SM을 사용한 IC 카드의 인증 및 서명 프로토콜

도 신 호*0, 하 재 철*, 박 영 호**, 문 상 재*
*경북대학교 전자·전기 공학부, **상주 산업 대학교

Authentication and signature protocol using SM in IC-card system

Syn-Ho Do*0, Jae-Cheol Ha*, Young-Ho Park**, Sang-Jae Moon*
*School of Electronic and Electrical Eng., Kyungpook National Univ.
**Dept. of Electronic and Electrical Eng., Sangju National Poly. Univ.

요 약 문

본 논문에서는 SM을 사용한 IC 카드의 인증 및 서명 프로토콜을 제안한다. SM은 연산 처리 능력이 우수하고, 안전한 보조 장치로 단말 내부에 장착된다. 제안된 프로토콜은 Königs의 인증 방식, NIST의 ASACS, 그리고 UEPS와 비교하여 안전하고, 8비트 IC 카드에서 적합하게 개선하였다. 따라서 SM을 주민용 IC 카드의 단말에 장착하여 인증 및 디지탈 서명을 구현하는 방안을 제안한다.

1. 서 론

정보 산업의 기술 및 사용자 환경의 급속한 발전은 생활의 편의성과 다양성을 증대시키고 있다. 정보 인프라 구축 및 신정보 시스템으로의 교체는 일반인들의 정보 통신에 대한 신뢰도를 높이고 있다. 특히 복잡한 정보 사회에서 신속한 정보 처리와 개인 생활 정보의 보호를 위해 IC 카드가 주민등록증, 의료보험증, 은행 카드 등의 역할을 통합적으로 수행하게 되었다. 국내에서는 98년부터 7개분야 41가지의 정보가 이 주민 카드에 집적되어 실용화할 것으로 알려져 있다.

인증 및 디지탈 서명은 정보 보호 서비스 중에서 필수적인 요소라 할 수 있다. 이러한 서비스의 필요에 따라 국내에서도 디지탈 서명 방식의 표준을 추진 중에 있으며, 차세대 IC카드에서는 카드 자체의 계산 능력 향상으로 제공 될 수 있다. 하지만, 주민용 IC카드 정도의 수준에서는 멱승과 같은 고속 연산이 불가능하다. 그러므로 안전한 보호 장치 SM을 IC 카드 단말내에 장착하여 이를 구현하는 것이 과도기적 방법으로 적당하다. 이를 구현하기 위해서 사용자 인증, 카드 인증, 단말 인증이 요구 된다.

Königs의 인증 방식[1]과 NIST(the national institute of standards and technology)의 ASACS(the advanced smartcard access control system)[2] 그리고 UEPS(the universal electronic payment system)[3]같은 시스템에서는 불법적인 단말에 대한 단말 인증이 실패하여도 사용자는 이를 알 수 없으며, 카드와 단말간의 인증 이전에 사용자 인증이 일어나므로 불법적인 단말이 사용자의 패스워드를 녹취할 수 있다. 그 외에도, 이들 IC 카드 시스템은 비대칭 키 형태의 디지탈 서명 서비스를 제공하지 못하는 문제점을 가지고 있다.

본 논문에서는 현재 실용화 단계인 주민용 IC 카드 정도의 수준에서 디지탈 서명 서비스를 제공하기 위한 인증 및 서명 프로토콜을 제안한다.

2. IC 카드 시스템

IC 카드의 형태는 기존의 플라스틱 카드에 마이크로 프로세서나 메모리 등의 IC 칩을 내장하고 있다. 외부와의 접속 단자를 갖고있어, 마이크로 프로세서는 이 단자를 통하여 단말장치와 인터페이스 제어, 메모리에 대한 엑세스 제어 등을 행하고 메모리 내에 정보를 저장 한다.

2.1. IC 카드의 구조

IC 카드는 정보를 처리하고 관리하는 중앙 처리 장치 부분, 정보를 저장하는 메모리 부분, 그리고 정보의 입·출력을 담당하는 입·출력 부분으로 구성된다. IC 카드의 8 비트 마이크로프로세서는 읽기 작업만을 할 수 있는 메모리에 이식된 운영 체계 프로그램을 통하여 정보의 처리, 저장, WRU(write/read unit)을 통한 정보의 이동 등을 관리하며, 연산부, 제어부와 버스부로 구성된다.[4]

IC 카드의 메모리로는 RAM, ROM, EPROM 혹은 EEPROM 이 있다. IC 카드의 RAM 에 저장된 정보는 전원이 꺼지면 소실되는 휘발성 메모리이지만, 억세스 속도는 가장 빠르다. ROM 은 비휘발성 메모리로서 쓰기가 불가능하고 읽기 만이 가능하여, 주로 COS(card operating system)가 저장되어 있다. EPROM 은 사용자가 처음에 기록 한 이후에는 자외선에 노출되기 전까지는 지워지지 않는다. IC 카드에서 EPROM 은 차폐되므로 데이타의 추가만 가능하고 삭제는 불가능하다. 따라서, 입·출력기를 사용하여 전자적으로 삭제와 재기록이 가능한 EEPROM 이 주로 사용된다.

2.2. Secure Module

현재 국내에서 추진 중인 주민용 IC 카드는 기본 연산과 대칭 키 방식의 암호화 알고리듬만을 구동할 수 있는 제한된 능력을 가지고 있으므로 고속의 멱승 연산이 필요로 하는 디지탈 서명을 구현하기에는 문제가 있다. 따라서, 정보 보호에 필수적인 디지탈 서명 문제를 해결하기 위해서는 단말내에 SM 를 장착하여 주민용 IC 카드에서의 디지탈 서명 구현을 가능케 한다.

SM(secure module)은 IC 카드의 WRU 과 연결된 호스트 혹은 단말의 내부에 있는 보조 장치로 IC 카드의 기본 연산, 서명에 필요한 고속 멱승, 해쉉 등의 능력을 가진다. 물리적인 형태는 IC 카드와 동일한 형태의 핵심부와 연동이 가능하고 고속의 연산이 가능한 보조 장치로 구성될 수 있다. 논리적으로는 핵심부와 보조 연산 장치는 동일한 정도의 안전도를 확보하여야 하며, 특히 단말 내부 핵심부의 비밀 영역에 저장되는 비밀 키는 가장 높은 정도의 보호 서비스를 요구한다.

기존의 8 비트 마이크로 프로세스를 내장한 IC 카드는 필요한 연산 능력을 SM 으로부터 제공받기 위하여, 중요 정보를 SM 으로 전송하여야 한다. 이를 위해서는 SM 이 적법한 보호 장치임을 인증한 후 서명에 필요한 중요 파라 미터 및 비밀 키를 안전하게 전송해야 한다. 일반적인 IC 카드 인증 시스템의 문제점인 사용자 인증이 단말과 카드간의 인증보다 먼저 일어나므로 인하여 사용자의 패스워드가 불법적인 단말에 의해 녹취될 수 있으므로 단말과 카드간의 인증이 먼저 일어나야 한다.

그리고 불법적인 단말은 카드를 삽입한 사용자가 인증의 성공을 기다릴 때 사실은 실패하였지만 화면에 성공하였을 때와 동일한 형태의 화면을 띄우므로 사용자의 패스워드를 녹취할 수 있다. 이는 카드가 단말이 불법 단말임을 사용자에게 알려줄 수 없기 때문이다.

따라서 사용자도 단말과 카드간의 인증이 성공적으로 이루어짐을 명확히 확인한 후에 자신의 패스워드를 입력하는 형태의 시스템이어야 하겠다. 이를 위해서는 적합한 단말 인증, 카드 인증, 사용자 인증이 암호학적 안전성을 유지하면서 일어 나야 한다.

3. 인증 및 서명 프로토콜 제안

본 장에서는 SM 과 IC 카드를 사용한 사용자의 인증을 기존의 인증 시스템의 문제점들과 비교 분석하고 새로운 인증 및 서명 시스템을 제안하다. 그리고 이를 사용하여 디지탈 서명를 구현하다.

3.1. 대표적인 인증 프로토콜

인증은 실체(entity)의 신분이 정당하고 적법하다는 것을 확인하는 것으로 보호 서비스 중에서 가장 기본이 되는 항목이다. 인증에 이용될 수 있는 정보 요소에는 패스워드와 같이 알고 있는 것, 열쇠나 IC 카드와 같은 소유하고 있는 것 그리고 지문, 음성, 망막 구조와 같이 유일하게 식별되는 것이 있다.

IC 카드를 사용한 인증에는 카드 사용자가 적법한 소유자임을 확인하는 사용자 인증(user authentication), 사용되는 IC 카드가 적법한지를 확인하는 카드 인증(card authentication) 그리고 네트워크 혹은 호스트 컴퓨터에 연결된 단말기의 적법성을 확인하는 단말기 인증(terminal authentication)이 있으나, 응용 분야에 따라 이들 인증의 병행 혹은 개별적으로 수행할 수 있다. IC 카드 시스템에서는 초기 단계 서비스로 계산 부하가 적은 대칭 키 암호 알고리듬을 사용한 인증 방법을 사용하여 카드 인증 · 단말 인증 · 사용자 인증을 수행한 후 키 분배, 서명 등의 응용 서비스를 적법한 사용자에게만 제공하는 것이 바람직하다. 본 장에서는 대칭 키 암호 알고리듬을 사용한 Königs 의 인증 방식[1], NIST 의 ASACS[2] 그리고 UEPS[3]를 비교 분석하고 이들의 문제점을 제시한다. 그리고 이들의 문제점을 개선한 프로토콜을 제안한다.

3.1.1. Königs 의 인증 방식

1991 년 Königs 는 스마트 카드를 위한 인증 방식들을 발표하였으며 그 중 대칭형 암호 알고리듬을 사용한 인증법은 그림 3.2 에서와 같다.[1] 이 방식의 특징은 대칭형 암호 알고리듬의 가장 큰 문제점인 키 관리 문제를 해결한 것이다. 하지만, 실제 구현에는 패스워드를 IC 카드에 직접 입력하는 것은 차세대 IC 카드에는 가능하지만 주민용 IC 카드에서는 불가능하며 단말을 통과하여야 한다. 그러므로, 불법적인 단말이 패스워드를 녹취할 수 있는 문제점이 있고, 랜덤한 값이 암호화되지 않은 평문으로 시도되고, 이에 유일한 암호문이 응답되므로 공격자가 원하는 임의의 평문에 해당하는 암호문의 쌍을 결정하여 비밀 키 혹은 암호화 알고리듬을 찾아내는 adaptive-chosen-plaintext-attack 으로 공격이 가능하다.[5] 이 공격은 입력의 평문을 조금씩 바꿀 수 있으므로 출력되는 암호문의 쌍을 쉽게 얻을 수 있음을 의미하며, 의도한 다른 형태의 평문에 대한 암호문의 쌍들로부터 각 라운드를 지날 때마다 전파되는 출력으로 비밀 키를 찾아내는 differential-attack 에 치명적으로 공격 당한다.[3] 그리고 비밀 키를 알지 못하더라도 인증 정보를 그대로 중계하여 합법적인 사용자로 인증 받을 수 있는 main-in-the-middle-attack 와 필요한 세션의 인증값을 또 다른 세션을 이용하여 얻어내는 oracle-session-attack 에 공격 당할 수 있다.[5]

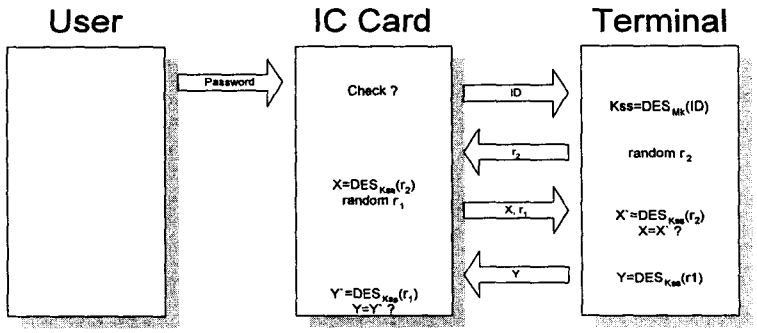

그림 3.2. Königs 의 인증 프로토콜
Fig. 3.2. Königs' authentication protocol.

3.1.2. NIST 의 ASACS 인증 방식

미국의 NIST 의 FIPS 190(federal information processing standards publication 190)[2]에서는 IC 카드와 단말기가

서로 동일한 비밀 키를 소유하고 있느냐를 확인하여 상호 인증을 수행한다. *Königs* 의 인증 방식과 다른점은 단말의 비밀 키(K_{st})와 IC 카드의 비밀 키 (K_{ss})를 키 인증 센타(key authentication center, KAC)에서 사전에 배분한다는 것이다. 그러므로, 키 분배 및 관리에 문제가 있다. 프로토콜 수행 절차상 사용자 인증이 먼저 일어나므로 단말을 인증하지않은 상태에서 패스워드를 전송하고 이는 패스워드를 녹취당할 위험을 가진다. 인증 프로토콜상으로는 Königs 의 인증 방식[1]과 같이 선택된 시도에 대한 응답을 얻어 인증하는 방법으로 공격 시 필요한 평문과 암호문의 쌍을 임의로 결정하는 adaptive-chosen-plaintext-attack 이 가능하다.[3] 그리고 man-in-the-middle-attack 과 oracle-session-attack 에 공격 당할 수 있다.[5]

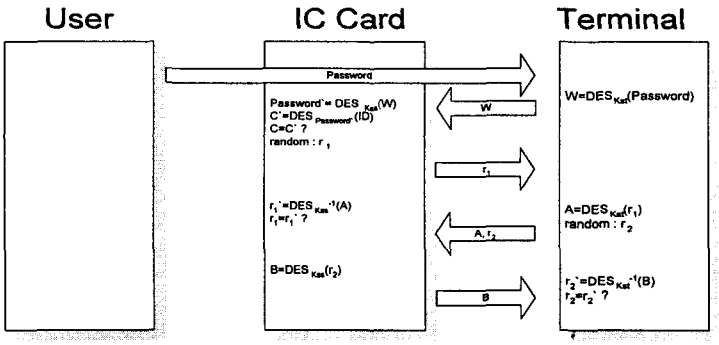

그림 3.3. NIST 의 ASACS
Fig. 3.3. The ASACS specified by NIST.

3.1.3. UEPS 의 인증 방식

UEPS[3]은 남부 아프리카의 금융 시스템에 사용하기 위해 개발되어 주요 금융계에서 채택되어 실제 사용되고 있으며 계속 개발되고 있다. 열악한 전화 사정으로 온라인(on-line) 증명이 불가능한 지역에서 은행 캐쉬 카드로 사용된다.

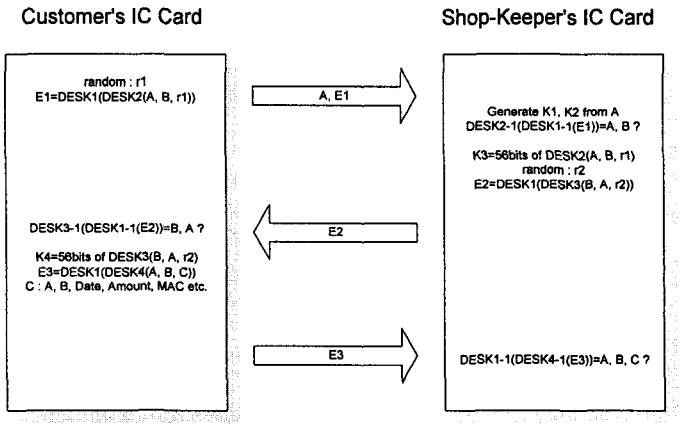

그림 3.4. UEPS 의 인증 프로토콜
Fig. 3.4. The authentication protocol of UEPS.

사용자의 개인 정보로부터 유일한 두 개의 상호 독립적인 비밀 키 쌍을 발생시키는 알고리듬을 비공개함으로써 시스템의 안전성을 유지한다. 따라서, 다른 시스템에서의 문제점인 키의 관리 문제가 알고리듬의 비밀성 유지 문제로 바뀐다. 하지만, 모든 IC 카드가 개인의 정보로부터 비밀 키를 발생시키는 알고리듬을

내부에 가지고 있어야 하므로 전체 시스템의 안전성이 각 개인의 IC 카드에 달려있다. 전체 시스템의 안전성에 관계되는 알고리듬이 모든 사용자의 IC 카드 내에 저장되어 있으므로 시스템 안전성의 집중적 관리가 문제된다. 프로토콜의 진행 중 직전에 전송된 내부 암호화된 메시지로부터의 새로운 비밀 키 생성으로 중복 인증을 수행한다. 두 사용자는 동일한 성능의 IC 카드를 소지하게 되며 프로토콜 진행 중에 분배되는 비밀 키 K_3, K_4가 비밀 키 암호화 방식의 서명의 역할을 한다. 하지만, 단말을 인증하지 않은 상태로 두 사용자가 통신을 개시하므로 전송상의 메시지를 녹취하여 불법적인 재사용을 가능케 하며, 사용자 비밀 정보의 노출 시 재발급을 위해서는 변하지 않은 개인 정보로부터 노출된 비밀 키와는 다르면서 유일한 비밀 키를 발생시키는 것이 불가능하며 만약 가능케 하기 위해서는 모든 사용자의 IC 카드 내에 있는 비공개 된 알고리듬을 수정하여야 한다.

3.2. 디지탈 서명

본 논문에서는 일반적인 비대칭 키 방식의 디지탈 서명 서비스를 제공하고자 한다.[6-9]

3.3. Secure Module 을 사용한 인증 및 서명 프로토콜

본 장의 앞부분에서 대칭 키 인증 방식의 비교·검토를 통하여 기존의 8 비트 마이크로 프로세스를 내장한 IC 카드에서 디지탈 서명 서비스를 제공하기 위한 인증 및 서명 프로토콜을 제안한다.

3.3.1. 인증 및 서명 시스템 환경

본 논문에서 제안하는 IC 카드를 사용하는 인증 및 서명 프로토콜의 환경은 다음과 같다. IC 카드 발급과 갱신을 위한 신뢰할 수 있는 TTP(trusted third party)와 SM 그리고 각 사용자의 IC 카드이다.

TTP 는

1) 사용자의 개인 정보($ID_{[user]}$)로부터 사용자의 인증용 비밀 키($K_{S[user]}$) 발생;
2) 사용자의 서명 생성용 공개 키 증명서($CERT(Y_{[user]})$) 발급;
3) IC 카드의 모든 메모리 영역에로의 인가된 접근 가능;

의 능력을 가진다. 그리고 IC 카드의 주요 사양은

1) CPU, ROM, RAM, 8Kbyte EEPROM 및 COS 로 구성;
2) 데이타 보호 알고리듬[9] 및 랜덤수 생성[10]과 메세지를 해쉬하는 해쉬 함수[11]가 내부에서 S/W 로 실시간 처리가 가능;
3) 다수의 비밀 키가 보호되는 장치가 있고, 비밀 키의 안전한 삽입도 보장 (단, 사용자의 비밀 패스워드도 하나의 비밀 키가 됨);

과 같고, SM 의 구성은

1) 물리적 : 사용자의 IC 카드와 동일한 능력인 SM 의 핵심부와 연동이 가능한 보조 연산 장치;
2) 논리적 : 핵심부와 보조 연산 장치는 동일한 수준의 안전도를 확보;

하여 단말 내에 구성된다. 전체 시스템의 안전도는 TTP 와 SM 의 핵심부 내의 비밀 영역에 저장 되는 단말 비밀 키(K_T)의 안전도와 동일하다. 단말 비밀 키(K_T)로 SM 은 사용자의 개인 정보로부터 사용자의 인증용 비밀 키($K_{S[user]}$)를 생성시킨다. 즉, 사용자 IC 카드 내의 비밀 정보가 노출되어도 전체 시스템의 안전도에는 영향을 미치지 못하는 장점을 가진다.

3.3.2. IC 카드 발급

IC 카드 사용자 A 는 TTP 에게 자신의 개인 정보(ID_A)와 사용하고자 하는 패스워드($Password_A$), 단말 인증용 비밀 구문(*Secret phrase*) 그리고 사용자 A 의 서명 생성용 비밀 키(X_A)를 제출한다. TTP 는

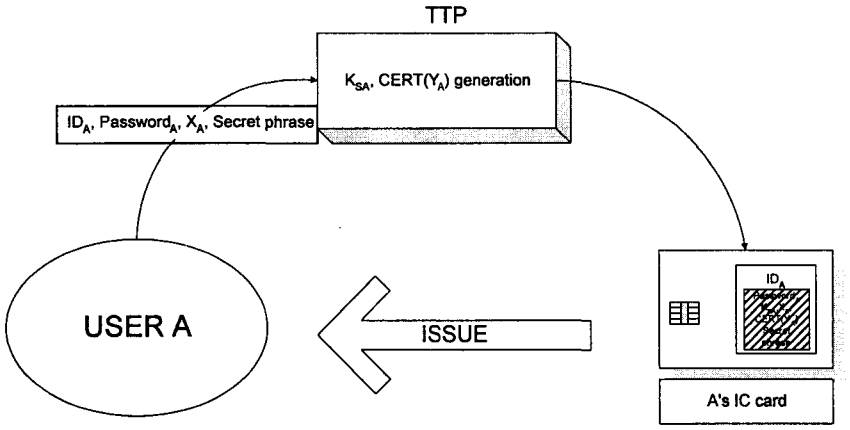

그림 3.5. IC의 발급
Fig. 3.5. The issue of IC card.

공개 영역에 사용자의 개인 정보를 비밀 영역에는 패스워드($Password_A$), 서명 생성용 비밀 키(X_A), 서명 생성용 공개 키 증명서($CERT(Y_A)$), 사용자 A가 선택한 단말 인증용 비밀 구문(*Secret phrase*) 그리고 개인 정보로 생성하여 개인에게 유일한 인증용 암호화 키(K_{SA})를 저장하여 사용자 A에게 발급한다. IC 카드 발급은 그림 3.5에서와 같다. 여기서 단말 인증용 비밀 구문(*Secret phrase*)은 단말의 적법함을 인증 한 후에는 사용자가 임의로 갱신 할 수 있다.

3.3.3. 인증 및 서명 프로토콜

주민용 IC 카드 정도의 능력으로 디지탈 서명을 구현하기 위해서는 서명 생성용 비밀 키는 IC 카드에 저장하여 단말의 적법함을 인증한 후 단말내의 계산 능력이 우수한 SM으로 전송하여 SM이 서명을 생성하여야 하겠다. 이를 위해서는 단말 인증, 카드 인증, 사용자 인증이 디지탈 서명 서비스에 선행되어야 하고 그림 3.6에서와 같다.

1) IC 카드가 ID_A와 $T1$을 전송

$$T1 = DES\left[\left(r_A, ID_A\right), K_{SA}\right], \quad where\ K_{SA} = DES\left[ID_A, K_T\right]$$

2) SM은 ID_A를 가지고 K_{SA}를 만들고 $T1$을 복호화하여 r_A를 저장하고, r_{SM}을 발생하여 K_{SA}'로 암호화하여 $T2$를 전송

$$T2 = DES\left[\left(r_A, r_{SM}, ID_A\right), K_{SA}'\right], \quad where\ K_{SA}' = K_{SA} \oplus r_A$$

3) K_{SA}를 생성하여 $T2$를 복호화하여 r_A를 확인하여 SM을 인증하고, $T3$를 전송

$$T3 = DES\left[\left(r_A, r_{SM}, ID_A, Password, Secret\ phrase\right), K_{SA}''\right]$$

$$, where\ K_{SA}'' = K_{SA}' \oplus r_{SM}$$

4) $T3$를 복호화하여 r_{SM}을 확인하므로, IC 카드 인증
5) Terminal이 *Secret phrase*를 display 하여, 사용자가 단말과 IC 카드의 인증이 성공함을 확인
6) 사용자는 패스워드 입력, 사용자 인증
7) IC 카드는 공개 키 증명서와 서명을 위한 비밀 키를 전송
8) SM 디지탈 서명 생성[6-8]

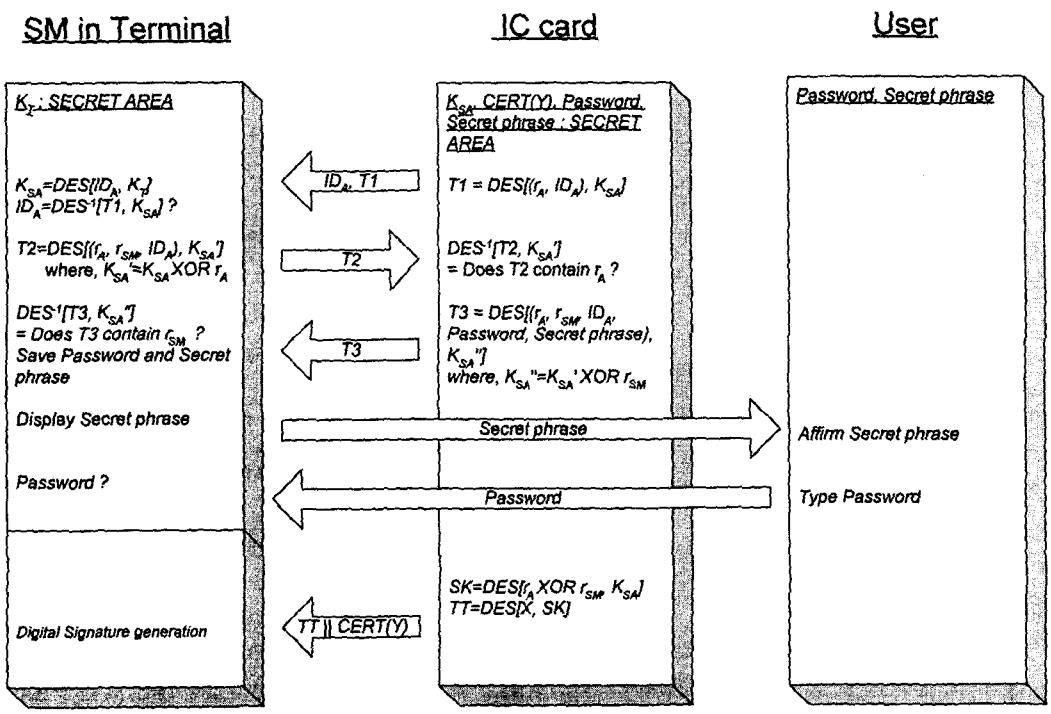

그림 3.6. 제안한 인증 및 서명 프로토콜

Fig. 3.6. Proposed authentication and signature protocol.

앞에서 설명한 대표되는 인증 시스템에서는 단말 인증이 일어나기 전에 사용자 인증이 먼저 일어나므로 불법 단말이 사용자의 패스워드를 녹취할 수 있는 문제점이 있었다. 따라서 본 논문에서는 단말 인증과 카드 인증이 사용자 인증보다 먼저 일어나도록 설계하였다. 단말과 IC 카드간의 인증은 대칭 키 암호화 알고리듬을 사용하여 시도·응답형 프로토콜로 이루어 지며, 대칭 키 암호화 알고리듬의 문제점인 키 분배 및 관리를 해결하는 사용자의 개인 정보로부터 사용자마다 유일한 인증용 비밀 키($K_{S[user]}$)를 SM이 생성하도록 하였다. 따라서, 카드와 단말간의 인증 프로토콜 수행 시 이미 알려진 인증을 원하는 사용자의 개인 정보만이 의미 있는 평문 상태로 전송되게 된다. 하지만, 키 관리상의 문제 외에 일반적인 상호 인증 프로토콜은 불법적인 사용자가 프로토콜 자체를 공격하여 적법하게 인증을 받을 수 있다.

비밀 키를 알지 못하더라도 적법한 사용자들의 통신 내용을 녹취하여 변경 혹은 재사용으로 통신 내용의 도청, 합법적인 사용자로 가장하는 공격인 man-in-the-middle-attack에 자유롭고, 필요한 세션의 인증값을 다른 세션을 이용하여 얻어내어 합법적인 사용자로 가장하는 oracle-session-attack에의해 공격 되지 않는 인증 프로토콜을 제안한다.[5]

위의 두 공격으로부터 자유롭기 위해서는 시도인 랜덤수의 발신지가 명확히 그 속에 내포되어야 한다. 그리고, 이에 대한 응답도 인증 당사자로부터의 응답임이 명확하여야 하며 시도와 응답이 일대일 대응이 되지 않아야 재사용 공격으로부터 안전하게 된다.

제안하는 프로토콜은 시도가 사용자의 인증 비밀 키($K_{S[user]}$)로 암호화되어 전송되므로 인증을 원하는 사용자로부터의 발신이 명확하게 되고, 사용자의 개인 정보($ID_{[user]}$)로부터 사용자의 인증 비밀 키($K_{S[user]}$)를 생성시키는 단말 비밀 키(K_T)를 가지고 있어야 시도를 제대로 복호화 할 수 있고 적합한 응답을 전송할 수 있으므로 인증이 공격으로부터 안전하고, 각 전송 정보는 랜덤수가 각각 포함되고 암호화하는 비밀 키가 직전에 전송된 랜덤수와의 결합으로 새로이 생성되므로 각 세션에서 유일하며 연속된 인증의 의미를 가지는 인증 프로토콜이 수행된다.

일반적인 인증 프로토콜은 단말이 적법하지 않아서 인증 프로토콜이 성공하지 못하여도 불법 단말이 모니터에 인증이 성공하였다고 출력하고 패스워드를 입력하라는 메세지를 성공했을 때와 동일하게 띄우면 사용자는 패스워드를 입력하게 되므로 패스워드를 녹취당하게 된다.

제안 프로토콜에서는 불법 단말의 사용자 패스워드 녹취를 방지하기 위해 사용자가 IC 카드 발급 시에 선택하여 IC 카드의 비밀 영역에 저장되어 있는 비밀 구문(*Secret phrase*)를 모니터에서 확인함으로써 단말과 카드간의 인증이 성공함을 확인하게 되는 방식을 제안하여, 종래의 IC 카드만이 단말을 인증하는 단말 인증의 정의를 사용자가 IC 카드를 통하여 단말을 인증하는 것이 단말 인증임으로 새롭게 재정의 하였다.

이로써 인증은 끝나게 되고, 사용자는 원하는 서비스를 받을 수 있게 된다. 특히, 디지탈 서명 서비스를 원하는 경우에 쌍방은 인증 과정에서 사용된 랜덤수의 조합으로 세션 키를 생성하여 서명 생성용 비밀키($X_{[user]}$)와 공개 키 증명서($CERT(Y_{[user]})$)를 전송하고 SM이 디지탈 서명을 하게 된다. 단말을 통하여 서명의 온라인 전송이 가능하고 전송된 디지탈 서명 검증도 SM이 수행하게 된다.

3.4. 제안 프로토콜의 비교 분석

제안 프로토콜은 사용자의 정보 보호를 위하여 단말과 카드간의 상호 인증이 선행된 후 사용자 인증이 일어나는 방식이다. 전송문에 대한 공격 시 제안 프로토콜에서는 ciphertext-only-attack 만 가능하고[3], 프로토콜에 대한 공격 시에는 man-in-the-middle-attack, oracle-session-attack 과 같은 프로토콜 공격에도 안전하게 설계되었다.[5] UEPS[3]에서는 패스워드를 사용하지 않으므로 사용자 인증이 일어나지 않고 있으며, Königs 의 방식[1]에서는 암호화되지 않은 패스워드가 전송로상에서 드러나게 된다. 하지만, 제안 프로토콜에서는 IC 카드 내에 저장되어 있는 패스워드가 암호화된 상태로 인증된 단말로 전송되어 단말 내에서 사용자가 입력한 패스워드와 비교되어 사용자 인증을 수행하므로 사용자 인증이 안전성을 유지하며 일어난다.

그리고 Königs 의 방식,[1] ASACS,[2] UEPS[3]에서는 단말과 카드간의 인증이 사용자와는 무관하게 일어나므로 사용자는 단말과 카드간의 인증이 성공하였음을 알 수 없지만, 제안 프로토콜에서는 사용자가 단말과

표 3.1. 프로토콜 비교
Table 3.1. The comparison of protocols.

	Königs	ASACS	UEPS	Proposal
Possible message attack	chosen-plaintext attack	chosen-plaintext attack	ciphertext-only attack	ciphertext-only attack
Possible Protocol attack	man-in-the-middle attack, oracle-session attack	man-in-the-middle attack, oracle-session attack	×	×
Password usage	○	○	×	○
Terminal authentication by user	×	×	×	○
The number of key in Terminal	1	as many as user	secret algorithm	1
key distribution	×	×	○	○
Signature	×	×	Secret key signature	Public key signature
The number of times of DES execution in card	≥ 2	≥ 4	≥ 6	≥ 5+2(for sign)

카드간의 인증이 성공하였음을 확인하는 확장된 의미의 단말 인증을 제안하여 불법적인 단말에 의한 패스워드 녹취 위험을 제거하였다. 즉, 단말 인증은 IC 카드로 사용자가 단말이 적법함을 인증하는 것이다.

단말이 저장하고 있어야 되는 비밀 키의 수는 개인 정보로부터 각 사용자에게 고유한 인증용 비밀 키를 생성하는 단말 키 하나만 있으면 되므로 단말의 키 저장 문제점이 없다.[2] 그리고, 대칭 키 암호화 알고리듬인 DES(data encryption standard)[9]를 사용하여 인증을 원할 때 IC 카드에서는 5 회 서명 생성용 비밀 키 전달을 위해 2 회로 7 회의 실행이 필요하므로 실시간 동작이 가능하다. 사용자의 개인 정보로부터 독립적인 2 개의 키를 발생시킬 때는 동일한 프로토콜상에서 안전성을 강화 할 수 있다.

4. 결 론

본 논문에서는 안전한 보호 장치 SM 을 사용한 IC 카드의 인증 및 서명 프로토콜을 제안하였다. 카드와 단말간의 인증은 개인의 정보를 이용하여 대칭 키 암호 시스템에서의 문제점인 단말의 비밀 키 보관의 어려움을 제거하고, man-in-the-middle-attack 과 oracle-session-attack 에 강한 인증 프로토콜을 제시하였다. 이에 부가적으로, 카드와 단말간의 인증이 사용자 인증보다 먼저 일어나야 함과, 취약한 단말 인증의 정의를 확장하여 정의하였다. 따라서, 일반적인 디지탈 서명을 안전한 보호 장치인 SM 에서 계산 능력이 약한 IC 카드의 역할을 대신할 수 있도록 하였다.

참 고 문 헌

[1] H. P. Königs, "Cryptographic Identification Methods for Smart Cards in the Process of Standardization," *IEEE Comm. Magazine*, pp. 42-48, June 1991.

[2] NIST, Guideline for the Use of Advanced Authentication Technology Alternatives, *FIPS PUB 190*, 1994.

[3] Bruce Schneier, *Applied Cryptography*, John Wiley & Sons, 1996.

[4] J. L. Zoreda, J. M. Oton, *Smart Cards*, ARTECH HOUSE, 1994.

[5] R. Bird, P. Janson, S. Kutten, R. Molva, M. Young, A. Herzberg, and R. Gopal, "Systematic Design of Efficient Provably Secure Two-Way Authentication Protocols," *Advances in Cryptology-Crypto '91*, pp. 12-24, 1991.

[6] NIST, Digital signature standard, *FIPS PUB 186*, 1994.

[7] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Trans. Inform. Theory*, IT-31, pp.469-472, 1985.

[8] C. P. Schnorr, "Efficient Signature Generation for Smart Cards," *Advances in Cryptology-CRYPTO'89 Proceedings*, Spinger-Verlag, pp.239-252, 1990.

[9] NIST, Data Encryption Standard, *FIPS PUB 46*, 1977.

[10] Knuth, *The Art of Computer Programming: Vol. 2, Seminumerical Algorithms*, 2nd edition, Addison-Wesley, 1981.

[11] NIST, Specification for a Secure Hash Standard(SHS), *FIPS YY Draft*, January 1992.