정당한 사용자임을 확인한다. 패스워드를 이용한 인증 보안 메커니즘은 사용자의 권한을 보호하기 위하여 제공되는 기능이다.
2) 암호 키와 암호기법을 이용한 인증 : 인증을 받고자 하는 인증실체는 인증 절차에서 요구하는 암호 키를 알고 있음을 암호기법을 이용하여 증명하여야 한다.
3) 데이터 인증 : 대칭 키 암호시스템에서의 비밀키나 비대칭 키 암호시스템의 공개키와 같은 스마트카드의 내부 데이터를 이용하여 외부에서 전송 받은 데이터에 대한 인증 값에 대한 유효성을 검증한다. 내부 비밀데이터를 사용하여 스마트카드 외부로 유출하는 데이터에 대한 인증 값(암호학적 확인함수 또는 전자서명을 이용한 데이터 인증)을 계산하여 명령어를 통해 외부로 유출되는 데이터와 더불어 전송함으로써 전송데이터에 대한 무결성 기능을 제공할 수 있다.
4) 데이터 암호화 : 스마트카드는 명령어를 통해서 전송받은 암호문을 복호화하기 위하여 스마트카드의 내부 데이터를 이용한다. 카드 외부로 유출되는 데이터에 대한 비밀성 기능을 제공하기 위하여 전송 데이터에 대한 암호문을 생성한 후 이를 명령어에 삽입하여 전송한다. 이러한 기능을 제공하기 위해서는 키 관리 및 접근조건 등이 뒷받침되어야 한다. 암호문을 생성하는 보안 메커니즘을 이용하여 데이터에 대한 은닉기능도 제공할 수 있다. 이러한 경우 스마트카드는 은닉하고자 하는 데이터 스트링을 계산하고 여기에 전송할 데이터 값과 exclusive-or 연산을 수행한다. 이로써 데이터에 대한 프라이버시 기능을 제공할 수도 있으며 메시지 필터링에 대한 가능성을 줄이는 효과도 얻을 수 있다.

3.2 Secure messaging(SM)

Secure messaging의 목적은 암호기법을 이용하여 명령어를 통해 교환되는 데이터에 대한 보호기능, 즉, 데이터 인증 및 데이터 기밀성 기능을 제공하는 것이다. 하나 이상의 보안 메커니즘을 적용하여 SM을 수행하기 위해서는 관련되는 암호알고리즘, 암호 키, 인수 및 초기 값 등 보안관련 정보를 스마트카드에서 제공하여야 한다. SM을 수행할 수 있는 대상 객체의 유형을 데이터 평문 값, 보안 메커니즘에서 사용되는 데이터 객체 및 보안기능 데이터 객체 등 3가지로 분류한다. 보안 메커니즘에서 사용되는 데이터 객체 중에서 인증 및 기밀성 기능에서 이용되는 데이터 객체는 다음과 같다.

1) 인증기능 수행에 사용되는 데이터 객체

(1) 암호학적 체크섬 값을 이용한 데이터 인증

암호학적 체크섬을 계산하기 위해서는 초기 블록값, 비밀키, 블록암호알고리즘 등이 사용되어야 한다. 암호학적 체크섬을 계산하기 위하여 사용되는

알고리즘은 입력 값을 K바이트 블록 크기의 입력 값을 받아 K 바이트 블록 크기의 출력 값을 계산해 낸다. 암호학적 체크섬 방식의 동작모드는 CBC (Cipher Block Chaining)를 이용한다. CBC 모드는 출력 암호문이 다음 평문 블록에 영향을 미치게 하여 각 암호문 블록이 전단의 암호문의 영향을 받도록 만든 방식으로 동일한 평문에 의한 동일한 암호문이 발생하지 않도록 구성한 동작모드이다[11].

암호화 Ci = EK(Mi⊕Ci-1)

복호화 Mi = DK(Ci)⊕Ci-1

전송중에 암호문 블록 C에서 발생하는 한 비트의 오류는 복호화된 해당 평문 블록 M에서는 여러 비트의 영향을 주게된다. CBC 모드의 평문 블록 M에서의 오류 발생시 암호문 분석에 미치는 영향을 살펴보면 평문 블록 M에서의 한 비트 오류는 그 다음에 출력되는 모든 암호문 블록 C1, C2 C3, C4, . . ., Cn 에 영향을 미치게 된다. 이러한 특징은 메시지 인증에 유용하게 사용될 수 있다. 즉, 스마트카드와 외부실체간의 CBC 모드를 사용하면 MAC로 사용할 수 있다. 스마트카드는 평문 M1, M2, M3, . . ., Mn을 CBC 모드로 암호화 한 마지막 블록 Cn을 함께 수신자에게 전송한다. 수신자는 전송 받은 평문 M1, M2, M3, . . ., Mn의 이상 유무를 CBC모드의 암호화 과정을 거쳐 C1′, C2′ C3′, C4′, . . ., Cn′을 구하여 마지막 Cn′과 수신한 Cn을 비교하여 확인할 수 있다.

(2)전자서명 데이터 객체

전자서명 값의 계산은 비대칭 암호시스템을 기반으로 이루어진다. 전자서명의 유형은 부가형 전자서명과 메시지 복원형 전자서명 두 가지로 구분할 수 있다. 부가형 전자서명은 서명을 계산하기 위한 중간 값에 해쉬 값이 포함된다. 메시지 복원형 전자서명에는 해쉬 함수를 사용하지 않는다.

2) 기밀성 기능을 제공하기 위하여 사용되는 데이터 객체

기밀성을 위한 데이터 객체는 평문 값을 암호문으로 생성하여 이를 전송하는 수단이 된다. 블록암호 알고리즘을 이용하는 경우 동작모드에 대하여는 제한하지 않으나 고정 블록크기를 맞추기 위하여 패딩 비트에는 크기에 제한을 하게 되며 패딩 비트의 추가여부를 표시하여야 한다. 하지만 패딩 비트의 크기가 고정블록 크기 보다 큰 경우 메시지 전환에 영향을 미칠 수 있다. 스트림 암호알고리즘을 이용하여 전송데이터에 대한 기밀성 기능을 제공하는 경우 패딩 비트를 추가할 필요가 없다.

3.3 보안기능 데이터 객체

보안 메커니즘을 적용하기 위하여 필요한 정보들을 담고있는 객체이며 각각의 보안 메커니즘에 적당한 정보들을 템플릿에 저장하여 사용한다. 즉, CRT(Control Reference Template)는 보안기능 데이터객체를 운반하는 container이다. 스마트카드의 Secure Messaging 수행 시 필요한 정보들이므로 스마트카드에서는 암호학적 체크섬 SM 처리를 위한 템플릿 CCT(Cryptographic checksum Template), 전자서명 SM을 처리하기 위한 템플릿 DST(Digital Signature Template) 및 기밀성 SM을 처리하기 위한 템플릿 CT(Confidentiality Template)으로 CRT를 정의한다.

표 1 스마트카드 보안기능 데이터 종류

보안기능 데이터 객체	비 고
Algorithm reference	암호알고리즘, 동작모드 등 암호기법을 사용하기 위한 정보를 결정
File reference	암호키에 대한 정보가 저장된 파일을 결정
Key refernece	사용할 암호키의 식별자를 결정
Initial data refernece	암호학적 체크섬을 계산할 경우 초기 블록 값을 결정 ※도전-응답 방식의 암호기법을 이용할 경우 도전값, 난수, 시간변이 값 등을 결정할 수 있음
Cryptogram contents reference	암호문의 내용을 명세

Ⅲ. 데이터 보호를 위한 접근통제 모델

1. 접근통제 개요

정보보호의 핵심 기술인 접근통제 기능은 데이터를 보호하기 위한 메커니즘을 구현하는 것이 목적이다. 접근통제는 시스템의 주체의 신분에 근거한 ID-based 보안통제를 수행한다. 접근통제를 스마트카드에 적용하기 위해서는 접근통제의 대상이 되는 주체 및 객체의 정의와 접근통제규칙이 기술되어

야 한다.

접근통제를 하기 위해서는 주체 및 객체에 대한 정의가 되어야 하는데, 주체 및 객체의 범위는 접근통제를 구현하는 개발자에 따라서 차이가 있을 수 있으며, 보안정책에 합당한 나름대로의 주체 및 객체에 대한 정의가 되어야 한다. 일반적으로 스마트카드의 접근통제를 위한 주체는 스마트카드에 저장되어 있는 데이터를 이용하기 위하여 스마트카드에 접근하는 외부 실체가 되며 객체는 스마트카드의 내부 자원이 될 수 있다. 또한, 주체 및 객체를 그룹화 하여 관리할 수 있다[6].

본 절에서는 접근통제 개념을 이해하기 위하여 일반적인 시스템 관점에서 접근통제 기능을 서술하였으며 스마트카드에서 구현할 수 있는 접근통제 모델을 ISO 스마트카드 보안모델 표준에서 정의한 접근통제 모델[4], 상용 COS에서 구현한 접근통제 모델[5]들을 중심으로 하여 스마트카드의 데이터 보호를 위한 접근통제 기능을 분석해 본다.

일반적으로 시스템에 대한 접근통제는 다음의 2가지 방법으로 구현할 수 있다[7].

- "누가 시스템에 접근할 수 있는가"를 제한하는 방법으로 다음의 2단계 절차에 의하여 이루어진다.
  ① 식별(Identification) : 시스템에 접근하는 주체가 누구인지를 유일하게 판별하는 단계
  ② 인증(Authentication) : 식별된 주체가 원래 의도된 것인지를 입증하는 단계
- "시스템을 접근한 자가 무엇을 행할 수 있는가"를 제한하는 방법으로 대표적인 예로 서비스 제한 시스템(Limited Service System)을 들 수 있다.

이러한 서비스 제한 시스템은 시스템이 식별할 수 없는 사용자들에게는 매우 제한되고 통제된 기능만을 제공하는 것으로 비행기 예약 및 일정 등에 관한 항공 업무 등에 적합하다. 이러한 기법은 범용 OS에 적용하기는 어렵다.

식별과 인증 외에 내부적인 권한부여(Authorization)를 고려할 수 있으며 다음의 그림 2와 같이 다단계 접근통제 개념으로 표현된다.

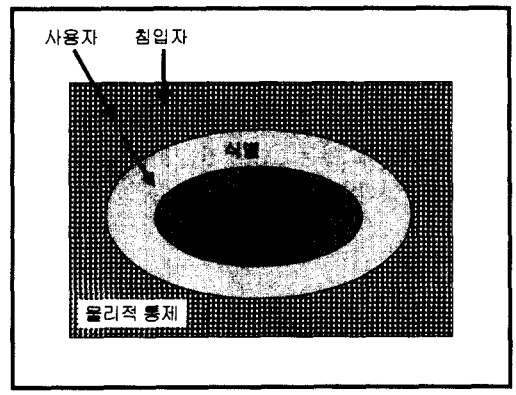


그림 2 다단계 접근통제

1.1 접근통제 정책

보안정책은 사용자들로 하여금 시스템 정보 및 자원을 이용할 수 있도록 하는 조건을 정의한 것이다.

따라서 보안정책에는 시스템 구현 시에 만족시켜야 하는 요구사항의 집합을 정의한다. 보안정책은 시스템이 적용되는 환경에 따라 다르게 정의될 수 있으며 정의된 보안정책을 주체, 객체, 오퍼레이션의 개념을 이용하여 구현할 수 있으며 이러한 기능이 접근통제 기능이다. 접근통제는 시스템의 내부동작을 통제하는 목적으로 주체의 객체에 대한 접근을 통제하는데 일반적으로 주체는 프로세스가 될 수 있으며 객체는 파일이나 디렉토리와 같이 정보를 담고 있는 논리적 구조이며 주체가 객체에 접근한다라고 함은 읽기, 쓰기와 같은 오퍼레이션을 수행하는 것이다.

시스템의 보안정책은 어떠한 주체에 의한 접근이 참조 모니터의 기능으로 연결될 수 있는지를 명시한 조건을 정의한 것으로써, 시스템을 통제하는 요구사항으로서의 이러한 조건들은 접근통제규칙으로 표현될 수 있다.

참조 모니터는 일정조건에 따라 주체의 요청을 승인할 것인지 거부할 것인지를 결정하는 일종의 필터링 기능을 가지고 있다. 보안정책은 접근통제규칙을 설정할 수 있으며 이러한 규칙을 적용할 수 있는 보안 메커니즘을 구현하여 접근통제를 이룰 수 있다. 보안정책은 시스템에 대한 요구사항이고 보안 메커니즘은 이러한 요구사항의 구현이다.

보안 메커니즘은 소프트웨어나 하드웨어 내에 보

안기능을 구현하기 위한 논리 또는 알고리즘으로 시스템 하부의 일부분으로서 자동화된 기능처리를 하는 컴포넌트들로 구성된다. 보안 메커니즘의 설계 및 개발 시 궁극적인 목표는 시스템 고장 시에도 안전성을 유지할 수 있는 고장안전(Fail Secure) 기능을 가지는 것이다.

1.2 보안모델

보안모델은 정보시스템이 보호대상 정보 및 객체를 어떻게 보호 및 관리해야 하는지에 대한 보호 규칙을 명시하기 위하여 정보시스템에 의해 시행되어야 하는 시스템 보안정책을 서술한 모델이다. 보안모델과 보안정책 사이에는 미묘한 차이가 있는데 보안정책은 특정 시스템에 대한 요구사항을 명시한 집합을 나타내는 반면 보안모델은 필요하지 않은 상세사항들을 생략하고 시스템의 동작 특성만을 제한적으로 표현한 것이다. 따라서 특정 보안정책을 설계한 것으로 보안모델을 이용할 수 있다[9].

2. 국제표준(안) ISO(7816-9)에서 제시한 접근통제 모델

ISO 7816-9 국제표준(안)에서는 객체별 접근통제 리스트(Access Control List) 모델을 이용하여 스마트카드의 접근통제 모델을 제시한다. 객체별 접근통제 리스트는 객체를 접근할 수 있는 권한을 가진 주체들의 리스트를 유지하는 방법으로써, 접근행렬(Access matrix)에서 각 열(column)의 필드에 접근권한이 설정된 행(row)의 주체들로 표현한다. 접근통제 리스트는 시스템에서 관리하는 각 객체들에 대해서, 접근권한을 가지는 주체와 접근권한을 리스트로 관리하는 모델이다[8]. 객체별 접근통제 리스트에는 다음과 같은 목록들이 반드시 포함되어야 한다.

- 객체 및 객체의 식별자
- 각 객체에 접근할 수 있는 주체 리스트
- 각 객체에 대한 주체의 접근권한

2.1 접근통제를 위한 보안속성 및 보안환경

스마트카드에서는 각 객체에 대한 주체의 접근권한이 보안속성에 저장되어 있다. 보안속성은 접근통제 규칙을 적용하기 위해 필요한 보안 메커니즘을 정의한 것이며 보안속성으로 나타낼 수 있는 정보들은 보안조건, 접근모드(오퍼레이션 유형), 접근통제 규칙이 적용되는 카드 자원의 범위 등이다. 스마트카드의 안전한 운영을 유지하면서 저장된 데이터, 프로세서 등 스마트카드의 자원을 사용할 수 있도록 하는 조건을 보안속성에서 명시할 수 있으며 보안속성을 가질 수 있는 객체의 종류는 표 2와 같다.

접근통제를 위한 보안환경이란 보안속성에서 정의된 접근통제규칙을 적용하여 접근통제를 이루기 위한 정보들을 말하여 이러한 정보들은 시스템 파일에 저장되거나 보안환경을 정의한 템플릿(SEDO: Security Environment Data Object)에 저장된다. 보안환경 템플릿에는 보안환경 식별정보와 보안환경 CRT가 저장되어 있다.

2.2 접근통제

객체에 대한 접근통제는 접근통제규칙에 연관되는 객체를 연결하여 접근을 통제하는 것이다. 객체는 파일, 명령어 및 데이터 객체 등이 될 수 있으며 파일에 대한 접근통제규칙은 파일제어정보(File Control Information ; FCI)내에 저장되어 있다. 파일에 대한 오퍼레이션이 적용될 경우 자신의 FCI에 저장되어 있는 접근통제규칙을 적용하여 접근을 통제한다. 반면 명령어 및 데이터 객체에 대한 접근통제 규칙은 현재 전용파일의 FCI내에 저장되어 있다[4]. 접근통제규칙을 명시하는 방식은 기본형(Compact format)과 확장형(Expanded format)이 있다.

표 2 접근조건을 나타내는 보안속성 특징

보안속성	내 용
대상 객체	· 파일 : 파일의 특성을 나타내는 descriptive data object에 보안속성 값을 가지고 있음 · 명령어, 데이터 객체 : 보안속성 값은 reference data에서 나타내고 있음.
역할	· 데이터에 대한 접근허가가 이루어지기 전에 카드의 보안상태를 명시하는 수단 · 데이터 처리기능(주체)의 데이터(객체)에 대한 접근을 제한하기 위한 수단 · 보안상태를 획득하기 위하여 수행하여야 하는 보안기능을 정의
접근 규칙	· 자원에 대한 접근통제범위를 명시적으로 또는 내재적으로 규정하는 접근규칙집합 · 보안조건과 접근모드를 명시하는 접근규칙 - 보안조건(Security Condition) : 정의된 접근규칙을 적용하기 위하여 필요한 보안 메커니즘을 명시 - 접근모드(access mode) : 접근 오퍼레이션의 유형, 즉, 읽기, 쓰기, 갱신 등과 같은 오퍼레이션을 명시하는 논리적 객체. ※ 접근모드에서는 때때로 접근통제규칙에서 명시한 조건을 만족시키기 위해서 실행되어야 하는 보안기능 및 외부 명령어를 명시하기도 한다.

1) 기본형(compact format)

접근통제 규칙 = 접근모드(access mode) + 보안조건(security condition)

2) 확장형 (Expanded format)

확장형 접근통제규칙을 명시하기 위해서는 객체에 대한 접근통제를 적용할 수 있는 접근규칙 참조 데이터 객체를 정의하여야 한다.

접근통제규칙 = 접근모드 데이터 객체 + 보안조건 데이터 객체

- 접근모드 데이터 객체(AM_DO) : AM byte + 명령어 특성정보 목록
- 보안조건 데이터 객체(SC_DO) : SC byte + CRT

보안조건(1byte)에는 보안환경 식별정보, 보안메시지처리를 요청한 명령어 및 응답, 사용자 인증 등과 같은 조건정보들을 표현할 수 있다. CRT에는 데이터에 대한 접근을 허가 받기 위하여 만족시켜야 하는 보안조건의 보안기능을 수행할 수 있는 보안기능데이터 정보를 가지고 있다. 스마트카드는 이러한 정보들을 기초로 주체가 객체에 접근을 시도할 경우 접근통제규칙을 적용하여 객체에 대한 접근을 통제할 수 있다.

접근모드 데이터 객체와 보안조건 데이터 객체로 이루어진 접근통제규칙은 스마트카드의 내부 요소파일(EF)에 저장되며 파일구조는 선형레코드 구조이다. 접근통제규칙을 내부파일에 저장할 경우 파일식별자를 이용하여 접근통제규칙을 참조할 수 있다. 파일제어정보에 포함된 보안속성을 이용하여 접근을 통제하는 경우 ARR(Access Rule Reference) 데이터 객체를 통해 접근통제규칙을 참조하게 된다. 즉 ARR에는 보안속성 값을 가지고 있다.

〔ARR 구조〕

1. AM_DO ‖SC_DO1 ‖SC_DO2 ‖AM_DO‖. . . .
2. AM_DO ‖SC_DO1 . . .

ISO 7816에서는 객체별 접근통제리스트를 가지고 있으며 이는 접근통제 객체를 통해 표현할 수 있다. 객체에 대한 접근통제 규칙을 참조하기 위한 값은 접근통제Descriptor(ACD)가 가지고 있다. 위에서 기술한 접근통제 관련 정보들을 접근통제 객체를 통하여 나타낼 수 있으며 이 객체에 대한 구조는 표3에서 나타내었다.

표 3 접근통제 객체(ACO) 구조

접근통제 객체요소		내 용
ACID		ACO Identifier
ACL		Link to parent
L		Length of ACO value
ACD	ACDID	First ACD
	L	Length of ACD
	ARR	Access Rule Reference 1
	. . .	Further ARRs
ACD	ACDID	Further ACDs
	L	Length Field
	. . .	

3. STARCOS에서 정의한 접근통제 모델

STARCOS(Smart Card Chip Operating System)는 1996년 독일 Giesecke & Devrient GmbH사에서 개발한 COS로 ISO 표준을 준용하면서 더 나은 기능을 제공한다. COS의 기본적인 역할은 데이터 전송, 저장영역 및 정보처리 기능을 제공하는 것이다.

즉 스마트카드의 자원을 관리하고 스마트카드 운영에 필요한 모든 기능을 제공하며 응용에 따라 난수에 대한 관리기능도 제공한다. 본 절에서는 상용제품으로서 접근통제 기능을 실제로 어떻게 구현하였는지를 분석하여 본다[5].

3.1 접근통제를 위한 보안속성 및 접근조건

파일을 생성할 경우 각 파일에 해당하는 보안속성을 정의하는데 STARCOS는 응용프로그램 식별자(AID)/파일 식별자(FID), 접근조건(AC), 오퍼레이션 모드 등을 보안속성으로 정의한다.

1) 응용프로그램 식별자/파일 식별자 : 외부실체 및 스마트카드 운영체제는 AID 및 FID를 이용하여 스마트카드의 파일에 접근을 할 수 있다. AID 및 FID는 파일유형에 따라 서로 다른 길이와 코딩 값을 가진다. 모든 DF에는 서로 다른 AID나 FID가 정의되어야 한다.

표 4 파일식별정보

파일 유형	식별정보 크기
MF	'3F00'
DF	· AID : 최대 16byte · FID : 2byte
EF	· EF : FID(2byte)

2) 접근조건(Access Condition - AC) : 특정 명령어를 수행하기 위해서는 파일에 대한 접근조건을 만족시켜야 하여 이러한 접근조건을 표현하는 것이 AC이다. MF의 AC에 저장되어 있는 접근조건은 REGISTER, CREATE DF 명령어와 관련된 것이며 CREATE EF, WRITE KEY Install 명령어와 관련된 접근조건은 DF의 AC에 저장되어 있는 접근조건과 관련이 있다. 각 EF의 AC에는 9가지의 접근조건을 가지고 있으며 EF의 AC들은 서로 다르게 정의된다.
3) 오퍼레이션 모드(Operation Mode : OM) : 파일 오퍼레이션 모드는 접근통제를 위한 보안속성을 명시하는 것이다.

3.2 접근통제 모델

STARCOS는 스마트카드의 내부 상태를 정의하여 내부 상태에 따라 응용프로그램의 수행순서를 제어한다. 적절한 상태전이가 일어나면 EF에 응용프로그램의 데이터를 저장할 수 있다. EF내에 있는 데이터를 보호하기 위하여 서로 다른 접근유형(read, update, invalidate, rehabilitate 등)에 따라 접근을 통제할 수 있도록 접근조건(AC)을 가지고 있다. EF에 대한 현재 진행상태가 정의되어 있지 않기 때문에 상태전이가 교환되지 않고 유지되는 상태에서 AC를 기초로

표 6 EF(Element File) 오퍼레이션 모드

OM		플래그 비트
EF 보안속성	EF locked	EF에 대한 접근 허가여부를 표시
ISF 보안속성	Write (WR)	WRITE KEY 명령어를 통해 ISF에 기록되어 있던 암호 키를 갱신할 수 있는 지의 여부를 표시
	Write Once (WO)	WRITE KEY 명령어를 통해 ISF에 기록되어 있던 암호 키 레코드를 단 한번만 갱신할 수 있음을 표시
	Virgin	암호 키 레코드에 기록된 사실여부를 표시

하여 EF에 저장되어 있는 데이터에 대한 접근이 가능하며 EF의 AC는 EF가 생성될 당시에 정의된다.

STARCOS에서는 16가지 서로 다른 상태를 정의하고 있다. 상태전이를 일으키는 명령어는 실체인증에 관련된 명령어로 VERIFY PIN, VERIFY AND CHANGE, EXTERNAL AUTHENTICATE 및 MUTUAL AUTHENTICATE 가 있다. 실체인증 관련 명령어를 수행하는 과정에서 암호 키를 사용하기 때문에, 암호 키 정보를 기록하고 있는 암호 키 레코드는 상태전이가 일어날 때 중요정보로 이용된다. 상태전이를 일으키기 위하여 필요한 정보는 암호 키 레코드와 접근통제 값(Access Control Value : ACV)이며 ACV에는 다음과 같은 정보들을 가지고 있다.

- 접근조건
  - 스마트카드 동작 초기상태
  - 상태 및 접근조건 비교 연산자 : =/</≥/≠
  - 현재상태 참조
  - SECM 플래그(Secure Messaging Flag)
- 스마트카드 진행 상태(consecutive state)

STARCOS에서의 명령어 수행동작은 일반적으로 다음과 같은 일련의 순서를 거쳐서 이루어진다. ① MF나 DF의 현재상태(current state)에서의 접근조건을 비교한 후 접근조건이 만족되면 ② SECM 모드를 체크한다. 그리고 ③ 인증 데이터를 이용하여 검증하여 인증이 성공되면 ④ 스마트카드 현재 진행상태(consecutive state)를 설정한다. 예를 들어 EF의 읽기 및 쓰기 명령어를 수행하기 위하여 그림3과 같은 일련의 동작들이 일어나야 한다. DF의 상태를 전이시키기 위해서는 스마트카드 자체를 스마트카드가 DES 암호 키를 이용하여 인증하여야 하고 인증 결과에 따라 상태전이가 일어나면 DF에 있는 응용프로그램에서는 PIN 검증만으로 응용프로그램을 동작할 수 있도록 설정하였다.

이렇게 설정된 동작환경을 갖추기 위하여 필요한 정보들은 MF-ISF와 DF-ISF에 저장되어 있다. 응용프로그램이 동작하는 DF는 EF내에 응용프로그램의 데이터를 포함하고 있으며 DES 암호기법을 이용한 외부실체 인증이 성공한 후에 EF에 대한 데이터를 읽을 수 있다. EF의 데이터 영역에 데이터를 기록하기 위하여서는 PIN 검증을 하여야 하는데 STARCOS는 PIN 검증을 위한 전제조건으로 DES 검증이 성공적으로 완료된 후에만 PIN 검증

수행이 가능하도록 보안조건을 설정해 놓고 있다.

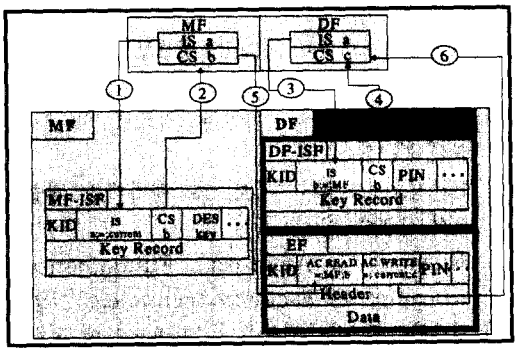


그림 3 STARCOS 접근통제 모델

1) 카드 접촉 : 스마트카드에 전원이 들어오면 자동적으로 MF가 선택되고 MF와 DF의 초기상태가 모두 'a'로 설정된다.
2) 실체인증 : EXTERNAL AUTHENTICATE 명령어를 수행하기 위하여, 먼저 GET CHALL- ENGE 명령어를 통하여 카드에서 생성한 난수를 터미널에서 암호화하여 다시 카드로 전송한다. 이때 난수 암호화에 이용되는 DES 키는 스마트카드의 MF에 저장되어 있는 암호 키와 동일한 암호 키여야 하며 스마트카드 시스템 구축 시에 터미널에 안전하게 저장하여야 한다. 터미널에서 암호화한 난수 값과 더불어 KID를 EXTERNAL AUTHENTICATE 명령어를 통해 스마트카드로 전송하게 되면 스마트카드는 KID로 식별할 수 있는 MF-ISF에 저장되어 있는 암호 키를 이용하여 암호화된 난수를 복호화 하여 이전 단계에서 카드자체에서 생성한 난수 값과 일치하는 지를 검사하여 인증 과정을 마치게 된다. 스마트카드는 MF-ISF에 저장되어 있는 암호 키를 사용하기 전에 암호 키에 대한 접근조건으로 MF의 현재 초기상태를 검사한다. MF-ISF에 저장되어 있는 접근조건과 현재 MF의 초기상태를 비교하여 암호 키에 대한 접근허가 여부를 결정한다.(그림 ①) 이렇게 인증이 성공하면 초기상태로서의 'IS = a'가 현재 진행상태 'CS = b'로 변경된다. (그림 ②)
3) DF 선택 : SELECT 명령어를 수행하면 스마트카드의 DF가 선택된다. 선택된 DF의 현재상태는 자동적으로 초기상태 ' IS = a'로 재초기화 된다.
4) PIN 검증 : VERIFY 명령어가 스마트카드로 전송되면서 PIN과 KID 정보가 같이 전송된다. STARCOS는 PIN을 검증하기 이전에, ISF에 저장되어 있는 PIN에 대한 접근허가를 받기 위하여 MF의 현재 진행상태가 접근조건을 만족하는 지를 검사한다. 즉 MF의 현재 진행상태가 'b'로 설정되어 있는지를 검사한 후, ISF에 저장되어 있는 PIN과 전송 받은 PIN이 일치하는 지를 검증한다.(그림 ③) PIN 검증이 성공적으로 완료되면 현재상태 DF의 진행상태를 'c'로 설정한다. (그림 ④)
5) EF의 데이터 읽기(그림 ⑤) : DF가 선택된 이후 DF에 속한 EF의 데이터에 READ 명령어를 통하여 접근할 수 있다. 접근조건 READ는 MF의 현재상태가 'b'로 설정되어 있는지 검증하는 것이다. 접근조건이 만족되면 READ 명령어에 대한 응답으로 EF의 데이터를 전송한다.
6) EF의 데이터 쓰기(그림 ⑥) : UPDATE 명령어를 수행하기 위하여 EF의 접근조건 WRITE를 만족시키기 위한 PIN 검증을 성공적으로 마치면, EF에 데이터를 overwrite 할 수 있다. UPDATE 명령어를 수신하면 DF의 현재상태가 접근조건 WRITE에서 명시한 상태를 만족하는지 검사하고 검사가 성공적으로 완료되면 UPDATE 명령어에 같이 수반되어 전송된 데이터를 EF에 overwrite 할 수 있다.

V. 결 론

생활의 많은 부분이 인터넷 세계로 자리를 잡아가는 시점에서 스마트카드는 중요한 역할을 수행할 수 있는 도구이다. 소형 컴퓨터의 능력을 가진 신용카드 크기의 보안장치이므로 휴대하기 간편하다는 점이 가장 큰 이점으로 부각되고 있다. 우리의 생활과 가장 밀접한 금융거래, 화폐, 출입통제 신분카드 등을 사이버 세계에서 구현하기 위한 수단으로 많은 인터넷 서비스 업체들이 스마트카드를 채택하고 있다. 최근 공개키 인증서를 활용하기 위한 인증 서비스가 국내에서도 제공됨에 따라 스마트카드의 이용

이 일반 사용자에게까지 실제적으로 자리잡을 수 있을 것으로 보인다. 보안시스템의 개념이 아직 일반 사용자들에게까지는 이해되지 못한 상태에서 이용환경만을 조성한다면 사이버세계에 잠재하고 있는 보안위협을 더욱 가중시킬 수 있다. 본 문에서는 스마트카드가 가지는 보안성을 이해하고자 스마트카드의 보안구조를 살펴보았다. 그리고 스마트카드 데이터 파일을 보호하기 위하여 구현하는 접근통제 모델을 분석하여 보안장치로서의 스마트카드를 이해하고자 하였다. 스마트카드의 보안구조는 보안속성, 보안상태 및 보안 메커니즘으로 구성되며 보안상태와 보안속성 정보를 기초로 하여 접근통제 메커니즘을 구현할 수 있다. 스마트카드 기술의 발달로 다기능 스마트카드가 다양한 응용서비스를 제공하게 되며 이와 더불어 개방형 구조의 스마트카드는 카드 발급 이후에도 새로운 응용프로그램을 로딩하여 설치할 수 있는 post-issuance application 기능을 지원한다. 여러 가지 응용서비스가 하나의 스마트카드에서 제공되는 환경에서 응용서비스간의 독립성을 유지하기 위하여 스마트카드 내부 파일에 대한 접근통제는 더욱 중요한 보안기능으로 제고되어야한다.

참 고 문 헌

[1] W.RANKL & W.EFFING, SMART CARD HANDBOOK, 1997

[2] ISO 7816-4 Interindustry commands for interchange, 1996

[3] ISO 7816-8 Security related inter-industry commands(draft)

[4] ISO 7816-9 Additional interindustry commands and security attributes (draft)

[5] Giesecke & Devrient GmbH, STARCOS S 2.1, 1996.10

[6] 한국정보보호센터, 전산망 정보보호 -접근통제 기술-, 1996.12

[7] 한국정보보호센터, 침입차단시스템 평가기준 해설서, 1998.5

[8] 한국정보보호센터, 정보보호 평가기준 개발보고서, 1999.12

[9] Edward G. Amoroso, "Fundamentals of computer security technology",1993

[10] 김태훈, 김승주, 원동호, "스마트카드에 적합한 효율적인 인증 모델", 한국통신학회 하계종합학술발표회 논문집 상권, pp 605 ~ 608

[11] 원동호, "IC 카드 보안" 발표자료

[12] 한국전자통신연구소편, "현대암호학", 한국전자통신연구소, 2장, 7장

[13] Morrie Gasser, "Building a Secure computer system", 1988

[14] Mike Hendry, "Smart Card Security and Application", 1999

[15] VISA,"Integrated Cirucuit Chip Card Security Guidelines",1997.4

[16] EMV '96 Integrated Circuit Card Specification for Payment Systems

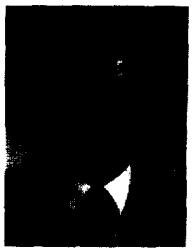
[17] VISA Open Platform Specification 2.1, 1999

[18] Ross Anderson, Markus Kuhn, "Low Cost Attacks on Tamper Resistant Devices"

[19] 한국정보보호센터, 정보보호뉴스 5월호, 2000.5

〈著者紹介〉

권 현 조(Hyun-Jo Kwon)
1997년 2월 : 성균관대학교 정보공학과 졸업
1997년 1월~1997년 7월 : (주)나라계전 기술연구소 연구원
1997년 7월~현재 : 한국정보보호센터 연구원
2000년 8월 : 성균관대학교 정보통신대학원 정보통신공학과 졸업 석사
〈관심분야〉 암호 응용분야, 스마트카드, 정보보호시스템 평가기준



원 동 호 (Dong-Ho Won)
1976년 : 성균관대학교 전자공학과 졸업
1978년 : 성균관대학교 전자공학과 석사
1988년 : 성균관대학교 전자공학과 박사
1978년~1980년 : 한국전자통신연구소 전임 연구원
1985년~1986년 : 일본 동경공대 객원연구원
1992년~1994년 : 성균관대학교 전산소장
1995년~1997년 : 성균관대학교 교학처장
1996년~1998년 : 국가정보화 추진위원회 자문위원
1990년~1999년 : 한국통신정보보호학회 이사
1998년~1999년 : 성균관대학교 정보통신기술연구소장
1982년~현재 : 성균관대학교 전기전자 및 컴퓨터 공학부 교수
1999년~현재 : 성균관대학교 전기전자 및 컴퓨터 공학부장
(겸)정보통신대학원장, 한국통신정보보호학회 부회장
〈관심분야〉 암호이론, 부호이론