어깨넘어 훔쳐보기 공격에 대항하는 모바일 기기를 이용한 이중 사용자 인증 기법

이학준, 이종협
*한국교통대학교 소프트웨어학과
dorek99@naver.com, jhlee@ut.ac.kr

A two factor authentication using mobile devices against shoulder surfing attacks

Hak-Jun Lee*, JongHyup Lee*
*Dept of Software, Korea National University of Transportation

요 약

비밀번호를 비기술적인 방법으로 해킹 중 어깨넘어 훔쳐보기 공격은 사회공학적인 공격기법으로서 많은 보안 메커니즘의 등장에도 불구하고 원천적인 차단이 어려운 공격이다. 특히 현금자동입출기기는 개방적인 공간에 설치되어있어 어깨넘어 훔쳐보기 공격에 취약하다. 본 논문에서는 사용자가 금융서비스를 받고자 할 때, 현금자동입출기기, 스마트폰, 사용자 사이의 안전한 신뢰관계를 구축하고 비밀번호와 지문인식을 이용한 안전한 이중 사용자 인증 기법을 제안한다. 제안하는 기법은 어깨넘어 훔쳐보기 공격의 용이성 및 재현 가능성을 제한하여 안전한 금융서비스가 가능하도록 한다.

1. 서 론

한국은행에 따르면 2010년 기준 국내 금융서비스 전달 채널 중 현금자동입출기기(Automatic Teller's Machine, 이하 ATM)의 업무처리 비중은 38%로, 인터넷뱅킹(35%), 창구(14%), 텔레뱅킹(13%)을 제치고 가장 유용한 채널로 자리 잡고 있다. 2009년 기준 국내 ATM설치 대수 및 이용건수는 10.2만대, 약 40억 건으로 추산되고 있으며 설치 장소 또한 은행 내부뿐만 아니라 편의점, 대형마트, 쇼핑몰, 공공장소 등으로 확대되었다[1,2].

현재 대부분의 ATM의 경우 금융서비스를 받기 위하여 이른바 Personal Identification Number(PIN)이라 불리는 4자리의 숫자 비밀 번호를 입력하는 방식을 이용한다. 설치 장소가 노출되어 있는 ATM의 특성상 PIN의 입력 과정 또한 다른 사람에게 노출되기 쉽고 PIN이 외우기 쉬운 숫자 4자리에 불과하기 때문에, 악의적인 목적으로 사용자의 입력과정을 주시하여 PIN 비밀번호를 유추하려는 공격들이 쉽게 발생하고 있다. 이러한 공격은 사용자의 어깨넘어로 훔쳐보는 과정에서 일어난다는 의미에서 "어깨넘어 훔쳐보기(shoulder surfing)" 공격이라고 불린다.

어깨넘어 훔쳐보기 공격에 대응하기 위하여 다양한 기법들이 연구되고 있다. 입력하는 숫자 키의 위치를 랜덤하게 바꾸는 방식은 이미 현재 많은 ATM에 적용되어 있으며, PIN 비밀번호를 단순히 숫자가 아닌 문자나 다른 그림으로 확장하여 사용하는 방법들도 연구되고 있다. 또한 사용자가 자신의 PIN 비밀번호를 바로 입력하는 것이 아니라 입력과정에서 ATM에서 매번 주어지는 방식으로 PIN 번호를 변형하여 입력하는 방법들 또한 개발되었다.

다양한 연구 및 개발 결과에도 불구하고 ATM의 입력 과정이 크게 변화되지 않고 어깨넘어 훔쳐보기 공격이 아직까지 유효한 이유는 크게 1) 오랜 시간동안 사용되어오던 숫자 중심의 PIN 비밀번호에 대한 사용자 편향성과 2) 사용자에게 입력 시마다 단순히 비밀번호 암기만이 아닌 계산 과정을 강요하는 사용상의 불편성 때문이라 할 수 있다. 이 뿐만 아니라 악성코드에 의해 감염된 ATM 기기들은 공격자가 직접 훔쳐보지 않더라도 사용자가 ATM에 입력하는 내용을 공격자에게 전달함으로써 기존 기법들의 효과를 기대할 수 없게 되었다.

본 논문에서는 어깨넘어 훔쳐보기 공격에 대하여 효과적으로 대응하며 사용자의 편이성을 강조한 새로운 인증 방식을 제안한다. 제안하는 방법에서는 사용자 인증 시에 ATM과 함께 최근 널리 보급되고 있는 지문인식 스마트폰을 이용한 2단계 인증(two factor authentication)을 통하여 어깨넘어 훔쳐보기나 rogue ATM과 같은 공격에 효과적으로 대응하는 인증 기법을 제공한다. 제안하는 기법에서는 1단계에서는 인증 서버를 통하여 ATM과 스마트폰 기기 사이의 신뢰관계를 구축하고, 2단계에서는 ATM-스마트폰을 바탕으로 PIN 비밀번호 및 생체정보(지문)을 이용하여 사용자를 안전하게 인증한다.

2. 관련연구

현재 어깨 넘어 훔쳐보기 공격에 대항하기 위한 방법으로 대표적으로 그래피컬 패스워드에 대한 연구들이 진행

되고 있으며 기존 공인인증서의 신뢰도가 떨어지면서 지문인식을 통한 전자서명 구성 방안과 안전한 사용자인증을 하기 위한 많은 연구들이 진행되고 있다.

2.1 그래피컬 패스워드

스마트폰 환경에서 패스워드를 입력하는 사용자의 편의성 개선과 어깨 넘어 훔쳐보기 공격, 무차별 공격(Brute Force Attack)등을 막기 위한 그래픽 패스워드 방식이 있다[3]. 그래피컬 패스워드는 기존의 문자, 숫자 패스워드와는 달리 사용자가 사전에 지정한 그림들을 이용하여 인증하고자 하는 기기에서 제시하는 여러 그림들 중에서 자신이 지정한 그림을 이용하여 인증을 받는 방식으로, 기존 텍스트나 숫자 기반의 비밀번호보다 월등히 큰 비밀번호 영역(domain)을 가질 수 있으며 다양한 형태로 조합이 가능하기 때문에 공격자가 손쉽게 구성이나 내용을 파악하기 어렵다는 장점을 가지고 있다. 하지만 이는 사용자에게도 적용되는 문제로 사용자가 자신이 지정한 그림을 다시 기억해내기가 어렵고 어깨넘어 훔쳐보기 공격의 난이도가 다소 높아졌을 뿐 여전히 공격의 위험성이 남아있다는 문제점을 가지고 있다.

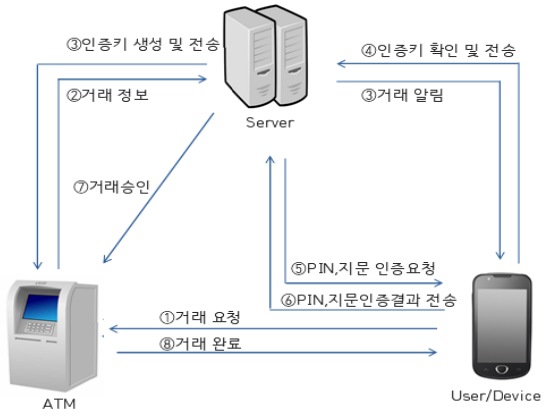
2.2 지문을 이용한 인증의 확대

지문은 대표적인 생체정보인증방법으로 금융기관가 같이 몇몇 지정된 장소에서 강력한 인증 방법으로 사용되고 있다. 공인인증서의 취약점들이 제시되면서 신뢰도가 떨어지는 경우에도 지문을 이용한 공인인증서 인증 및 폐기 기법들이 연구된 것처럼 지문은 기존의 인증을 강화하는 좋은 수단으로 제시되어 왔다[4].

지문이 가지는 인증의 효과가 큼에도 널리 사용되지 못하는 이유는 지문 인식을 위한별도 장치가 필요하기 때문이었다. 하지만 최근 많은 스마트폰에서 지문 인식 장치를 내장하여 지문을 스마트폰 잠금 해제나 어플리케이션 구입을 위한 인증 과정에서 사용하면서, 지문을 이용한 인증 방법이 다시 각광받고 있다.

3. 제안 방안

3.1 제안시스템의 개요 및 구성



(그림 1) 제안시스템의 동작 과정

본 논문에서 제안하는 방법은 ATM 거래 인증을 위하여 1) 인증서버와 ATM간의 통신을 통한 인증번호 제시, 2) 스마트폰에 인증번호 입력을 통한 기기 신뢰도 확보, 3) 생체인증 수단으로 스마트폰 지문 입력을 통한 보안강화의 3단계로 구성된다. 따라서 인증서버-ATM-스마트폰 간의 신뢰 정보 구축을 바탕으로 인가된 사용자만이 제공할 수있는 지문을 입력함으로써 안전한 인증 절차가 수행된다.

사용자의 입력 자체는 ATM이 아닌 스마트폰을 통해서 이루어지기 때문에, rogue ATM에 의한 정보 누출을 최소화 할 수 있으며, 입력과정이 쉽게 노출되지 않기 때문에 어깨넘어로 훔쳐보기의 공격의 효과가 최소화된다. 또한 사용자는 기존의 PIN 비밀번호 방식에 지문 입력과정만이 추가되었기 때문에 시스템 이용의 편이성 또한 크게 저해되지 않는다는 장점이 있다.

3.2 제안시스템 과정

(그림 1)은 제안하는 방법의 구성 및 과정을 보여준다. 제안하는 방법은 다음과 같이 진행된다. 사용자가 ATM을 통해 금융서비스를 요청하면 사용자의 스마트폰, ATM, 금융서버에서 일어나는 일련의 모든 통신 과정은 암호화하고 사용자의 지문은 사용자의 스마트폰에 등록되어 있으며 해당 금융기관의 지문인식기능을 지원하는 어플리케이션이 설치되어 있다고 가정한다.

Step 1: 금융서비스를 받고자 하는 사용자는 ATM에 카드 또는 통장을 삽입하고 화면에서 서비스 및 거래내용 입력

Step 2: ATM은 서버에 카드 또는 통장 정보 및 거래내용을 전송하고 금융기관은 거래하고자 하는 사용자의 정보를 식별.

Step 3: 인증서버는 사용자 스마트폰에 Push Notification 등의 방법을 이용하여 거래 사실을 알리고 사용자가 확인을 하면 인증번호 생성 후 ATM에 전송, ATM은 화면에 전송받은 인증번호 출력

Step 4: 사용자는 ATM 화면에 출력 된 인증번호를 확인하고 스마트폰에 입력하여 인증서버에 전송

Step 5: 사용자가 정확히 인증번호를 입력했으면 인증서버는 거래정보를 고객에게 전송하고 확실한 사용자 인증을 위해 스마트폰을 통한 사용자 지문 및 PIN 4자리 입력 인증을 요청

Step 6: 사용자는 스마트폰에 거래 정보가 출력되면서 거래에 대한 최종 확인 후 PIN 비밀번호를 입력하고 스마트폰의 지문인식 기능을 이용하여 사용자의 지문을 정보화하여 인증서버에 전송

Step 7: 인증서버는 사용자의 지문과 PIN 비밀번호를 이용하여 사용자 확인 후 사용자가 인증되었다면 최종 거래 승인하고 ATM에게 요청한 거래가 승인되었다고 알림

Step 8: ATM은 고객에게 요청한 거래가 완료되었음을 알려주고 서비스 완료

4. 어깨넘어 훔쳐보기 공격의 보안성 분석

본 논문에서는 ATM 사용자에 대해 공격자가 직접 사용자의 입력을 염탐하는 '직접 어깨넘어 훔쳐보기' 공격과 ATM 기기의 장악 또는 카메라 설치 등의 추가 작업을 통하여 사용자의 입력 정보를 노출시키는 '확장된 어깨넘어 훔쳐보기' 공격을 가정한다.

직접적인 어깨넘어 훔쳐보기 공격 성공은 1) 훔쳐보기의 용이성과 2) 입력의 재현 가능성의 두 가지 조건에 의해서 결정된다. 기존의 ATM 인증 방식의 경우에는 큰 화면 또는 위치에 따라 숫자를 쉽게 유추할 수 있는 키패드를 통해서 4자리의 PIN 숫자만을 입력하였기 때문에, 주변에 위치한 공격자가 입력과정에서 PIN 정보를 쉽게 얻어낼 수 있었으며, 같은 번호를 반복하기만 하면 되기 때문에 입력이 재현 가능하여 어깨넘어 훔쳐보기 공격이 성공할 수 있었다. 게다가 ATM 기기의 입력을 가로채거나 별도의 장비를 이용하는 확장된 어깨넘어 훔쳐보기 공격의 경우는 사용자의 입력정보를 더 정확하고 쉽게 얻어낼 수 있다는 점에서 어깨넘어 훔쳐보기 공격의 성공률을 더 높일 수 있었다. 하지만 제안하는 기법에서는 사용자의 PIN 입력은 ATM보다 크기가 작고 쉽게 감출 수 있는 스마트폰을 통해서 이루어지고 있으며 ATM에 직접적으로 입력되는 정보가 없기 때문에 ATM을 장악하거나 카메라를 설치한다고 하여도 노출되는 정보가 없다. 또한 인가된 사용자만이 제공할 수 있는 생체정보인 지문을 이용하고 있기 때문에 공격자의 입력 재현 가능성은 현저하게 떨어진다. 즉, 제안하는 기법은 공격자에게 낮은 훔쳐보기의 용이성 및 입력 재현 가능성을 강제함으로써 안전한 인증이 가능하도록 한다.

5. 결론

본 논문에서는 스마트폰 지문인식 기능을 이용한 ATM기기에서의 이중 사용자 인증 방법을 제안하였다. 제안하는 방법은 기존 ATM에서 사용하던 PIN 기반의 사용자 인증 방식이 어깨넘어 훔쳐보기 공격에 취약하다는 점을 지적하고 스마트폰과 생체정보를 이용하여 어깨넘어 훔쳐보기 공격에 대응하는 새로운 인증 방법을 제안한다. 특히 안전한 인증 과정을 위하여 2단계에 걸쳐 ATM과 스마트폰, ATM과 사용자 사이의 신뢰관계를 구축할 수 있도록 기법을 구성하였다. 이는 지문인식과 같이 생체정보를 입력받을 수 있는 스마트폰이 보급이 활성화되고 있는 현재의 상황에서 효과적인 사용자 인증 방법으로 활용될 수 있을 것으로 기대된다.

참고문헌

[1] 한국은행, "우리나라 및 주요국의 지급결제제도", 2010. 8.

[2] 금융결제연구소, "국내외 ATM 현황 및 시사점", 지급결제와 정보기술, 44호, pp. 68~96, 2014. 4.

[3] 김태은, 김현홍, 전문석, "스마트폰 GPS 기반 그래피컬 패스워드 기겁에 관한 연구", 정보처리학회논문지, 컴퓨터 및 통신시스템, 2 권, 12 호, pp. 525~532, 2013.

[4] 박국환, "스마트폰에서 지문을 이용한 전자서명 구성방안", 숭실대학교 대학원, 학위논문(석사), 2013.