The Journal of The Institute of Internet, Broadcasting and Communication (IIBC)
Vol. 15, No. 4, pp.25-31, Aug. 31, 2015. pISSN 2289-0238, eISSN 2289-0246

http://dx.doi.org/10.7236/JIIBC.2015.15.4.25
JIIBC 2015-4-4

핀테크 환경의 안전한 결제를 위한 인증 기법에 관한 연구

A Study on Authentication Method for Secure Payment in Fintech Environment

박중오*, 진병욱**

Jung-Oh Park*, Byung-Wook Jin**

요 약 핀테크(FinTech: Financial Technology)는 IT 기술을 이용하여 금융 서비스를 효율적으로 만드는 기술로 정의한다. 핀테크 기술은 빅 데이터와 IT플랫폼을 통한 혁신적인 기술이며, 기존의 금융시스템의 보안성 및 문제점을 개선하는데 크게 개선할 것으로 기대되고 있다. 국내의 금융기관에서는 효율성 있고 안전한 서비스를 사용자로부터 제공하기 위해 기술도입과 투자를 하고 있다. 그러나 금융환경에서는 정보유출, 보안사고가 발생하여 고객의 신뢰를 얻지 못하고 있으며, 신규 및 변종의 보안위협 및 공격기법이 발생하고 있다. 그러므로 본 논문에서는 핀테크 환경에서 사용자로부터 안전한 결제 시스템에 관하여 연구하여 인증기법을 설계하도록 한다. 제안된 논문은 금융환경에서 발생한 공격기법에 대해서 안전성을 분석하여 기존의 시스템과 보안성을 평가하였다.

Abstract FinTech(Financial Technology) is defined as the technique to create efficient financial services using IT technologies. FinTech is an innovative technology through IT platform and big data, and is expected to improve the security and problems of the conventional banking system. Domestic financial institutions has introduced the technologies and investment in order to provide safe and effective services to users. However, In the financial environment, information disclosure and security incident has occurred so they has lost the trust from their customers. Moreover new variant of the security threats and attack techniques have occurred. Therefore, in this paper, we designed a authentication scheme for secure payment system in FinTech environment. The proposed study evaluated the stability of the existing security systems with respect to attack methods occurred in the financial environment.

Key Words : Fintech, Authentication, E-Commerce

Ⅰ. 서 론

금융 산업과 ICT융합기술을 통하여 금융시장에 혁신적인 요소와 부가가치를 창출하며 급격하게 성장하고 있다. 이러한 기술을 핀테크(Fintech)라 정의하고 있으며 사용자들로부터 활발한 금융서비스를 제공을 목표로 하며 현신적인 트랜드로 주목받고 있다[1,3]. 오프라인 서비스 중에서 온라인, 스마트기반으로 확대되고 있으며 Apple, Google, Paypal 등 국외 ICT 기업에서 금융서비스의 제공 범위를 지속적으로 확대하고 있다[2].

*정회원, 동양미래대학교 정보통신과
**준회원, 숭실대학교 컴퓨터학과 (교신저자)
접수일자 2015년 7월 21일, 수정완료 2015년 8월 7일
게재확정일자 2015년 8월 7일

Received: 21July, 2015 / Revised: 7 August, 2015 /
Accepted: 7 August, 2015
**Corresponding Author: quddnr4511@naver.com
Dept of Computer Science and Engineering, Soongsli University, Korea

또한 핀테크 기술은 사용자들이 기존의 금융환경보다 안전하고 편리하게 금융서비스를 접근하고 안전하게 결제, 송금, 거래하는 서비스를 수행하기를 원한다. 이에 따라 사용용자들로부터 편리하고 혁신적인 기술을 적용하기 위해서는 안전한 보안 기술을 제공해야 한다. 하지만 다양한 금융 서비스를 제공하기 위한 측면에서는 해킹, 신•변종 보안위협, 보안위협들에 대한 증가로 많은 어려움이 발생하며 어려움에 직면하고 있다[4].

국내에서는 2013년 카드사의 개인정보 유출사고, POS 시스템 해킹과 같은 전자침해사고에 대한 안전성 우려가 높아지고 있다. 그러므로 본 논문에서는 핀테크 환경에서 사용자들이 스마트폰을 활용하여 안전한 결제를 위한 인증 기법에 대하여 연구를 하도록 한다.

본 논문은 5장으로 구성되어 있다. 2장은 관련연구 항목으로 핀테크 환경 및 주요기술이며, 금융환경의 보안 요구사항이 작성되어 있으며, 3장은 제안 프로토콜은 기기등록 및 사용자인증, 결제 진행절차에 대하여 작성하였다. 4장은 3장의 제안된 프로토콜을 기반으로 안전성 분석 및 보안성에 대하여 평가를 하였다. 마지막 5장 결론에서 핀테크 환경의 연구 및 방향을 제시하고 끝낸다.

II. 관련연구

1. 핀테크 환경 및 국내외 산업현황

융합시대가 도래하면서 하나의 분야만 고수하며 분석 할 수 없는 시절이 다가오고 있다. 금융환경과 IT환경의 합성어인 핀테크가 대표적인 예라고 할 수 있으며 최근 글로벌 트랜드로 불어오고 있다. 과거시절에는 금융환경 내부에서 IT기술이 운영되어 왔지만 현재는 스마트기기를 통하여 비금융회사가 주도하면서 금융영역으로 들어오고 있다[2,5].

예를 들어 금융환경 및 서비스는 인터넷환경의 은행, 증권에서 모바일 기반의 은행, 증권 서비스로 확대되어지고 있으며, IT기업의 경우 독자적으로 또는 금융기관과 제휴를 통하여 전자결제, 송금, 자산관리 등의 서비스가 확대되어 지고 있다[6].

핀테크 환경이 발전하고 활성화가 됨에 따라 2008년부터 2013년까지 대략 3배이상의 투자금액이 증가하고 있으며, 금융데이터분석과 소프트웨어 부문의 투자비중이 증가하고 있다[2].

국외에서 살펴보면 영국의 핀테크 산업이 전 세계적으로 주목받고 있으며 국가적인 차원에서 차세대 성장 동력으로 채택하여 규제완화, 자원지원을 적극적으로 지원하고 있다. 미국의 경우 실리콘밸리와 뉴욕을 중심으로 핀테크 산업이 활발해지고 있으며 기존의 페이스북, 구글, 이베이 등과 같은 대형 ICT기업들도 금융업진출을 하고 있다. Apple의 Apple Pay는 편리성과 보안성 부분에서 사용자들로부터 충족시키고 있다. 또한 중국은 정부로부터 지원을 전폭적으로 받아 알리바바라는 글로벌 회사가 설립되어졌으며 모바일 시장규모 또한 5억 명으로 활발하게 진행되고 있다[1].

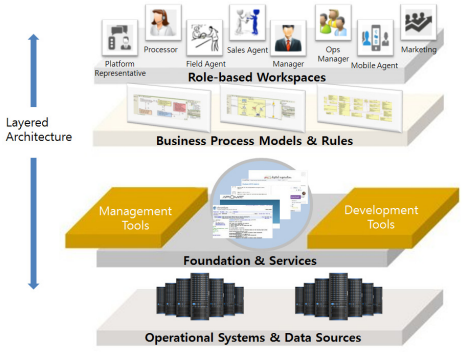

그림 1. 핀테크 구조
Fig. 1. Fintech Architecture

국내에서는 2014년 기점으로 스마트폰 가입자가 4000만명이 넘고 있으며, 모바일 뱅킹, 모바일 카드를 활용하여 스마트 시장이 급속도로 발전하고 있다. 국내 모바일 시장 규모도 급격하게 커지고 있으며 2014년 2분기만에 3.2조원으로 13.1증가하고 있다. 국내 기업에서도 모바일 금융화가 활성화되면서 핀테크 산업에 대한 관심도가 높아지고 있으며 기술연구가 진행되어 지고 있다.

2. 금융환경 보안위협 및 요구사항

핀테크 서비스는 사용자의 편의성이 중시되어지고 간편하지만 크로스 사이트 요청위조(CSRF)와 같은 계정이 탈취되는 공격과 인터넷기반으로 서비스가 수행됨으로서 서비스 거부공격(DOS), 세션 하이재킹(Session hijacking)등과 같은 보안위협에 노출도리 수 있다. 비금융관련 회사에서는 핀테크 환경에 접목됨에 따라서 개인정보와 같은 민감한 정보를 관리하지 못할 수도 있다.

더 나아가서 금융정보가 목표화되어서 대규모 공격을 받을 수가 있으며 스마트기기를 사용한 데이터의 증폭으로 인해서 대규모 공격을 받을 수 있다[2,7].

핀테크환경에서 보안위협을 살펴보면 크게 인증측면, 서비스측면, 규제측면으로 나눌 수 있다. 개방형 모바일 플랫폼으로 설계된 스마트기기의 취약점을 이용한 ID 도용, 추가인증 우회, 피싱 및 파밍공격에 위협될 수 있으며, 서비스 측면에서는 비인가된 사용자의 취약성을 노리는 공격, 사회공학적공격이 발생할 수 있다. 보안규제 측면에서는 기업에서 수주로 받는 외주형태의 책임불가 또는 책임영역이 모호해 질수가 있어서 보안위협으로 안전할 수 있는 견고한 규제 및 정책이 필요하다[8].

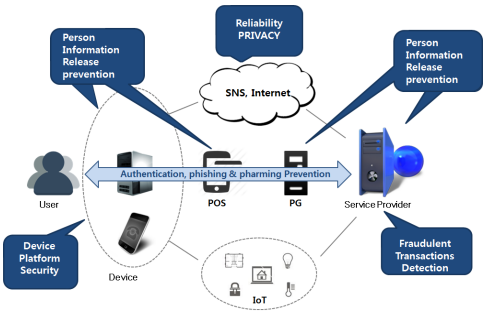

그림 2. 금융환경의 보안 위협 사항
Fig. 2. Security Threat Details In E-Commerce

이러한 보안위협이 발생함으로 인해 금융보안연구원에서는 모바일환경에서 금융서비스를 제공시 보안 요구사항은 다음 표 1과 같다.

표 1. 모바일 기반의 전자금융서비스를 위한 보안 요구사항
Table 1. Security Requirement for E-Banking Services In base Mobile

적용사항	설명
앱 무결성 검증	코드, 데이터 파일등에 무결성이 검증되어야 하며, 결제상태에서 주기적으로 검증되어야 함
악성코드 위협 대응	앱이 실행되기 시점에서 악성코드 감염여부가 진행되어야 함
암호 적용	중요정보 암호 적용, 암호키 관리, 알고리즘, 프로토콜 등은 안전성을 고려해야 함.
통신 구간의 암호화	유무선 통신구간에서 정보가 유출되지 않아야 함.
중요정보 암호화	End to End 즉 스마트기기에서 서비스 제공자까지 데이터가 암호화를 수행하여 전송되어야 함
거래전문 무결성 검증	거래값에 대한 해쉬값과 무결성은 검증되어야 함
키 관리	키 생성, 설정, 유효기관, 분배, 복구 및 파기 등의 안전하게 키가 관리되어야 함

Ⅲ. 제안프로토콜

본 논문에서는 핀테크 환경에서 안전한 거래를 위한 통신 프로토콜을 설계한다. 기기 등록 및 사용자 인증 프로토콜에 관하여 설계하며, 결제 진행 프로토콜에 관하여 연구한다. 우선 사용자는 스마트폰을 사용하여 사용자를 등록 후 서비스 제공자로부터 결제를 수행한다. 제안된 논문의 전제 조건은 다음과 같으며, 본 절에서 나오는 수식은 표 2과 같다.

표 2. 약어표
Table 2. abbreviation

Symbol	Description
IMSI	Subscriber Identifier
CIV	Certification Identification Value
MAC_{SP}	Mac Address
UIV	User Identification Value
RIGHT	Right Operation
$USER_{Cert}$	User of Certification Value
$Auth_{Value}$	Authentication of Value
TS	TimeStamp
PUB_TSM	Public Key of Encryption for TSM
PUB_SP	Public Key of Encryption for SP
PRI_SP	Private Key of Encryption for SP
Hash	Hash Function

1. 프로토콜 환경에서 기기는 스마트폰 기준으로 수행되며, LTE기반 기술을 참조한다.
2. 공개키 기반의 암호화를 사용하며, 기기는 Hash Function을 수행할 수 있다.
3. TSM는 기기의 $IMSI, MAP_{SP}$를 검증할 수 있으며 Certificate Authority의 역할을 수행한다.

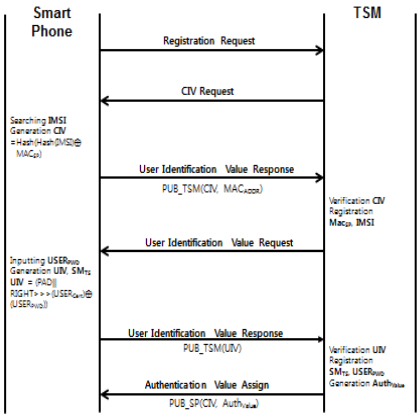

그림 3. 사용자 인증 및 기기 등록 프로토콜
Fig. 3. User Authentication And Devce Registration Protocol

1. 기기 등록 및 인증

사용자는 스마트폰을 이용하여 TSM로부터 사용자 인증을 완료 후 기기를 등록한다. 사용자의 패스워드 인증값과 기기의 식별번호와 기기의 MAC Address, 가입자 식별자를 검증을 한다. 기기 등록 및 인증절차는 아래 그림 3과 같다.

1. 사용자는 스마트폰을 이용하여 TSM로부터 등록요청 메시지를 전송한다.

2. TSM는 사용자로부터 $IMSI$을 검색 후, CIV를 생성한다.

$$CIV = Hash(Hash(IMSI) \oplus MAC_{SP}) \quad (1)$$

3. 스마트폰에서 TSM로 CIV, MAC_{Addr}을 TSM의 공개키로 암호화해서 CIV 메시지를 전송한다.

$$PUB-TSM(CIV, MAC_{SP}) \quad (2)$$

4. TSM는 CIV를 검증하고 스마트폰의 $MAC_{SP}, IMSI$을 등록한다.

5. TSM는 UIV를 검증하기 위해 스마트폰으로부터 UIV를 요청한다.

6. 사용자는 스마트폰으로 사용자의 비밀번호, 패턴, 이미지 암호화를 사용하여 $USER_{PWD}$를 생성한다.

$$UIV = (PAD \| \gg (USER_{Cert}) \oplus (USER_{PWD}) \quad (3)$$

7. UIV를 TSM의 공개키로 암호화하여 TSM로 전송한다.

8. UIV를 검증하고 타임스탬프, $USER_{PWD}$를 등록한다. 이후 $Auth_{Value}$를 생성 후 스마트폰으로부터 $Auth_{Value}$ 배정한다.

$$PUB-SP(Auth_{Value}) \quad (4)$$

2. 결제 진행 절차

등록 및 인증과정이 끝나고 사용자는 서비스 제공자로부터 결제 진행 절차를 진행한다. 등록 및 인증과정에서 추출한 사용자 신원 값을 추출 후 검증하며 타임스탬프를 비교한다. 결제 진행절차는 그림 4와 같다.

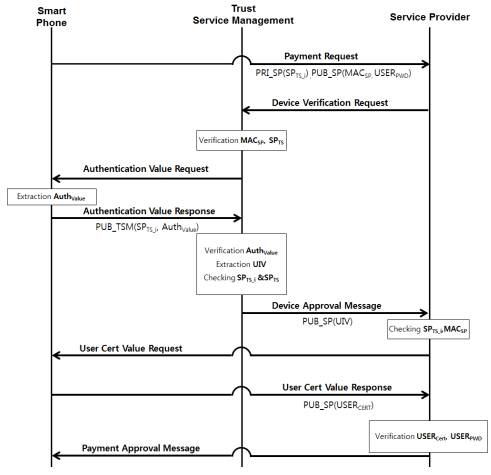

그림 4. 결제 진행 프로토콜
Fig. 4. Payment Processing Protocol

1. 사용자는 스마트폰을 활용하여 결제를 진행할 때 서비스 제공자로부터 결제 요청 메시지를 전송한다.

$$PRI-SP(ST_{TS-i}), \quad (5)$$
$$PUB-SP(MAC_{SP}, USER_{PWD})$$

2. 서비스 제공자는 수신한 값을 검증하기 위해 TSM

로부터 검증 요청 메시지를 전송한다.

3. TSM은 MAC_{SP}, SP_{TS}를 검증 후 스마트폰으로부터 인증 값을 요청 한다.

4. 스마트폰에서 $Auth_{Value}$를 추출하고 TSM로부터 인증 값을 전송한다.

$$PUB- TSM(SP_{TS-i}, Auth_{Value}) \quad (6)$$

5. TSM는 $Auth_{Value}$를 검증하고 UIV를 추출한 다음 SP_{TS-i} SP_{TS}를 비교한다. 이는 최근에 접속여부를 판단하기 위한 것이다.

6. 요청한 값의 응답메시지를 서비스 제공자로부터 전송한다. 그리고 SP_{TS-i}, MAC_{SP}를 검증한다.

7. 스마트폰으로부터 사용자 인증값을 요청 후 송신받고 $USER_{Cert}$, $USER_{PWD}$를 검증한 다음 결제 승인 메시지를 전송한다.

Ⅳ. 성능평가

1. 안전성 분석

- 중간자 공격 및 세션 하이재킹

중간자 공격은 공격자가 취약한 디바이스에 접근을 하여 전송되고 있는 데이터를 손상시키거나, 정보를 변경하는 기법을 말한다. 제안된 프로토콜에서는 이를 해결하기 위해 사용자 인증과정에서 CIV, UIV를 생성 후 인증 및 기기 등록하였으며, 이를 활용하여 결제 시스템에서 검증함으로서 중간자 공격을 막을 수 있다.

- 기밀성 및 무결성 위협

디바이스로부터 생성된 정보와 TSM와 서비스 제공자의 데이터는 상호간의 통신을 수행할 때 기밀성와 무결성에 대한 위협이 없어야 한다. 이에 따라 보안위협을 강화하기 위해서는 공개키 방식의 암호화를 사용하였으며, 이중 해쉬 함수와 Right연산을 활용하여 통신 프로토콜을 설계하였다. 또한 무결성을 검증하기 위해 SP_{TS}, SP_{TS-i}를 검사하여 데이터를 보호하였다.

- 피싱 및 가장공격

금융환경에서 대표적인 피싱 및 가장공격은 기기의 원래 소유주가 아닌 악의적인 목적을 가진 비인가 된 사용자가 실체가 할 수 있는 행위를 수행함으로써 금전, 개인정보를 탈취하는 공격을 말한다. 사용자 등록가정에서 사용자의 패스워드와 인증값을 확인하며, 기기의 $IMSI$를 검증함으로서 가장공격을 불가능하게 한다. 결제 과정에서는 타임스탬프를 검사하고 등록과정에서 생성된 $USER_{PWD,}$ $USER_{Cert}$를 확인 후 UIV를 검증함으로써 피싱 및 가장공격에 대하여 안전하다.

- 재생공격

재생공격은 핀테크 환경뿐만 아니라 금융환경에서 발생하는 공격이다. 공격자가 이전 인증 처리를 수행하는 과정에서 정보를 획득하여 다시 공격하는 방법이다. 하지만 본 논문에서는 사용자가 생성한 $USER_{PWD}$ (ex. 비밀번호, 패턴, 이미지 암호화방식)와 $USER_{Cert}$를 활용하여 UIV를 검증하였다. 또한 TSM에서 $Auth_{Value}$를 사용자로부터 부여하여 결제 시스템에서 검증하므로 재생공격은 실패한다.

2. 보안성 평가

본 절에서는 제안된 방식의 Factor, 채널, 입력방식, 공격기법, 연산속도, 특징에 대하여 보안성을 비교하였다. 기존의 시스템에서는 OTP, 보안카드, 공인인증서, HSM을 사용하여 인증을 수행하며 상황에 따라 2채널 인증을 수행한다. 제안된 프로토콜에서는 1채널에서 패스워드, 인증값을 활용하였다. 입력타입은 터치패드로 Password를 입력하며 2채널 방식에서 ARS 안내에 따라 인증된 숫자를 입력한다. 기존의 환경에서 공격기법은 백도어, 피싱, 세션 하이재킹, 재생공격, 중간자 공격들이 존재한다. 수행속도에서는 제안된 프로토콜과 비슷하나 또 다른 Factor가 필요하였으며, 제안된 프로토콜의 특징에서는 1채널기반의 간단한 패스워드와 $Auth_{Value}$가 있다. 기존 방식과 제안된 방식의 보안성을 평가한 자료는 다음 표 3과 같다.

표 3. 기존 시스템과 제안된 방식의 보안성 비교
Table 3. Comparison of the security of the conventional method with the proposed method

Classification	Existing System	Proposed System
Factor	OTP, Security Card, PKI, HSM	User Memory, Certificate
Channel	Situationally 2 Channel	1 Channel
Input Type	H/P, PSTN	H/P
Attack Technique	Back door Phishing Session Hijacking Replay Attack MITM	-
Operation Speed	2E + 2H +1E(Another factor Need)	2E+1H+2E
Feature	Existing Payment System	1 Channel Based Simple Password Method And Auth Value

V. 결 론

핀테크 산업 환경이 주요화두로 부각되면서 발전됨에 따라 향상된 보안성과 안전성이 요구되어 지고 있다. 따라서 본 논문에서는 핀테크 환경에서 사용자 환경에 알맞은 인증 기법과 결제 진행 프로토콜에 관하여 연구하였다.

제안하는 방식은 사용자가 스마트폰을 활용하여 가입자 식별 값과 코드값을 활용하여 기기등록과 사용자 인증값을 활용하여 인증하였다. 결제시스템은 기기등록 과정에서 검증된 값을 기반으로 안전성 있게 결제과정을 설계하였다.

성능평가에서는 기존의 금융환경에서 발생했던 중간자 공격, 세션하이재킹, 가장공격, 재생공격, 피싱공격에 관하여 안전성을 분석하였다. 그리고 보안성 평가부분에서는 기존의 시스템과 보안성을 비교분석하여 요소, 채널, 공격기법, 특징에 관하여 평가하였다.

제안시스템에서는 기기 등록 및 인증과정에 대해서만 연구하였으나 사후 점검 강화 및 책임기준을 명확히 하기 위한 부정거래탐지시스템과 융합기술 대한 연구가 필요하다 향후, 제안된 기법을 확장하여 신규 및 변종 보안위협의 보안성을 강화하는 기술 및 정책이 요구된다.

References

[1] Jung Guk Park, “FinTech And Information Security”, KFT&CI, 2015.

[2] Suk Jae Lim, “Fintech Security Trend”, TTA, 2015. 3

[3] TTA, Framework for entity authentication assurance in a smart environment, TTA, 2014, 12

[4] Myung Guen Yoon, “Fintech Security”, kiise, 2015. 5

[5] Myung Gyu Lee, A Low Power Lifelog Management Scheme Based on User Movement Behaviors in Wireless Networks, jiibc. 2015.4

[6] Joo Yoen Lee, Next Generation Growth Fintech of Convergence and evolution, ie Magazine 2015

[7] Choon Kyeong Kim, Smart Card using Financial Card Services and Market Trends, TTA Journel, 2014

[8] E Turban, D King, JK Lee, E-Commerce Security and Fraud Issues and Protections, Springer Link,, 2015

저자 소개

박 중 오(정회원)

- 2000년 7월 : 성결대학교 컴퓨터공학과 졸업
- 2003년 3월 : 명지대학교 전자계산 교육 석사
- 2011년 8월 : 숭실대학교 컴퓨터공학 박사
- 2013년 3월 ~ 현재 : 동양미래대학교 조교수

- 관심분야 : PKI, Network security, 암호학
- E-mail : jopark13@dongyang.ac.kr

진 병 욱(준회원)

- 2000년 7월 : 청운대학교 멀티미디어학과 졸업
- 2013년 2월 : 숭실대학교 컴퓨터공학 석사
- 2013년 3월 ~ 현재 : 숭실대학교 컴퓨터학과 박사과정
- 관심분야 : 네트워크 보안, 인증 시스템, E-Commerce
- E-mail : quddnr4511@naver.com