스마트 카드와 지문을 이용한 인증 시스템 설계

손인구° 민경진 류은경 유기영
경북대학교 컴퓨터 공학과
{sig3°, clenet, ekryu }@infosec.knu.ac.kr, yook@knu.ac.kr

The Design of an Authentication System using Smart Card and Fingerprint

In-Gu Son° Kyung-Jin Min Eun-Kyung Ryu Ki-Young Yoo
Dept. of Computer Engineering, Kyungpook National University

요 약

본 논문에서는 다양한 응용 분야에 이용되는 스마트 카드의 보안성을 높이기 위하여 스마트 카드와 무선 단말기, 무선 단말기와 사용자간의 인증을 구분하여 설계하였다. 기존의 스마트 카드와 지문을 이용한 인증 시스템은 스마트 카드내의 지문 정보의 유출이나 스마트 카드 상에서 지문 매칭시 현실적인 문제뿐만 아니라 카드와 단말기 양측을 모두 인증하는데 어려움이 있었다. 그래서 본 논문은 기존의 스마트 카드와 단말기의 양방향 인증 등을 이용하지 않고, 스마트 카드가 무선 단말기를 인증한 다음, 무선 단말기에 부착된 지문 센서를 이용해 입력된 사용자의 지문 정보로 단말기가 사용자 인증을 하도록 하였다. 제안된 인증 시스템은 스마트 카드 및 지문을 이용하여 사용자측(스마트 카드와 카드 소유자)과 단말기간의 상호인증을 제공한다. 이러한 이중 인증 메카니즘은 무선 인터넷 환경에서 보다 안전한 인증 시스템을 제공할 수 있을 것이다.

1. 서 론

차세대 디지털 기술을 대표하는 무선 인터넷과 M-commerce 가 점차 활성화되고 있는 추세에 있고, 이에 따라 무선 단말기에 대한 보안의 필요성이 증대되고 있다. 기존의 단말기 인증 방법은 PIN(Personal Identification Number) 을 사용하여 이루어 졌으나 이러한 방법은 타인에 의한 도용이나 분실, 망각의 위험이 있어 높은 수준의 보안을 보장할 수 없다. 이러한 문제점을 해결하기 위해 생체 인식을 이용한 보안 기술이 적용될 수 있다. 생체 인식은 신체의 고유한 특징을 이용해 개인을 인증하는 방식으로 홍채 인식, 정맥 인식, 지문 인식, 음성 인식 등 아주 다양하며, 이들은 신체의 일부분이므로 패스워드처럼 잊어버리거나 도난, 복사 혹은 공유가 되지 않는다. 그러므로 사용자 인증에 있어 신뢰성 있는 보안을 제공한다. 그 중에서 지문 인식은 정확도가 높고, 편의성이 뛰어나며 여러 측면에서 가격 대 성능비가 탁월하기 때문에 사용 범위가 아주 넓다. 하지만 이러한 장점을 지닌 생체 인식 정보가 데이터 서버에 저장되어 이용되면 해킹이나 분실의 위험이 있으므로 생체정보는 서버에 저장되지 않고 스마트 카드나 USB 토큰 등에 저장되어 이용될 수 있다[1][2].

기존의 스마트 카드와 지문을 이용한 인증 시스템은 스마트 카드내의 지문 정보의 유출이나 스마트 카드 상에서 지문 매칭시 현실적인 문제뿐만 아니라 카드와 단말기 양측을 모두 인증하는데 어려움이 있었다.

본 논문에서는 스마트 카드가 무선 단말기를 인증하기 위해 PIN값을 이용하였고, 무선 단말기의 사용자를 인증하기 위해 지문 정보를 이용하였다. 따라서 제안하는 인증 시스템은 스마트 카드 및 지문을 이용하여 사용자측(스마트 카드와 카드 소유자)과 단말기간의 상호인증을 제공한다. 이러한 이중 인증 메카니즘은 무선 인터넷 환경에서 보다 안전한 인증 시스템을 제공할 수 있을 것이다.

본 논문의 구성은 다음과 같다. 2절에서는 기존의 PIN 기반의 인증 방법과 지문 기반의 인증 기법에 대해 살펴보고, 3절에서는 본 논문에서 제안하는 인증 시스템의 구조 및 인증과정을 설명한다. 4절은 결론과 향후 연구 과제로 끝을 맺는다.

2. 관련 연구

기존의 스마트 카드 인증 방식은 PIN에 기반한 인증 방법과 지문 인증에 기반한 방법으로 구분할 수 있다. 스마트 카드와 단말기간의 인증 방법 중 가장 간단한 방법은 PIN 기반의 인증 방법이다[3]. 일반적으로 이러한 인증방식은 스마트 카드 상에서 PIN 매칭을 수행함으로 이루어진다. 단말기에서 전송된 값과 스마트 카드의 PIN 값을 비교하여 일치하면 스마트 카드는 단말기를 인증하여 타당한 단말기로서 인식한다. 그러나 이러한 기법은 PIN값의 분실, 도난이나 스마트 카드 자체의 분실등과 같은 문제점이 있다. 이와 같은 문제점을 보완하기 위한 방법으로는 신체의 고유한 특징중 하나인 지문을 이용하는 인증기법이 있다.

지문 인증에 기반한 스마트 카드 인증 시스템은 지문 매칭 메카니즘과 매칭하는 위치에 따라서 다양하게 나타난다. 지문을 사용한 스마트 카드 인증 시스템의 주요 연구들을 살펴보면 다음과 같다.

Noore[4]는 스마트 카드에서 두 개의 지문을 입력받아 각각의 매칭 과정을 스마트 카드 상에서 수행하는 시스템을 제안하였다. 이 시스템은 스마트 카드의 보안을

강화시키는 장점은 있으나 스마트 카드의 메모리나 계산적 능력의 문제를 야기시키는 단점도 수반된다.

Struif등[5]은 지문 입력은 단말기를 통해 입력을 받고, 지문의 매칭은 스마트 카드 상에서 수행하는 시스템을 제안하였다. Struif의 제안은 사용자의 지문이 인증을 받지 않은 스마트 카드로 전송되어 짐으로서 충분히 문제의 소지를 가지게 된다.

위의 두 가지 지문 인증에 기반한 스마트 카드 인증 시스템의 경우와 더불어 지문 매칭 과정 자체를 단말기 상에서 수행할 수도 있다. 이러한 시스템은 지문 매칭을 단말기 상에서 수행시켜 스마트 카드의 부담을 덜어 주지만, 스마트 카드의 정보가 단말기를 통해 유출될 수 있는 단점도 가지고 있다.

3. 인증 시스템 설계

본 장에서는 제안된 시스템의 전체적인 구조와 구체적인 인증절차를 기술한다.

3. 1 제안한 시스템 구조

본 논문에서 제안한 시스템의 구성은 지문 센서가 갖추어진 무선 단말기, 스마트 카드 소유자의 지문 정보와 PIN값이 내장된 스마트 카드로 이루어진 시스템이다. 이 때 단말기는 휴대 전화기나 PDA와 같은 무선 단말기라고 가정하였다.

현재 스마트 카드의 안전성을 위해선 스마트 카드와 단말기간의 양방향 인증을 사용한다[6]. 그러나 올바른 스마트 카드 소유자가 아닐지라도 인증 과정을 수행하는데 문제가 없을 수 있다. 이런 문제는 지문 인증 기술로 어느 정도는 해결이 가능하지만 지문 매칭을 수행하는 위치가 스마트 카드 상에서라면 스마트 카드에 부담을 가중시킬 것이다. 게다가 지문 매칭이 단말기 상에서 수행하더라도 여러 가지 문제가 발생할 수 있다. 즉, 단말기 상에서 지문 매칭이 수행되므로 단말기에 의한 지문 인증만 이뤄지고 타당한 단말기인지를 인증하지 못한다.

이러한 문제를 해결하기 위해서 본 연구에서는 단말기 인증을 위해 PIN 값을 이용해 스마트 카드 상에서 매칭을 수행하고, 사용자 인증을 위한 지문 매칭을 단말기 상에서 수행하도록 하였다. 아래 그림 1은 제안한 시스템의 전체적인 구조이다.

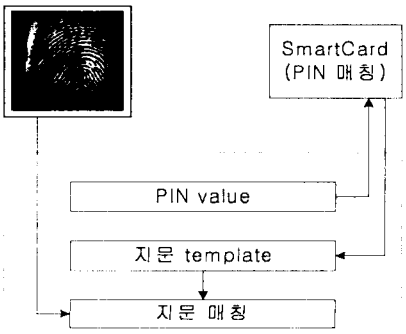

그림 1 시스템의 전체 구조

3. 2 인증 메카니즘

제안된 시스템의 인증과정은 스마트 카드에 의한 무선 단말기 인증과 단말기의 사용자 인증으로 구성된다. 각 인증 절차를 살펴보면 다음과 같다.

● 무선 단말기 인증 절차

우선 사용자가 스마트 카드를 단말기에 삽입하고, 무선 단말기상의 지문 센서를 통해 사용자의 지문을 입력하는 것으로부터 인증과정이 시작된다.

① 무선 단말기는 RESET신호를 카드로 보내고, 스마트 카드는 COS(card operating system)를 활성화시킨 후 ATR(Answer To Reset) 신호를 무선 단말기로 전송하게 된다.

② 카드로부터 ATR을 받으면, 무선 단말기는 내장된 값(단말기의 고유한 값 - 이 값은 카드내의 PIN값과 일치하며, 외부인이 알 수 없는 값)을 전송할 COMMAND APDU를 생성하여 ISO7816-4의 VERIFY COMMAND를 전송한다.

③ 스마트 카드는 수신된 데이터 값이 카드의 PIN값과 일치하는지를 확인하고, 일치한다면 올바른 무선 단말기임을 인증한다.

스마트 카드가 아래 그림 2와 같은 파일구조를 가질 때 두 값이 일치하면 무선 단말기는 WEF(Working EF)에 접근 할 수 있는 권한을 가지게 된다.

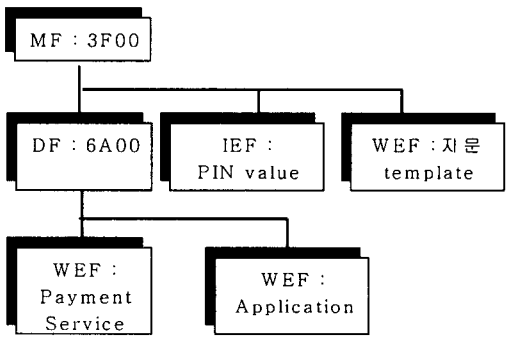

그림 2 스마트 카드의 파일 구조

④ 스마트 카드는 PIN매칭의 성공 여부를 알리기 위해 무선 단말기로 Response APDU를 보낸다. 매칭이 성공적이었다면 무선 단말기는 단말기 상에서 지문 매칭을 수행하기 위해 스마트 카드에게 지문 template를 요청하는 READ BINARY COMMAND를 전송한다.

⑤ 스마트 카드는 Response APDU로 스마트 카드 내부에 저장되어 있던 지문 template를 무선 단말기로 보낸다. 스마트 카드에 저장된 사용자의 지문정보를 사용자와 단말기간의 인증에 사용하기 위해 무선 단말기로 전송한 것이다.

지문 template는 스마트 카드 소유자 지문의 특징점들을 미리 추출해 저장해 둔 정보를 나타낸다. 아래 그림 3은 ① ~ ⑤ 까지의 과정을 나타낸 그림이다.

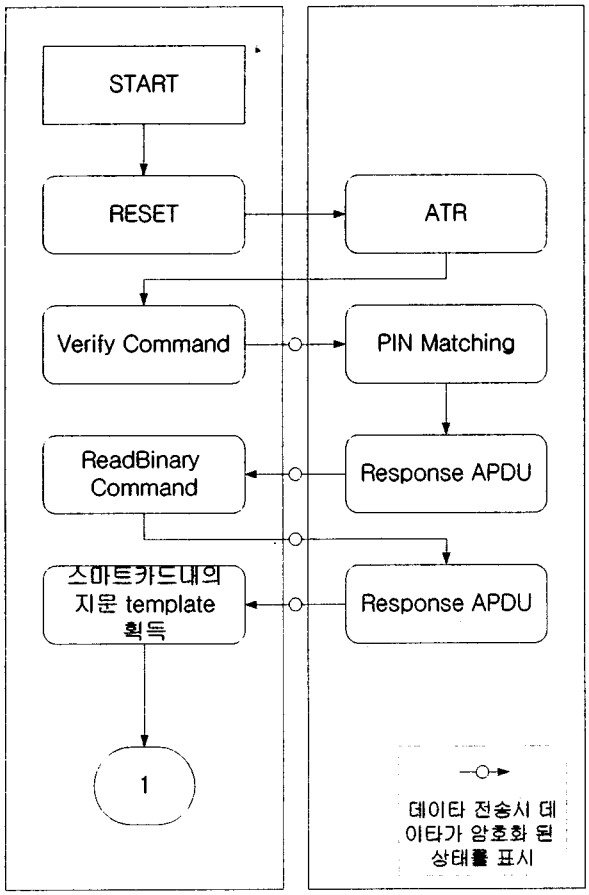

그림 3 스마트 카드가 무선 단말기를 인증하는 절차

● **단말기의 사용자 인증 절차**

이제 단말기에서는 사용자가 입력한 지문 정보와 스마트 카드로부터 받은 지문의 template를 매칭하는 과정을 수행하게 된다. 두 번의 매칭 과정이 성공적으로 마쳤다면, 스마트 카드에 의한 단말기 인증이 이루어지며, 아울러 단말기는 사용자의 입력된 지문을 통해 사용자를 인증하게 된다. 스마트 카드와 단말기의 인증이 모두 이뤄지면 이제 사용자는 안전하게 어플리케이션을 수행할 수 있다.

아래 그림 4는 무선 단말기 상에서 지문의 매칭과정을 보여준다.

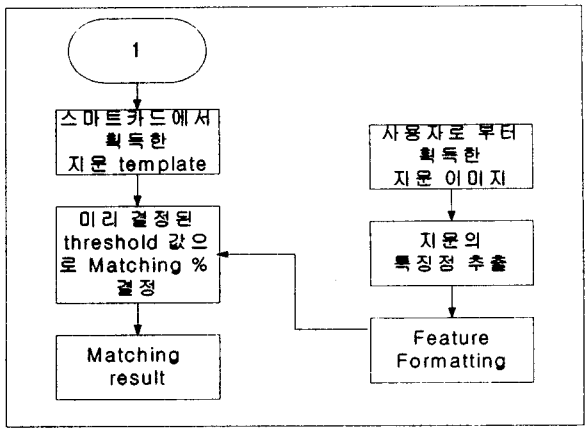

그림 4 무선 단말기 상의 지문 매칭 과정

4. 결론 및 향후 연구과제

본 논문에서는 여러 객체(사용자, 무선 단말기, 스마트 카드, 응용 서버)를 상호 인증할 수 있는 인증시스템을 구성하였다. 이러한 시스템이 주는 장점은 응용 프로그램 및 중요한 정보가 카드나 단말기 중 어느 곳에 존재하더라도 효율적인 인증을 수행 할 수 있다는 것이다. 따라서, 제안하는 시스템은 뱅킹, 전자 지불, 증권 거래 등 다양한 금융정보와 개인 정보를 무선 단말기 상에서 보호하기 위해 사용 될 수 있다. 현재의 PIN을 이용한 단말기 보안은 빠른 속도로 확대되고 있는 무선 서비스 보안에서 효과적으로 대처하지 못하여 많은 부작용을 낳고 있다. 단말기 상에서 이루어지는 상호 인증은 부정한 사용자와 단말기를 차단하여 이러한 부작용을 막는 대안으로 제시 될 수 있을 것이다.

향후 연구과제로 우리가 제안한 시스템에 원거리 응용 서버에 대한 인증 수행의 프로토콜을 추가하여 보다 발전된 시스템이 필요하다.

5. 참고 문헌

[1] 류시룡, "지문의 특징점과 방향성 정보를 이용한 매칭 방법", 경북대학교 석사 학위 논문, 2002

[2] 최정호, "데이터보안을 위한 생체측정 보안시스템", 경영과 컴퓨터,1992

[3] W. Rankl, W. Effing, "Smart Card Handbook", WILEY-VCH, 2000

[4] Afzel Noore, "Highly Robust Biometric SmartCard Design", IEEE Transactions, 2000

[5] Bruno Struif, Dirk Scheuermann, "Smartcards with Biometric User Verification", IEEE Multimedia and Expo, 2002

[6] 김증섭, 조병호, 김효철, 이종국, 유기영, "다양한 응용을 위한 스마트카드 운영체제", 정보과학회논문지, 2002