생체인증을 통한 핀테크 결제 시스템 공격기법

김정훈, 윤다예, 이근호
백석대학교 정보통신학부
e-mail:security_jh@bu.ac.kr, ydelin@bu.ac.kr, root1004@bu.ac.kr

A Scheme of Fin-Tech Payment System Attacks using Biometric Authentication

Jung-Hoon Kim, Da-Yea Yoon, Keun-Ho Lee
Division of Information & Communication, Baekseok University

요 약

앞으로 IoT가 활성화 됨에 따라 IoT 디바이스(TV, 냉장고, 카트 등)에서 결제가 가능한 시스템이 보편화 될 것이다. IoT에 핀테크 결제 시스템이 융합되어 결제 시스템이 간소화 되면서 인증 시스템 또한 간소화 되고 있다. 편리성을 추구하는 핀테크 결제 시스템은 보안에 더욱 취약해질 것으로 예상된다. 현재의 핀테크 결제 시스템을 대상으로 패스워드 인증방법의 취약점과 지문 인증방법의 취약점을 도출하여 공격 시나리오를 제안한다. 본 논문에서는 지문 패턴 인증을 통하여 편리성을 유지하면서 보안을 강화하는 대응방안을 제안한다.

1. 서론

앞으로 IoT가 활성화 됨에 따라 IoT 디바이스(TV, 냉장고, 카트 등)에서 결제가 가능한 시스템이 보편화 될 것이다. IoT에 핀테크 결제 시스템이 융합되어 결제 시스템이 간소화 되면서 인증 시스템 또한 간소화 되고 있다. 본 논문에서는 지문 패턴 인증을 통하여 편리성을 유지하면서 보안을 강화하는 패턴을 활용한 지문인식 시스템을 이용한 대응방안을 제안한다.

2. 관련연구

2.1 핀테크

금융을 뜻하는 파이낸셜(financial)과 기술(technique)의 합성어로 모바일 결제 및 송금, 개인자산관리, 크라우드 펀딩 등 정보기술(IT)을 기반으로 한 새로운 형태의 금융 기술을 말한다. 핀테크 비즈니스 모델과 사업 영역을 분류하는 기준은 크게 은행업 및 금융 데이터 분석(Banking & Data Analytics), 지급 결제(Payment), 자본시장 관련 기술(Capital Market Tech), 금융자산 관리(Finance Management) 등 4가지 영역으로 정리돼 가고 있다.

핀테크의 등장은 기존의 금융 질서를 파괴하며 창의와 혁신에 바탕을 둔 비즈니스 모델들을 쏟아내고 있다. 통화의 종류, 결제 시스템 같은 기존의 장벽을 허물고 보다 간편하고 보안 이슈까지 잡은 기술들이 속속 등장하기 때문이다. 최근 들어서는 단순한 결제나 송금 서비스뿐만 아니라 고객의 개인정보·신용도·금융사고 여부 등을 빅 데이터 분석으로 정확하게 파악하는 알고리즘 기술까지 등장해 개인 자산 관리 서비스까지 그 영역을 확대 중이다.

2.2 핀테크 결제 시스템

핀테크 결제 시스템은 대한민국에서 신 성장 산업이자 창조산업이다. 엑티브X, 공인인증서를 대체제로 기업, 국가의 적극적인 지원을 통해 결제 시장의 혁신 중심지로 성장하고 있다. 현재 핀테크 결제시스템의 인증 방법으로 패스워드 6~8자리만 입력하게 되어있다[1].

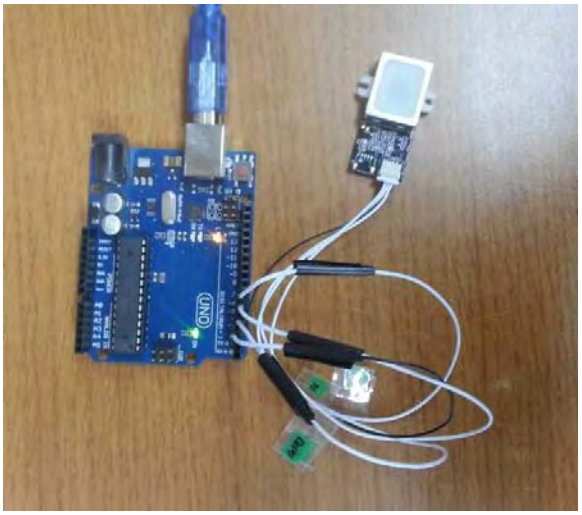
(그림 1) 핀테크 간편 결제 시스템

국외 시장 현황으로 그림 2와 같이 전망이 밝은 것을 보아 생체인증과의 융합과 많은 발전이 있을 것으로 예상된다.

(그림 2) 국외 핀테크 현황

2.3 지문 인증

지문생체 인증은 실험실 및 군사 기지와 같은 높은 보안 수준을 요구하는 장소에서 접근 제어를 위해 널리 채택되었다. 최근에는 거주지 출입통제, 사내 출입통제로 활용되고 있다. 모바일 기기에 지문 스캐너를 홈버튼에 장착함으로써 생체 인증이 앞으로 핀테크 결제 시스템을 넘어 사소한 인증 시스템의 보안을 위해 활용될 수 있다[2].



(그림 3) 아두이노를 활용한 지문인식 시스템

스마트폰 이외에도 공공 부문에서 모바일 지문인식 기기들을 이용하여 법 집행이나, 공항, 항구, 국경, 기업 시설, 네트워크 보안, 출입 통제 등을 위하여 사용된다.

3. 공격 시나리오

현재의 핀테크 결제 시스템은 패스워드기반으로 패스워드 6~12자리만 입력하면 된다.

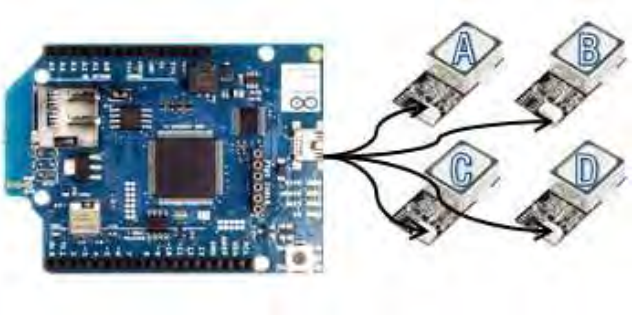
패스워드 취약점 첫 번째로 보안에 취약하다. 6~12자리는 누군가 몰래 스마트폰을 훔쳐봐서 쉽게 외울 수 있는 암호이므로 심각한 취약점이 발생한다.

또한 사용자 식별이 불가능하다는 취약점이 있다. 피의자가 피해자의 스마트폰을 훔쳐본 후 스마트폰을 훔쳐 결제를 해도 피의자가 결제 했는지 피해자가 결제 했는지 사용자 식별이 불가능하다[3,4].

4. 대응방안

4.1 패턴을 활용한 지문인식 시스템

스마트폰 또는 IoT 디바이스에 그림 4와 같은 지문인식 설계도처럼 4개의 지문인식 센서를 부착한다. 지문인식 A,B,C,D 센서로 패턴인식한다.



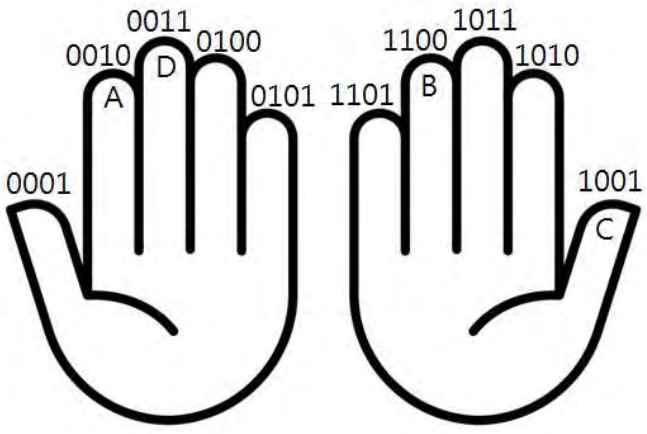
(그림 4) 지문 패턴인식 설계도

①. 은행에서 신용카드 패스워드 등록 시 손가락 4개를 A,B,C,D 원하는 위치에 등록한다.

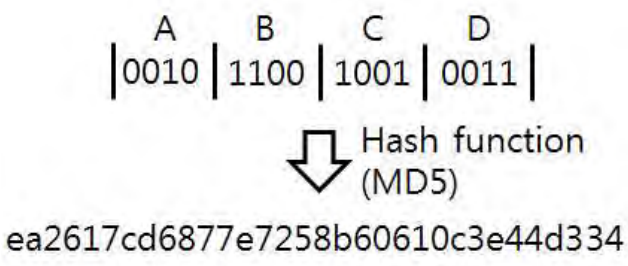
②. 예를 들어 손가락 4개를 등록했을 때 왼손 검지 - A / 오른손 약지 - B / 오른손 무지 - C / 왼손 중지 - D 순으로 등록한다.

③. 결제 할 때 등록한 순서대로 왼손 검지 - A / 오른손 약지 - B / 오른손 무지 - C / 왼손 중지 - D 순으로 등록한다. 인식하여 결제한다.

④. 해당하는 손가락을 다쳤을 경우 은행에 방문하여 다시 지문패턴을 다시 등록한다.



(그림 5) 손가락별 지문데이터



(그림 6) 지문데이터 비교검증

은행에 등록된 지문데이터 ea2617cd6877e7258b60610c3e44d334와 지문 패턴 인식 시스템에서 인증된 데이터 ea2617cd6877e7258b60610c3e44d334를 비교하여 결제 가능 유무를 판단한다.

기존에 나와 있는 애플, 삼성 등의 지문인식 핀테크 결제 시스템은 등록된 지문이 유출당하면 쉽게 해킹에 노출되어 있다. 제안하는 대응방안은 10개의 손가락 모두 유출당해야하며 또한 A,B,C,D에 왼손, 오른손, 몇 번째 손가락의 패턴까지 알아야 한다.

5. 결론

본 논문에서 현재의 패스워드 기반으로 핀테크 결제 시스템의 취약점 시나리오를 제안하였다. 제안한 취약점 시나리오의 대응방안으로 패턴을 활용한 지문인식 시스템을 제안하였다. 앞으로 IoT 발전과 핀테크 결제 시스템의 활성화와 발전 가능성으로 보아 편리하고 보안성이 뛰어난 생체인증 시스템이 도입될 것으로 예상된다. 이에 따라 패턴 인증 방식으로 편리성, 수용성을 유지하면서 좀 더 강화된 보안성을 갖춘 패턴을 활용한 지문인식 시스템이 채택될 가능성이 높다고 판단된다.

감사의 글

이 논문은 2013년도 정부(미래창조과학부)의 재원으로 한국연구재단의 기초연구사업 지원을 받아 수행된 것임 (2013R1A1A1A05012348)

참고문헌

[1] Pil-ju Choi, Sang-Seon Park, Dong-Ggyu, "Mobile payment and biometric fusion technology trend", KIPS, Vol. 22, Vol. 4, pp. 21-28, 2012.

[2] Kwang-Sun Park, Sang-jin Lee, "A Study on Structural Vulnerability of MobilePhone Micropayment System And Improvement of Standard Payment Module for User Protection", KIPS, Vol. 23, No. 8, pp. 1007-1015, 2013.

[3] Jun-Yeop Lee, Gyeong-Jeon Lee, "Virtualization Smart Card (ViSCa) platform based mobile payment Service offerings and other comparative analysis of the case", KIISS, Vol. 20, No. 2, pp. 163-178, 2014.

[4] Byeong-Gwan Lee, Eun-hui Jeong, "Safe AKA (Authentication Key Agreement) module designed for mobile payment systems for open smartphone environment", KMMS, Vol. 13, no. 11, pp. 1687-1697, 2010.