위조 지문 공격에 안전한 인증길이 기반의 지문 인증 기법

윤다예*, 김승규*, 유진아*, 김형주*, 윤성현*
*백석대학교 정보통신학부
e-mail:ydelin@naver.com

The Personal Time based Fingerprint Authentication Scheme Safe Against Forged Fingerprint Attack

Dayea Yoon*, Seunggyu Kim*, Jina Yu*, Hyeongju Kim*, Sunghyun Yun*
*Div. of Information & Communication Engineering, Baekseok University

요 약

최근 바이오메트릭 센서를 내장한 스마트폰 및 모바일 기기의 보급으로 바이오메트릭 인증에 대한 사람들의 관심이 증대되고 있다. 지문 인식은 사람마다 고유한 지문 정보를 이용하여 사용자를 인증하는 것으로 다른 바이오메트릭 인증 방법에 비하여 상대적으로 비용이 저렴하고 인식률이 높아 많은 응용에 적용된다. 하지만 사람의 지문은 실리콘 또는 젤라틴과 같은 물질을 이용해 쉽게 위조가 가능한 단점이 있다. 따라서, 지문인식용 센서는 온도, 빛 등의 2차적인 인증 수단을 함께 측정할 수 있어야 하는데, 이 경우 비용이 많이 들게 된다. 본 연구에서는 인증길이(지문인식을 위해서 스캔한 시간)와 지문인식에 사용된 손가락을 2차적인 인증 수단으로 사용하여 위조 지문 공격에 대응할 수 있는 지문 인증 기법을 제안한다. 제안한 기법은 2차 인증을 위한 키패드 기반의 패스워드 입력 부담을 줄일 수 있고 경제적이다.

1. 서론

최근 지문인식 기능을 내장한 스마트 폰의 보급으로 사용자 인증을 위한 수단으로 지문 인식에 대한 수요가 늘어나고 있다. 지문인식 기술은 출입통제, 근태·출결 관리, 결제 시스템 인증과 같이 대리 인증이 허용되지 않는 응용에 많이 이용되고 있다. 지문은 개인이 몸에 지니고 있는 고유정보로 지문인식 센서로 그 모양을 추출하여 인증에 사용하기 때문에 기존의 PIN 방식에서 발생하는 분실 및 도용의 위험을 최소화 할 수 있다 [1].

그러나 지문인식의 단점은 실리콘 또는 젤라틴과 같은 물질을 이용해 쉽게 지문을 위조할 수 있다는 것이다. 유리나 플라스틱에 남겨진 잔여 지문 흔적만으로도 위조가 가능하기 때문에, 지문인식은 더 이상 안전한 인증 수단으로 보기 어렵다 [2, 3].

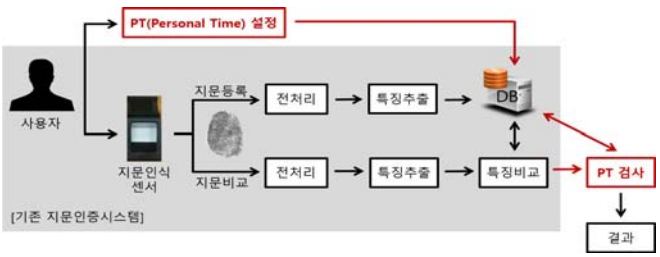
본 논문에서는 위조 지문 공격에 대응하는 2차 인증 수단으로 지문인식에 사용된 손가락과 인증길이(Personal Time)를 조합한 방법을 제안한다.

2. 관련연구

위조 지문에 대응하기 위한 기존의 연구는 크게 온도와 빛을 이용한 방법으로 구분된다. 온도를 이용한 방법은 온도 센서를 이용하여 입력된 지문의 온도를 측정하고, 이를 미리 생체 온도로 설정한 일정 범위 내에 존재하는지 판별하는 것이다. 만약 온도가 사용자가 설정한 일정범위에 속하면 올바른 사용자로 인증한다. 빛을 이용한 방법은 피부에 빛을 투과시켜서 나타나는 광감쇠 현상을 측정하여 사용자 인증에 사용하는 방법이다 [4].

그러나 기존의 위조 지문 검출 기법은 주변 환경의 영향에 민감하여 오차율이 높다는 문제점이 존재한다. 위조 지문의 온도를 생체 온도로 유지 시키면, 온도 측정 센서가 위조 지문과 생체 지문을 식별하지 못할 가능성이 크다. 더불어, 이러한 기술들을 결합하기 위해서는 부가적인 하드웨어를 추가해야 하는데, 이 경우에 비용이 증가하고 시스템의 소형화가 어렵게 된다 [2].

3. 인증길이를 포함한 사용자 인증기법



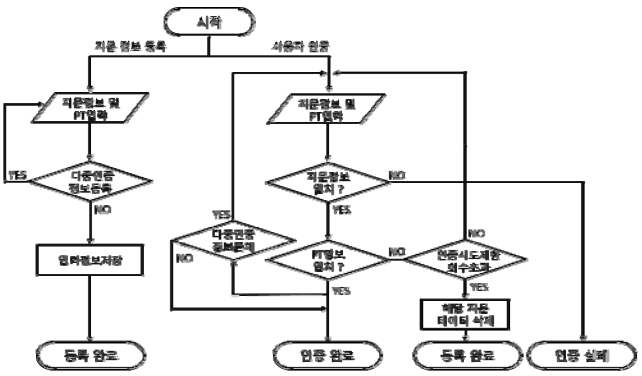
(그림 1) 인증길이 기반의 지문인증 시스템

본 논문에서는 (그림 1)과 같은 사용자 인증 기법을 제

안한다. 제안한 방법은 지문등록과 지문인증 크게 두 가지로 구분된다. 인증길이는 사용자가 지문인식 센서에 손가락을 대고 있는 시간을 의미한다. 최소 1초부터 최대 10초까지 1초 단위로 설정이 가능하다.

그림 1의 지문인증 시스템을 사용하기 위해서는 먼저 사용자의 지문과 인증길이를 등록해야 한다. 사용자는 자신이 설정하고자 하는 특정시간 동안 자신의 지문으로 지문인식 센서를 누른다. 이 때, 사용자마다 인지하는 시간의 정도가 상대적이기 때문에 비프 음을 1초마다 울리도록 하여 정확한 시간을 입력할 수 있도록 한다. 센서에 캡춰된 이미지는 전처리 단계를 거쳐서 지문 융선을 만들어 내고, 여기서 특징점을 추출한다. 이 값과 센서에 의해서 측정된 인증길이를 데이터베이스에 함께 저장한다.

지문인증 단계에서는 입력된 사용자 지문으로부터 얻은 특징점과 인증길이를 데이터베이스에 등록된 값들과 각각 비교한다. 두 값의 비교가 모두 성공하면 올바른 사용자로 인증한다.



(그림 2) 확장된 인증길이 기반의 지문인증 시스템

해커가 사용자의 위조 지문을 만들었다고 가정하고, 이를 이용하여 인증길이를 알아내기 위한 전사적 공격을 하게 되면 제안한 인증 시스템에 접근이 가능하다. 따라서 제안한 인증길이 기반의 2차 인증 방법을 실제 구현하려면, (그림 2)와 같이 인증시도를 제한하고 여러 지문을 다중으로 등록하여 해커의 공격 위험을 최소화 하도록 알고리즘을 확장해야 한다.

(그림 2)의 인증시도 횟수 제한 기능은 지문정보는 일치하나 인증길이가 사용자가 지정한 일정 횟수 이상 불일치하게 되면 해당 지문정보를 삭제하는 기능이다. 횟수는 시스템에서 10번으로 지정되어 있으며 데이터베이스에 등록된 지문정보가 삭제되기 때문에, 해커는 더 이상 공격할 대상이 없어지게 된다.

다중 인증정보 등록기능은 두 개 이상의 지문 정보 및 인증길이를 등록하여 해커가 찾아내야 하는 총 경우의 수를 늘리는 방법이다. 만약 해커가 사용자의 열 손가락 지문정보를 모두 위조한 경우에 만들 수 있는 인증정보의 경우의 수는 10(손가락의 개수)*10(인증길이)으로 총 100가지 경우의 수가 발생한다. 이 때, 다중 인증 정보 등록 방법을 이용하면 해커가 전사적 공격을 성공할 확률이 $1/100^{x}$(x=등록한 지문 수)이 된다. PIN을 이용한 2차적 보안 방법보다 간편할 뿐만 아니라 보안성을 응용에 따라서 여러 단계로 조정할 수 있다.

제안한 다중 인증 정보 등록 방법을 적용한 지문등록과 지문인증 단계는 다음과 같다.

시스템은 지문정보 등록 시 사용자의 지문정보와 인증길이를 입력받는다. 만약 사용자가 다중 인증 정보를 등록하길 원한다면, 추가적으로 다른 지문정보와 인증길이를 입력받는다. 마지막으로 인증시도 제한 횟수를 입력 받아서 기존에 입력한 지문 및 인증길이 정보와 함께 모두 데이터베이스에 등록한다.

지문인증 단계에서 사용자는 자신의 지문과 인증길이를 입력하여 인증을 시도한다. 입력된 지문정보와 데이터베이스에 저장되어있는 지문정보를 비교하여 두 값이 일치하면 인증길이를 비교한다. 이 값이 데이터베이스에 저장되어있는 인증길이와 일치하면 올바른 사용자로 인증한다. 만약 인증길이를 비교하는 과정에서 불일치하는 것으로 나타나면 인증 시도 제한 횟수가 카운트 되고 해당 제한 횟수 안에 인증을 성공하지 못하면 저장되어있던 사용자의 정보는 삭제되도록 한다.

4. 결론 및 기대효과

본 논문에서는 위조를 통한 지문정보 도용의 문제를 해결하기 위해서 인증길이와 손가락 수를 조합한 새로운 지문인증 기법을 제안하였다. 더불어 실제 구현 시 고려해야 할 취약점을 분석하였고, 이에 대응하기 위하여 인증시도 제한, 다중인증 정보 등록 기능을 갖는 확장 알고리즘을 제시하였다. 제안한 방법은 사용자의 지문정보가 노출되어도 인증길이를 알지 못하면 인증을 수행할 수 없으며, 지문 인식 센서만을 사용하기 때문에 기존의 PIN을 사용한 인증 방법보다 비용이 저렴하고 간편하다. 또한 다중 인증정보 등록 방법을 통해서 경우의 수를 조절할 수 있기 때문에, 적용하고자 하는 응용에 따라서 보안성과 편리성을 조절할 수 있는 장점이 있다.

감사의 글

본 연구는 문화체육관광부 및 한국콘텐츠진흥원의 2016년도 문화기술 연구개발 지원사업으로 수행되었음.

참고문헌

[1] 이현숙 “지문을 이용한 사용자 인식 시스템” 한국인터넷정보학회 학술발표대회 논문집 6(2), 2005.11, 799-802

[2] 이지선 "광학식 지문센서에서의 위조 지문 검출 방법" 멀티미디어학회논문지 11(4), 2008.4, 492-503

[3] A.J. Menezes "Handbook of Applied Cryptography" CRC Press, 2014.12

[4] 최희승 “위조 생체 검출 기술의 현황과 전망” The Magazine of the IEEK 33(1), 2006.1, 64-73