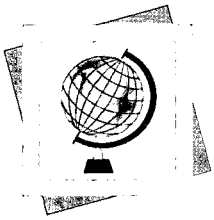


전자선거에서의 스마트카드 보안 위협요인 분석

박해룡 · 주학수 · 전길수
(한국정보보호진흥원)

목 차

1. 서 론

중앙선거관리위원회(이하 선관위)는 2004년 11월, 전자투표 사업추진단을 설치하여 정보화 전략계획을 수립하고, 2005년 5월부터 전자투표기 및 인터넷 투표시스템 개발에 들어간다고 밝혔다. 선관위는 전자투표시스템의 도입을 위해서 해킹이나 시스템 다운 등의 비상사태에 대비해 분산된 방식의 중앙처리시스템을 구축하고 선거기간동안 모든 시스템에서 안정적으로 자료가 실시간으로 저장될 수 있는 백업시스템을 개발 중이다. 또한, 중복투표 방지를 위한 통합선거인명부 확인시스템과 키오스크(Kiosk)를 사용하는 전자투표시스템, 실시간 검증이 가능하고 개표상황의 실시간 체크와 후보자 자신이 자신의 득표에 대한 역추적이 가능하도록 하는 시스템도 개발 중에 있는 것으로 알려졌다. 이런 전자투표시스템은 투표자 인증이 가능한 스마트카드를 도입하거나 인터넷 등 원격으로 투표가 가능한 시스템을 도입하여 운영될 계획이다[1].

1974년 프랑스의 Roland Moreno가 스마트카드에 대한 특허를 출원한 후, 세계 여러 나라에서는 마그네틱 카드보다 보안 및 저장 공간이 더 좋은 스마트카드 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, 전자투표, 전자주민증, 공과금 납부, 병원 업무, 전자지갑 등 일상적인 생활에서 스마트카드를 안전한 도구로 사용하고 있다.

그러나, 스마트카드가 갖는 물리적 안전성에 대한 위협 및 최근에 대두된 부채널 공격(Side Channel Attack)등으로 인해 스마트카드에 저장된 비밀키에 대한 정보를 알아 낼 수 있는 다양한 공격기법들이 나타나고 있다. 또한, 스마트카드를 이용함으로써 안전한 시스템을 설계할 수 있는 것은 사실이지만 단순히 시스템에 스마트카드를 사용한다고 하여, 시스템을 안전하게 만드는 것은 아니다. 이에 본 고에서는 전자선

거에서 사용되는 스마트카드의 역할을 알아보고 스마트카드 안전성 관련 기능 및 공격기법을 분석하고자 한다. 또한, 전자투표시스템에서 스마트카드의 역할은 정해졌지만 스마트카드 관련 세부 프로토콜 등은 정해지지 않은 바 본 고에서는 기존 스마트카드를 활용한 서비스를 기반으로 전자투표시스템에서 스마트카드 관련 사항을 재구성하였다.

2. 국내 전자선거 시범시스템 분석

2.1. 스마트카드를 활용한 본인확인

선관위는 유권자의 개인정보가 담겨있는 통합선거인명부를 온라인화하되 전자투표기는 오프라인으로 구성하여 유권자가 전국의 어느 투표소에서든 투표가 가능하도록 할 계획을 수립했다. 즉, 도시지역의 경우 기존의 투표소 외에 선거인의 왕래가 잦은 곳(백화점, 시장, 공단 입구, 전철역 입구, 유원지 입구, 고속도로 휴게소 등)에 투표소를 설치해, 선거인이 어디서나 투표를 할 수 있게 된다.

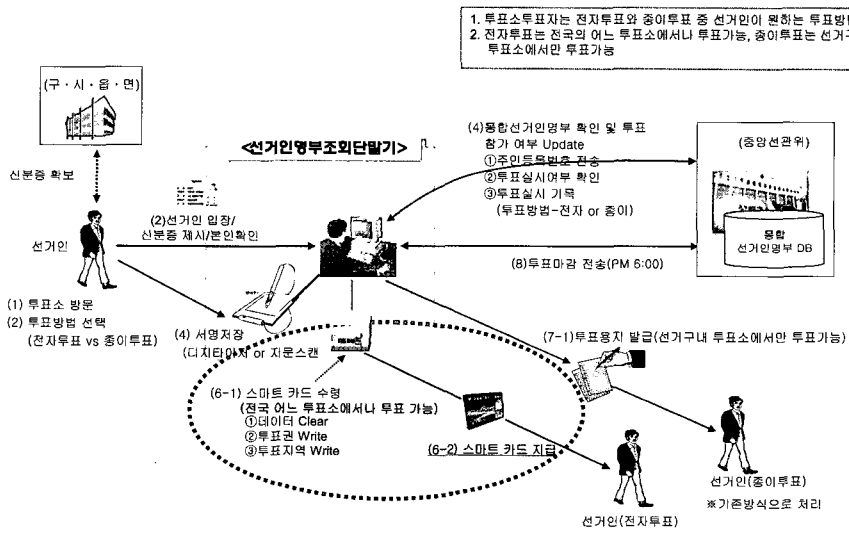
선거인명부 확인시스템에서 선거인의 본인여부 확인 절차를 거치면, 스마트카드에 선거인이 속한 해당 선거구의 투표용지를 화면 상에 띄우는 기능과 1회 투표를 할 수 있는 기능이 동시에 부여되고, 선거인은 해당 스마트카드를 받아 전자투표기에 입력하여 투표를 진행하게 된다. 전자투표기는 전국의 선거구 투표용지를 스마트카드의 지시대로 스크린에 띄우는 기능과 투표결과를 선거구별/후보별로 기억하는 장치가 설비되어 있다.

현재 계획으로 2008년도에 기존의 종이투표 방식과 터치스크린에 의한 전자투표방식을 병행하여 선거인이 편리한 방식을 투표소에서 선택하여 투표할 수 있도록 하고 있으며, 선거인명부 확인 시스템과 터치스크린 방식의 전자투표기는 상호 독립적으로 운영되어 오프라인 상태임을 가정한다. 오프라인으로 운영됨에 따라, 전자투표기 상호 간 또는 중앙집계시스템과는 독립적으로 운영된다.

3. 전자선거에서의 스마트카드 보안기능

3.1. 스마트카드에서의 인증

스마트카드에서의 인증방법은 크게 스마트카

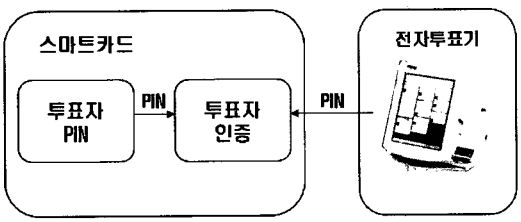


(그림 1) 국내 전자선거 시범시스템 흐름도[2]

드에 접근하려는 투표자의 신분을 증명하는 투표자 인증, 스마트카드와 전자투표기 간의 인증 방식인 실체인증으로 분류할 수 있다.

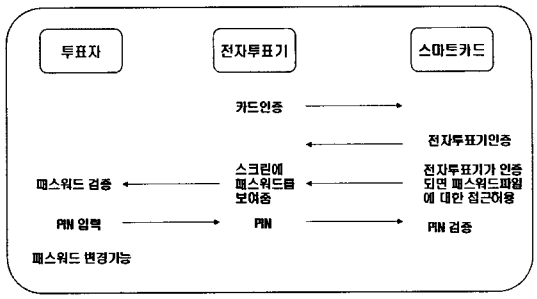
3.1.1 스마트카드에서의 투표자 인증

스마트카드에서 사용자 인증 방법으로 PIN 또는 패스워드를 이용하는 방법이 가장 많이 사용되고 있으므로, 전자투표시스템에서 스마트카드를 활용하여 투표자 인증을 수행하는 방식을 설명하고자 한다. PIN은 보통 4자리의 숫자(0~9)로 사용되는데, 그 이유는 현재 사용되는 전자투표기에 숫자로 구성된 Keypad(키패드)만이 장착되어 있으며 투표자들이 기억하기 쉽기 때문이다[3]. 보통 PIN이 전자투표기의 키패드를 통해 입력되면 그 정보는 스마트카드로 보내어지게 되고 스마트카드는 내부에 저장된 PIN정보와 비교해서 그 결과를 전자투표기에 알려주는 방식으로 투표자를 인증하게 된다.



(그림 2) PIN을 이용한 투표자 인증

보통 PIN의 입력 시, 공격자가 간섭(Tampering) 공격을 함으로써 PIN 정보를 알아낼 수 있기 때문에 PIN정보는 암호학적 보호기능을 갖춘 "PIN Pad[1]"에 의해 암호화되어 전송된다. PIN을 이용한 방식은 전자투표기가 투표자를 인증하는 방식으로 사용되지만, 투표자가 전자투표기를 인증하는 방법도 필요하다. PIN방식과 함께, 투표자만이 아는 패스워드를 스마트카드에 저장하는 방식이 결합되어 사용될 수 있다. 여기서 스마트카드 운영체제(OS)는 스마트카드가 전자투표기를 인증한 후에만 전자투표기가 패스워드 파일을 읽을 수 있는 접근권한을 허락한다. 전체 방식은 다음과 같이 구성된다.



(그림 3) PIN과 패스워드를 이용한 투표자와 전자투표기의 상호인증

투표자가 스마트카드를 전자투표기에 넣으면 스마트카드와 전자투표기 사이의 상호 인증이 가장 먼저 일어나고, 이 상호 인증이 성공하면 스마트카드는 전자투표기에게 투표자의 패스워드 파일에 대한 읽기 권한을 허용한다. 전자투표기는 패스워드 파일을 스크린을 통해 투표자에게 보여주고 투표자는 자신의 패스워드가 맞는지를 검증함으로써, 전자투표기를 인증하게 된다. 이와 같은 과정이 성공하면, 투표자는 자신의 PIN정보를 입력하여 투표자 인증과정을 수행한다.

3.1.2. 스마트카드의 실체 인증

스마트카드와 전자투표기 간의 인증(실체인증)방식으로는 공개키 암호알고리즘을 이용한 인증, 대칭키 암호알고리즘을 이용한 인증 등이 있다.

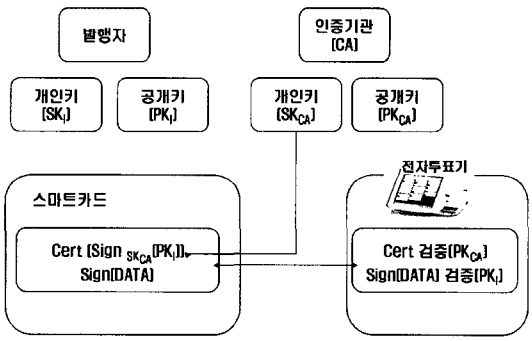
가. 공개키 암호알고리즘을 이용한 인증

공개키 암호알고리즘을 이용한 인증방식은 인증기관(CA)으로부터 발급받는 공개키 인증서

1) EMV2000 표준에서는 PIN Pad를 Tamper-evident 장치로 규정하고 있으며, PIN을 표준 ISO 9564-1에 따라 암호화하여 스마트카드로 전송함

(Certificates)를 스마트카드와 전자투표기에 설치하여 인증을 수행하는 방식으로 구성된다. 공개키 암호알고리즘을 이용하는 인증방식은 EMV 표준[4]에 따라, 정적(Static) 인증과 동적(Dynamic) 인증으로 분류할 수 있다.

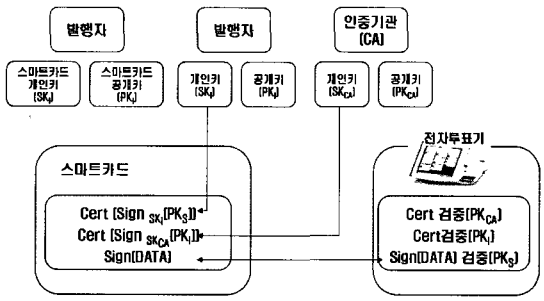
정적 인증 방식의 경우, 발급기관이 스마트카드를 개인화(Personalization)할 때 스마트카드에 전자서명 값이 카드번호, 투표자 이름, 주소 등과 같이 저장되게 된다. 스마트카드가 전자투표기에 삽입된 후 발행자의 공개키에 대한 인증기관의 서명값과 데이터에 대한 발행자의 서명값이 전자투표기로 전송되면 전자투표기는 미리 분배되어 있는 CA와 발행자의 공개키를 사용하여 서명값들을 검증함으로써, 스마트카드에 대한 인증을 하게 되는 방식이다. 이 방식은 단지 저장된 값만을 이용하므로 스마트카드 내에서의 공개키 암호 연산이 필요 없다는 장점이 있는 반면, 인증할 때마다 동일한 인증 정보를 사용하여 replay attack에 취약한 단점이 있다.



(그림 4) 스마트카드의 정적(Static) 인증방식

동적 인증의 경우, 스마트카드 자체의 공개키와 개인키를 갖고 있으며 투표 시 전자투표기가 생성한 난수값을 포함한 동적인 정보가 전자투표기로부터 전송되는 것으로부터 시작된다.

스마트카드는 이 동적인 정보에 스마트카드의 개인키로 서명한 뒤 스마트카드의 공개키에 대한 발행자의 서명값, 발행자에 대한 CA의 서명값을 전자투표기에 전송하면 전자투표기는 미리 분배되어 있는 공개키들로 서명들을 검증함으로써 스마트카드에 대한 인증을 하게 된다. 이 방식은 스마트카드에 암호(서명)연산을 수행할 수 있는 프로세서가 탑재되어 있어야 하며, 정적 인증과는 달리 매 인증마다 변하는 데이터를 사용하기 때문에 replay attack에 안전하다는 장점이 있다.



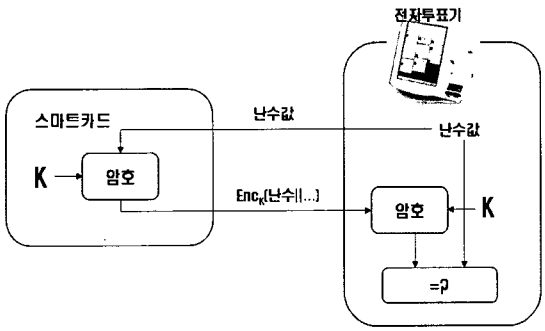
(그림 5) 스마트카드의 동적 인증방식

나. 대칭키 암호알고리즘을 이용한 인증

대칭키 암호알고리즘을 이용하는 인증방식은 단방향 인증과 상호 인증방식으로 분류할 수 있다. 단방향 인증의 경우, 스마트카드와 전자투표기가 동일한 키를 갖고 있으며 전자투표기에서 난수를 생성하여 스마트카드에 전송하면, 스마트카드는 난수값을 비밀키로 암호화(혹은 MAC) 값을 계산하여 전자투표기에 전송한다. 전자투표기는 같은 비밀키로 암호화된 값을 복호화하여 난수값이 유효한지 검증함으로써 스마트카드를 인증하는 방법이다.

상호 인증의 경우, 단방향 인증을 두 번 행함으로써 스마트카드가 전자투표기 간의 상호 인증을 수행하는 방법이다. 전자투표기는 카드 번호로부터 스마트카드의 세션키를 계산하여야 하기 때문에 카드번호 및 난수값을 스마트카드에 요청하고 자신도 난수값을 생성한다. 스마트카드로부터 받은 난수값과 자신이 생성한 난수값을 세션키로 암호화하여 결과값을 스마트카

드에게 보내고, 스마트카드는 전자투표기로부터 받은 결과값을 복호화하여 전자투표기의 난수값을 알아낸다. 이 때 스마트카드는 전자투표기의 인증이 끝나게 되고, 스마트카드는 전자투표기의 난수값과 자신의 난수값을 암호화하여 보내면 전자투표기는 스마트카드로부터 받은 결과값을 복호화하여 자신의 난수값과 확인함으로써 스마트카드를 인증하게 된다.



(그림 6) 스마트카드에서의 단방향 인증방식

3.2. 스마트카드에서의 접근통제 및 데이터 무결성/기밀성

3.2.1 접근통제

스마트카드의 보안기능 중 저장장치의 안전한 수단으로서 스마트카드가 가져야 할 핵심기능은 접근통제(Access Control) 기능이며, 데이터를 보호하기 위한 메커니즘들 중의 하나다. 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 1〉 보안정책 분류

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

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

■ ISO/IEC 7816-Part 9

ISO 7816-Part 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 방법으로서, 접근행렬(Access Matrix)에서 각 열의 필드에 접근권한이 설정된 행의 주체들로 표현한다.

■ MPCOS-EMV

MPCOS-EMV 카드는 파일 접근 시 파일 보호를 위해 비밀코드 또는 키들을 사용한다. 비밀코드는 요소파일에 저장되고 비밀코드 요소파일이라 불린다. 마스터파일과 각 전용파일은 하나의 비밀코드 요소파일을 가지고 있다. 전자투표기는 스마트카드의 요소파일 내에 저장된 데이터에 접근하려 할 때, 스마트카드는 요소파일 접근 조건에 저장된 값과 인증 레지스터에 저장된 값을 비교한다.

3.2.2 데이터의 기밀성/무결성

기밀성(Confidentiality)/무결성(Integrity)은 데이

터를 보호하기 위한 기능 뿐 아니라 앞에서 설명한 인증, 접근통제 등 다양한 기능에 필요한 기능이다.

■ 기밀성

기밀성이란, 정당한 권한이 부여된 투표자만이 데이터의 내용을 파악할 수 있게 하는 것으로서, DES, 3-DES 등의 블록암호알고리즘이 사용된다.

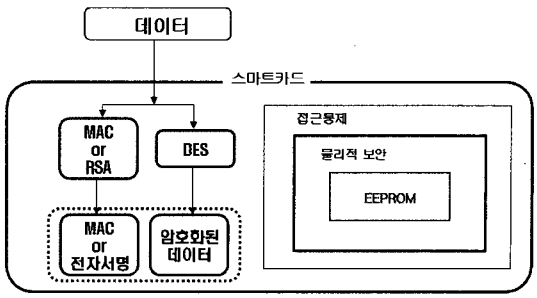
■ 무결성

데이터가 불법적으로 위조 또는 변조되었는지를 검출하는 것으로, 스마트카드의 메모리에 저장된 데이터를 인가되지 않은자가 임의로 변경할 수 없어야 한다. 무결성 기능을 위하여 메시지 인증 코드(Message Authentication Code)나 해쉬알고리즘 또는 전자서명이 사용된다.

스마트카드에서 보호해야할 데이터는 메모리에 저장되어있는 저장 데이터와 전자투표기와의 통신에 사용되는 전송 데이터로 구분지을 수 있다. 각각의 데이터에서 기밀성/무결성 기능은 다음에서 설명하기로 한다.

가. 저장 데이터

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

나. 전송 데이터

스마트카드의 전송데이터의 무결성과 기밀성 기능은 "Secure Messaging"기능이라고도 하며, 통신사에서 가해질 수 있는 각종 위협에 대한 방어수단이라고 생각할 수 있다[5]. 스마트카드와 전자투표기 사이의 데이터 전송은 스마트카드의 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. 이에따라, 안전한 전송을 위해서 전송되는 데이터의 일부 또는 전체에 대한 인증, 필요하다면 기밀성이 보장되어야 한다. 안전한 전송 프로토콜을 시작하기 전에 우선 스마트카드와 전자투표기 사이에 키 공유가 이루어져야 한다. 키 공유방법으로는 RSA, DH, ECDH 방식들이 사용된다. 스마트카드와 전자투표기 사이에 키 공유가 이루어진 후 데이터의 전송방법에 대하여는 ISO/IEC 7816-4에서 정의하고 있으며, 추가적인 기능은 ISO/IEC 7816-8에서 정의하고 있다.

3.3 스마트카드에서의 키관리

스마트카드에서의 키관리란 스마트카드의 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 암호알고리즘을 구현하는 모든 암호모듈에 의해 만족되는데, 대칭키와 개인키는 인가되지 않은 노출이나 수정으로부터 보호되어야 하며, 공개키는 인가되지 않은 수정과 치환에 대비하여 암호모듈 내에 보호되어야 한다.

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

■ 유도키(Derived Key)

전자투표기와 달리 스마트카드는 공격자가 가져가서 상당한 시간과 노력을 투자하여 다양한 공격들을 수행할 수 있다[자세한 공격기법들은 4절을 참조]. 따라서 스마트카드가 마스터키를 가지고 있지 않다면, 인증되지 않은 접근으로부터의 영향을 최소화 하기 위해서 마스터키로부터 얻어진 유도키(Derived Key)들만을 스마트카드 내에 저장하도록 한다[3]. 유도키는 암호알고리즘에 의해 생성되어지며, 입력값은 마스터키와 스마트카드의 식별정보를 사용하며 블록암호알고리즘으로는 보통 DES 혹은 3-DES를 보통 사용한다.

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

■ 동적키(Dynamic Key)

일명 임시용 키((Temporary Key) 혹은 세션키(Session Key)로 언급되며, 안전한 데이터 전송을 위해 사용된다. 동적키(세션키)를 생성하기 위해서는 두 객체 중 한 객체가 먼저 특정 세션에 유일한 난수값을 생성한 뒤 다른 객체에게 전달하는 과정으로 구성되는데, 대칭키 암호알고리즘을 사용하는 방식과 공개키 암호알고리즘을 사용하는 방식으로 구분할 수 있다.

- 대칭키 암호알고리즘 방식을 사용하여 동적키(세션키)를 교환하는 경우, 한 객체에 의해 난수가 생성되어 평문의 형태로 다른 객체에 전달된다. 스마트카드와 전자투표기는 유도키(derived key)를 사용하여 난수값을 암호화하면 새로운 세션에 유일하게 사용될 동적키가 생성된다. 과정은 다음과 같다.

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

- 공개키 알고리즘 방식을 사용하여 동적키(세션키)를 교환하는 경우, 난수값으로부터 메시지 암호화에 사용될 동적키를 생성하고, 동적키의 교환을 RSA와 같은 공개키 암호알고리즘을 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[6]의 키 관리 방법에 대한 가이드라인과 "스마트카드 핸드북[3]"을 참조하여 스마트카드에서의 키관리 시 유의점에 대해 정리하고자 한다.

■ 키생성(Key Generation)

마스터키, 키암호용키(KEK)[2]와 PIN 암호용키는 최소 112비트(3-DES) 정도의 안전도를 가

2) 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.

져야 한다. 마스터키는 물리적 보호모듈(TRSM : Tamper Resistant Secure Module) 안에서 생성되어야 하며 물리적 보호모듈을 벗어나는 경우, 평문의 형태로 존재해서는 안된다[6]. 암호시스템의 구현 시 부적절한 난수 혹은 의사난수를 사용함으로써, 시스템이 공격당할 수 있는 문제점들[7,8]이 있기 때문에 암호키를 생성하기 위해 사용되는 난수는 안전해야 한다(안전한 난수, 의사난수 생성방법에 대해서는 [9]를 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[6].

■ 키의 사용 및 사용기간 제한

파일 시스템을 사용하는 스마트카드에서는 키들을 개인파일(private file)에서 관리하는데, 키를 사용하기 위해 파일로 접근하는 것은 투표자의 신분을 증명하기 위해 입력된 PIN이나 생체정보를 검증한 후에야 제공되어야 한다[6,10].

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) 사용방식들이 있다[5].

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 키들이 사용되어야 한다[3].

■ 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[3].

■ 키 버전(Key versions)

일반적으로 단 하나의 키를 생성해서 전체 스마트카드의 사용기간동안 이용하는 것은 바람직하지 않다. 따라서 현재 모든 시스템에서는 새로운 키를 생성하여 교환하는 것이 가능하도록 되어있다. 이 새로운 키의 생성은 키가 손상되거나 혹은 주기적인 간격으로 수행될 수 있다. 그러므로 스마트카드를 회수하지 않고 시스템의 모든 키를 새로운 키로 교환하게 된다. 마스터키는 전자투표기와 시스템의 가장 안전한 레벨로 보관되어야 하기 때문에, 안전한 데이터 통신을 위해서는 아직 알려지지 않은 새로운 버전의 마스터키가 필요하다.

4. 전자선거에서의 스마트카드에 대한 공격기법

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

이에 따라, 이 절에서는 스마트카드에 관련된 공격기법들을 알아보기 위해 스마트카드와 응용환경에서의 객체들 사이에 일어날 수 있는 공격모델들[11]을 정의하고, 스마트카드 자체에 대한 공격기법들을 조사하여 정리하고자 한다.

4.1 스마트카드에서의 공격모델

스마트카드의 공격주체란 스마트카드 응용시스템을 구성하는 모든 주체(즉, 투표자, 전자투표관리자 등)를 의미하며 이들은 카드에 대한 공격가능성을 가지고 있다.

먼저 스마트카드와 관련된 참여자는 투표자, 전자투표기, 전자투표관리자, 카드발행자, 카드제조업자, 소프트웨어 제조업자 등으로 분류할 수 있다.

■ 투표자

스마트카드를 활용하여 투표를 하는 참여자다.

■ 전자투표관리자

스마트카드 내부에 있는 데이터 통제 등의 전자선거 전반적인 업무를 수행하는 참여자다.

■ 전자투표기

투표자가 컴퓨터 시스템을 이용하는 위치로 최종 단말 위치에 연결되어 동작되는 장치로 스마트카드와 투표자를 연결시켜준다. 전자투표기는 스마트카드의 모든 입/출력(I/O)을 통제한다.

■ 카드발행자

스마트카드를 발행하는 참여자로서 스마트카드에 탑재되는 운영체제와 초기의 스마트카드에 저장되는 데이터를 제어한다.

■ 카드제조업자

스마트카드를 생산하는 참여자.

■ 소프트웨어 제조업자

스마트카드에 탑재된 소프트웨어를 제작한 참여자.

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

■ 투표자 또는 전자투표관리자에 대한 전자투표기 공격

투표자가 자신의 스마트카드를 전자투표기에 삽입할 때, 공격자가 전자투표기를 조작하여 공격하는 방법이다. 이러한 공격을 방지하기 위해 스마트카드에 탑재된 소프트웨어로 하여금 위조된 전자투표기에서 투표하는 것을 제한하는 방법이 사용될 수 있다.

■ 전자투표기에 대한 투표자의 공격

이 공격은 스마트카드와 전자투표기 사이의 프로토콜을 공격할 목적으로 스마트카드에 탑재된 소프트웨어 및 스마트카드를 위조하는 공격을 말한다. 이러한 공격을 막기 위해 스마트카드의 물리적인 면을 위조하기 어렵게 만들고 있다[3].

■ 전자투표관리자에 대한 투표자의 공격

스마트카드에 저장된 데이터에 대한 투표자의 공격을 말한다. 스마트카드에 저장된 데이터를 알아내기 위한 공격방법으로는 Reverse-Engineering, Fault Analysis, Power 혹은 Timing analysis와 같은 Side Channel attack 등이 있다.

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

■ 카드발행자에 대한 투표자의 공격

이 공격은 카드발행자가 스마트카드 내부에 시스템의 사용을 인가하는 정보를 저장하였을 경우, 이 정보 또는 프로그램의 무결성 또는 인증에 대한 공격들을 말한다.

■ 소프트웨어 제조업자에 대한 투표자의 공격

악의적인 투표자가 자신에게 발행되는 스마트카드에 새로운 소프트웨어를 설치하는 공격을 말한다.

■ 투표자에 대한 전자투표관리자의 공격

이 공격은 악의있는 전자투표관리자를 가정하는 것으로, 보통 투표자의 프라이버시를 침해하는 공격을 말한다. 스마트카드로 인해 투표자의 익명성을 제공하도록 설계되어야 하는데 시스템의 잘못된 설계 및 공격은 투표자의 정보를 발행자가 모을 수 있게 한다.

■ 전자투표관리자에 대한 제조업자의 공격

제조업자의 스마트카드구현 시 데이터 정보(예를 들어, 어플리케이션 키 정보 등)를 알아내기 위한 의도된 공격방법으로, 난수생성기의 사용으로 인한 공격방법[7], Kleptographic attacks [8, 9], Subliminal Channels[10] 등이 있다.

4.2 스마트카드 자체에 대한 공격기법

먼저 안전성을 분석하기 위해 스마트카드 자체를 공격하는 공격자의 레벨을 <표 2>와 같이 3단계로 구분하기로 한다.

제어 단계의 회로에서의 보안 장치는 무시하고, 스마트카드나 다른 칩 레벨의 보안 프로세서에 저장되어 있는 암호키를 복구하는데 공격을 집중하도록 공격모델을 설정하도록 하자.

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

〈표 2〉 스마트카드 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 자본과 전문 기술을 가진 전문가 팀 • 정교한 공격을 설계하고 가장 최신 분석도구를 사용하여 시스템 분석 • 공격팀의 일부로 Class II의 공격자들을 이용함

4.2.1 침입형 공격

침입형 공격은 스마트카드를 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.

■ 칩 분해단계

스마트카드의 칩은 1㎠ 크기로, 한쪽 면은 전자투표기와 접속하기 위해 노출되어 있으며, 반대쪽은 실리콘물질과 에폭시 수지로 덮여있다. 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(NHO_3) 몇 방울을 에폭시 합성수지 위에 떨어뜨리고,

칩의 일부가 보일 때까지 몇 분간 기다린다. 질산이 제거한 에폭시 합성수지가 다시 단단해지기 전에 이것들을 아세톤에 씻어낸다. 이러한 과정을 몇 번 반복함으로 스마트카드로부터 칩을 분리할 수 있다.

■ 아키텍처 재구성 단계

스마트카드에 열과 화학처리로 칩을 분리한 뒤 고해상도 CCD 카메라와 연동된 광학현미경을 통해 칩 표면의 아키텍처 및 모듈 경계를 확대하여 재구성하는 단계다. 공격자는 CMOS VLSI 설계기술과 마이크로프로세서 기술에 전문적인 지식을 가지고 있어야 하나, 이런 지식들은 많은 문서를 통해서 손쉽게 구할 수 있다. 칩은 여러 개의 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 스마트카드를 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 채움으로써 표면에서 금속층 내부로 접속이 가능하게 하여, 칩 상의 두꺼운 메탈층과 폴리 실리콘 라인으로 구성된 보호층을 해독할 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 공격도구다.

4.2.2 준침입형 공격

침입형 공격은 칩을 완전히 분해하는데 반하여 준침입형 공격은 칩의 보호층을 제거하지 않고 칩의 표면에서 공격을 시행한다. 트렌지스터에 빛을 비춤으로써 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 알려져 있다면 EEPROM의 출력을 증폭하여 읽어낼 수 있다.

마지막으로, EEPROM이 정보를 읽고 쓰기 위해서 비교적 높은 전압이 필요하다는 점을 이용하여 EEPROM에 공급되는 전압을 조작함으

로 공격을 할 수 있다.

4.2.3 비침입형 공격

■ Timing Attack

암호화나 전자서명 등에서 입력되는 정보에 따른 연산 시간의 차이를 이용한 공격이다. 이 공격은 스마트카드의 PIN이 알려져 있거나, 공격자가 원하는 입력을 스마트카드에 넣을 수 있어야 가능하다.

■ Power Analysis

전력분석법은 스마트카드의 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

스마트카드의 프로세서가 동작하는 환경을 조절함으로 프로세서가 오작동을 하도록 하는 공격방법으로, 입력되는 전압의 크기 또는 주위의 온도를 조절하는 방법이다.

■ Differential Fault Analysis

DFA는 스마트카드 등이 열, 진동, 압력 등의 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 동작 중에 나타나는 현상을 분석에 이용한다. 그러므로, 오류가 발생하지 않도록 프로세서를 설계하고, 정상적인 환경이 아닐 경우 EEPROM의 정보를 초기화시키고, 스마트카드 연산 중에 나타나는 전자파나 전류의 소모량들을 일정하게 유지시키거나 랜덤화시키는 등의 과정으로 공격을 막을 수 있다.

5. 결 론

스마트카드기반 전자투표의 안전한 구축을 위해서는 스마트카드 자체에 대한 안전성과 전자투표를 구성하는 암호 논리의 안전성이 필요하다. 기본적으로 스마트카드 자체에 대한 안전성은 갖추어져 있다는 가정 하에 전자투표시스템의 세부 설계내역이 공개되면, 다음과 같은 전자투표에 사용되는 암호 논리의 안전성 분석이 필요할 것으로 판단된다.

■ 완전성

모든 유효 투표가 정확하게 집계되어야 한다는 것으로, 최종 집계에서 정당한 투표가 제거되는 일이 없어야 한다.

■ 건전성

부정한 투표자에 의해 선거가 방해되는 일이 없어야 한다는 것으로, 최종 집계에서 투표가 집계 되어 선거에 영향을 끼치지 않아야 한다.

■ 비밀성

모든 투표는 비밀로 이루어져야 한다는 것으로, 투표자의 투표결과는 비밀로 유지 되어야 한다.

■ 익명성

투표결과로부터 투표자를 구별 및 추적할 수 없어야 한다는 것으로, 투표자의 익명이 보장되어야 한다.

■ 단일성(이중 투표 불가성)

정당한 투표자가 두 번 이상 투표할 수 없다는 것으로 단지 한 번만 투표할 수 있어야 한다.

■ 적임성(선거권)

투표 권한을 가진 자만이 투표할 수 있는 것으로 투표가 허락되지 않은 자는 투표할 수 없어야 한다.

■ 공정성

투표에 영향을 미치는 것이 없어야 한다는 것으로 투표 중에 일부분 결과를 알게 되어 투표에 영향을 미치는 상황 등이 없어야 한다.

■ 검증성

선거 결과를 변경할 수 없도록 누구라도 투표 결과를 확인하여 검증해 볼 수 있어야 한다.

본 고에서는 스마트카드를 구성하는 암호논리로 기밀성, 무결성, 인증, 키관리 기술에 대해 살펴보았다. 안전한 데이터의 관리와 스마트카드 및 전자투표기의 인증을 위해서는 전자투표를 구성하는 기밀성, 무결성, 인증, 키관리 등이 잘 갖추어져 있어야한다. 또한, 스마트카드기반 전자투표에서는 데이터의 신속한 처리 및 투표자의 개인정보 보호도 중요한 문제다.

참고문헌

[1] 월간 <네트워커>, http://networker.jinbo.net/nw-news/show.php?docnbr=1155

[2] 대우정보시스템(주), "전자투표 및 전자서거시스템 구축을 위한 정보화 전략계획(ISP) 수립완료 보고서(요약본)", 중앙선거관리위원회, 2005. 05

[3] W. Rankl & W. Effing, "Smart Card Hand book : Second Edition", WILEY 2002

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

[5] 한국정보보호진흥원, "스마트카드 제품 평가기준 해설서", 2000.11

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

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

[8] Pavel V. Semjanov, "On cryptosystems untrust worthiness", Information Security center, St. Petersburg Technical University, 1996.

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

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

[11] 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.

저자약력

박 해 룡

1999년 전남대학교 수학과 이학사
2001년 서울대학교 대학원 수학과 이학석사
2000년~현재 한국정보보호진흥원 암호응용팀 연구원
관심분야 : 암호프로토콜, 키관리, 정보보호

주 학 수

1997년 고려대학교 수학과 이학사
1999년 고려대학교 대학원 수학과 이학석사
2001년 고려대학교 대학원 수학과 박사과정 수료
2001년~현재 한국정보보호진흥원 암호응용팀 연구원
관심분야 : 암호학, 공개키암호, 응용보안프로토콜, RFID/USN 정보보호

전 길 수

1991년 서강대학교 수학과 이학사
1993년 서강대학교 대학원 수학과 이학석사
1998년 서강대학교 대학원 수학과 이학박사
1998년~1999년 서강대학교 기초과학연구소 박사후 연구원
2001년~2001년 서강대학교 컴퓨터공학과 연구교수
2001년~현재 한국정보보호진흥원 암호응용팀장
관심분야 : 암호학, 정보보호, RFID/USN 정보보호