디지털산업정보학회 논문지 제12권 제3호-2016년 9월
http://dx.doi.org/10.17662/ksdim.2016.12.3.111

핀테크의 보안 고려사항에 대한 연구

이 유 진* · 장 범 환** · 이 영 숙***

A Study on the FinTech : The consideration of the Security

Lee Yujin · Chang Beomhwan · Lee Youngsook

〈Abstract〉

Recently, mobile devices have been widely used. Therefore, the service users want that are not constrained by time and space. Among them, electronic payment services, mobile finance service is enjoying a tremendous popularity. The FinTech is the result of the fusion of finance and ICT(Information & Communication Technology). Security experts is pointed the FinTech security risk. New technology and Innovative FinTech services are even available, Insecure FinTech services is insignificant. In this paper we were surveyed market and product trends of FinTech and analyzed the threats about FinTech. Also, we analyzed the security considerations for FinTech using a questionnaire. As a result, users considers secure payment process and privacy. Therefore, we proposed security considerations for each vulnerability. So, we must be resolved of security technology and policy issues. If establishing a secure payment process and the unclear legal issue is resolved, FinTech service will provide a secure financial services to the user.

Key Words : FinTech, Finance Service, FinTech Threats, Security Consideration, Privacy, ICT

Ⅰ. 서론

최근 모바일기기가 널리 보급됨에 따라 시간과 공간의 제약을 받지 않고 편리하게 사용할 수 있는 서비스가 사용자의 요구를 충족시키고 있다. 그 중 전자결제서비스, 모바일뱅킹과 같은 비대면 서비스에 대한 관심은 폭발적으로 대두되고 있다. 이러한 서비스는 금융과 기술의 합성어인 핀테크(FinTech)라는 새로운 용어로 정의되고 있다. 핀테크는 과거에는 금융기관의 주도아래 IT기술을 활용한 금융서비스를 사용자에게 제공하였다면 최근에는 금융기관의 주도가 아닌 IT기업의 주도아래 금융서비스를 개발 또는 제공하는 방향으로 발전하고 있다.

금융 서비스를 제공하는 만큼 사용자의 민감한 개인정보를 취급한다. 이에 따라 국내·외 보안 전문가들은 개인인증과 개인정보처리과정에 대한 해커의 공격을 경고하였고, 한국인터넷진흥원에서도 핀테크 보안에 관한 보고서를 발표하는 등 핀테크 서비스에 대한 보안 관심도 커지고 있다.

* 호원대학교 사이버수사보안학부 학생
** 호원대학교 사이버수사보안학부 교수
*** 호원대학교 사이버수사보안학부 교수(교신저자)

국내에서는 금융서비스를 기반으로 한 유형과 ICT를 기반으로 한 유형의 핀테크 서비스를 하고 있다. 핀테크 서비스를 안전하게 사용하기 위해서는 사용자 스스로 안전수칙을 지키고 핀테크 서비스가 기본으로 제공하는 보안기술을 사용하는 것도 중요하지만, 핀테크 서비스 개발자들이 보안기술을 적용한 서비스를 개발하여 배포하는 것 역시 중요하다고 할 수 있다. 그러나 국내에서는 일반 어플 개발자를 위한 보안 가이드라인과 시큐어 코딩 안내서는 존재하지만 핀테크 서비스를 위한 보안 가이드라인은 전무한 상황이다. 본 논문은 금융 분야에서 활용될 수 있는 핀테크를 사용할 때 안전한 금융 서비스를 보장하기 위해 고려해야 할 보안 고려 사항을 제시하도록 한다.

본 논문의 구성은 다음과 같다. 논문의 2장에서는 핀테크의 정의와 특징을 살펴보고, 국내·외 시장동향을 분석하였으며, 3장에서는 핀테크의 내재적 특징과 관련된 위험, 사용자와 관련된 위험, 무선 네트워크와 관련된 위험, 웹 어플리케이션과 관련된 위험 그리고 핀테크 서비스와 관련된 위험으로 각각 분류하고 그에 따른 취약점을 분석하였다. 더불어 4장에서는 일반 사용자들을 대상으로 보안 의식동향을 조사하고, 3장에서 제시한 위험에 따른 보안 고려사항과 정책적·기술적 보안 고려사항을 제시한다.

Ⅱ. 핀테크의 개요

2.1 핀테크의 정의 및 특징

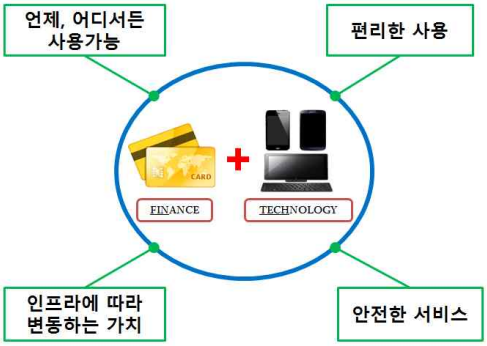
핀테크(FinTech)는 금융(Finance)과 기술(Technology)의 합성어로, 금융과 IT의 융합을 통한 금융서비스 및 산업의 변화를 통칭한다. 기존의 금융기법과 차별되는 점은 모바일, SNS, 빅데이터 등 새로운 IT기술 등을 활용하여 금융서비스를 제공하는 기술 혁신이 대표적이다. 최근 IT기술을 활용한 예로 모바일뱅킹과 앱카드 등이 있다[1]. 이러한 서비스들이 과거에는 금융기관의 주도아래 IT기술을 활용한 금융서비스를 사용자에게 제공하였다면 최근에는 금융기관의 주도가 아닌 IT기업의 주도아래 금융서비스를 개발 또는 제공하는 방향으로 발전하고 있다.

핀테크의 주요특징은 첫째, 언제 어디에서든 서비스를 사용할 수 있어야하고, 모바일 기기가 인터넷에 연결된다면 어떠한 장소와 시간의 제약 없이 서비스를 제공받아야 한다. 둘째, 인프라에 따라 가치가 변한다. 급격하게 변하는 사용자의 수나 요구에 따라서 서비스의 가치가 변동할 수 있다. 셋째, 사용하는데 불편함이 없어야한다. 서비스를 사용하는데 입력할 정보가 많고 복잡하지 않아야 한다. 또, 기존의 국내 전자금융서비스처럼 ActiveX를 설치하거나 또 다른 보안프로그램을 설치하는 등의 번거로움이 없어야 한다[2-3]. 마지막으로 금융소비자들에게 안전한 서비스를 제공해야한다. 핀테크는 사용자의 민감한 정보인 금융서비스에 접근하기 때문에 다양한 인증방법, 보안기술, FDS(Fraud Detection System), 빅 데이터 분석능력 등의 기술을 발판으로 고객의 편의성은 증진시키고, 보안위험과 위협은 최소로 낮추어 편리하고 안전한 서비스를 제공해야한다.

핀테크는 금융과 기술의 합성어인 새로운 용어이고, 언제 어디서든 서비스를 제공받을 수 있다. 또, 인프라에 따라 가치가 변하고, 편리하게 사용되어야 한다. 아울러 안전한 서비스를 제공해야 한다. <그림 1>은 핀테크에 대한 대략적인 개념도이다.

2.1.1 핀테크의 서비스 유형

핀테크의 서비스 유형은 핀테크에 대한 시각에 따라 다양하게 분류되고 있다. 하지만 공통적인 분류로



<그림 1> 핀테크의 개념도

는 금융서비스와 ICT기술로 분류할 수 있다. 금융서비스란 신용협동조합, 은행, 투자 펀드, 부동산 펀드, 일부 정부보증회사 등을 포함하여 돈을 관리하는 여러 단체를 아우르는 금융 산업이 제공하는 송금, 결제, 자산관리 그리고 투자이다[4]. ICT기술을 기반으로 한 금융서비스에는 금융 빅 데이터분석, 금융 소프트웨어, 금융보안이 있다[5-6].

(1) 금융서비스를 기반으로 한 유형

송금서비스는 주로 모바일과 이메일을 이용하여 제공된다. 온라인으로 거래 가능한 가상화폐를 이메일 또는 모바일 통신을 이용하여 개인과 개인 또는 개인과 기업 간의 송금서비스를 제공한다. 결제서비스에는 전자결제서비스가 있다. 전자결제서비스는 상품 및 서비스 결제의 편의성을 돕고, 가상계좌나 신용카드 등으로 지불이 가능하다. 특히 전자결제서비스는 현재 핀테크 사업 중 가장 폭넓게 이용되고 있는 분야이다. 자산관리서비스에는 온라인펀드, 인터넷은행 등이 있다. 온라인으로 다양한 펀드를 살 수 있는 슈퍼마켓과 같은 역할을 하고, 온라인 전용으로 주식, 채권 등의 서비스를 제공한다는 특징이 있다. 투자서비스에는 금융투자 플랫폼으로 쇼설트레이딩, 크라우드펀딩이 있다. 대출이나 창업자금을 지원하는 등의 투자 관련 금융을 서비스하는 온라인 플랫폼이고, 스마트폰과 같은 모바일 기기를 이용하여 투자정보교류를 하여 투자활동에 영향을 준다는 특징이 있다.

(2) ICT(Information & Communication Technology)를 기반으로 한 유형

ICT 기술을 활용한 핀테크 산업 서비스는 금융 빅데이터분석, 금융 소프트웨어 그리고 금융 정보보안으로 분류한다[5]. 금융 빅데이터 분석은 빅데이터 분석으로 소비자의 소비패턴의 인식을 통하여 소비활동을 증진시키고, 대규모 데이터를 활용하여 개인맞춤형 대출 금리를 산정할 수 있다.금융 소프트웨어는 각 은행사의 모바일 앱은 금융 서비스를 보다 편리하게 일상에서 사용하기 위해 새로운 아이디어와 기술이 접목된 소프트웨어이다.

<표 1> 핀테크 산업 분류에 따른 서비스 예

구분	종류	서비스명칭
금융서비스	모바일 및 이메일 송금	뱅크월렛카카오
		토스
	전자결제 서비스	삼성월렛, 삼성페이
		모카월렛
		Paynow+
		BLE 페이먼트
		MPay
		엠틱
		YellowPay
		모바일 NFC 간편결제
	온라인펀드, 인터넷은행·보험·증권	자산관리
	금융투자플랫폼	굿펀딩(P2P대출)
ICT 기술	금융 빅데이터 분석	PDM(Proit-Data Miner)
	금융 소프트웨어	은행사 각각의 앱 명칭
	정보보안	KSing Secure

2.2 시장동향

2.2.1 국외동향

세계 각국에서 핀테크는 서로 다른 분야에서 활성화되고 있다. 한국은 결제서비스 위주로 활성화되었다. 미국은 기술혁신을 통한 핀테크 시장을 형성하였다. 그리고 중국은 온라인 소비 정책에 힘입어 결제서비스와 함께 온라인 펀드도 지원하고 있다. 핀테크에 대한 적극적인 정부의 정책아래 영국은 결제서비스를 제공하고 있다.

미국의 경우 Apple사가 모바일 전자 상거래에 본격적인 진출을 하였다. 애플페이와 알리바바 간의 협력 체결을 발표하였고, 핀테크 기술에 대한 투자를 점차적으로 확대하고 있다. 아울러 Google사 또한 직접 개발한 모바일 결제시스템인 Google Wallet을 내놓았는데, NFC(Near Field Communication)기능이 내장되어있고 스마트 폰과 같은 모바일기기를 통하여 결제를 할 수 있다[7]. 온라인 대출 사업 분야에도 핀테크 기술을 접목시켰는데, 금융 빅 데이터 분석을 통한 대출 심사 및 신용등급과 대출여부를 결정하는 신속한 서비스를 제공한다[8]. 알리페이(AliPay)는 중국에서 금융 시장에 진출한 IT기업들 중 최대 규모인 알리바바의 금융 서비스이다. 알리바바는 2004년부터 핀테크 산업을 시작하였지만, 2013년도에 위어바오라는 일종의 머니마켓 펀드인 금융상품을 출시하면서 중국의 핀테크 산업의 패러다임을 무너뜨렸다. 이를 계기로 알리페이는 단순한 전자화폐에서 중국의 대표적인 금융상품이 되었다[8]. 영국의 금융그룹인 HSBC와 First Direct 등은 핀테크 기업인 Zapp와 제휴를 맺어 다른 개인정보를 추가적으로 요구하지 않고 비밀번호 입력만으로 간편하게 모바일 결제가 가능한 진화된 금융 서비스를 제공하고 있다.

2.2.2 국내동향

통계청의 2014년 온라인 쇼핑동향 보고서에 의하면 2014년 말에는 전자금융거래 액수가 약 46,000억 원에 불과하지만, 2015년에는 약 68,000억 원으로 1.5배가량 증가했다고 한다[9-10].

국내에서는 신용카드사, 오픈 마켓, PG(Payment Gateway)사 등이 공인인증서가 적용되지 않는 소액결제에 대하여 핀테크 결제서비스를 제공한다. 이러한 서비스는 기존 플랫폼에 신규 서비스를 결합하는 것이 특징이다. 핀테크 기업들이 서비스에 접근하는데 각종 규제가 많고, 금융기관에 따라 적용되는 핀테크 기술이 다르기 때문에 국내에서는 유독 결제서비스 위주로 발전 하고 있다[6].

한국, 미국, 중국 그리고 영국의 핀테크의 특징 및 주요서비스를 <표 2>에 정리하였다.

<표 2> 주요국의 핀테크 현황

분류	특징	주요서비스
한국	· 결제서비스 위주로 발전 · 기존 플랫폼에 신규 서비스를 더하는 형태	결제서비스
미국	· 기술혁신을 통한 핀테크 시장 형성	결제서비스, 금융 빅 데이터 분석
중국	· 온라인 소비 정책	결제서비스, 온라인 펀드
영국	· 핀테크에 대한 적극적인 정부의 정책	결제서비스

Ⅲ. 핀테크의 보안 위험 및 취약점 분석

우리나라에서는 금융권의 개인정보 유출사고, 텔레뱅킹을 통한 인출사고 등 연이은 금융사고가 발생하고 있다. 아울러 금융감독원을 사칭한 보이스피싱 사기도 급증하였는데, 금융감독원과 한국인터넷진흥

원에서는 금융 사고에 대한 보안인식을 강조하고 있다. 한국 인터넷 진흥원의 2015년도 정보보호 실태조사에 따르면 100명중 80명 이상이 전자금융사기를 통한 금전적 손실을 우려하고 있다.

해외의 경우에도 패션업체인 TJX에서 신용정보와 개인정보가 유출되어 신원도용, 계좌 부정인출, 카드 부정사용 등의 2차 피해가 발생한 적이 있었고, 신용카드 결제 업체에서도 해킹으로 인하여 금융정보가 유출되는 등의 사고가 있었다[6]. 본 장에서는 핀테크 서비스를 사용할 때 안전한 금융 서비스를 보장하기 위해 핀테크 서비스의 유형별로 위험을 분류하고 그에 따른 취약점을 분석하였다. <표 3>은 핀테크 서비스의 위험 및 취약점을 보여준다.

3.1 핀테크의 내재적 특징과 관련된 위험 및 취약점

핀테크는 비대면 금융 서비스라는 특징을 가지고

<표 3> 핀테크 서비스의 위험 및 취약점

분류		위험 및 취약점
내재적 특징	알고 있는 것	· 무작위 패스워드 공격 · 사회공학 공격
	가지고 있는 것	· 분실 및 도난
	사용자 그 자체	· 인증장치의 성능
	위치 해 있는 곳	· 기기의 오작동
사용자	개인정보 저장	· 개인정보 유출
	기기분실	· 공격자의 핀테크 서비스 악용
무선 네트워크	물리적	· 무선 장비의 물리적 보안 위험
	기술적	· 도청, 서비스 거부
	관리적	· 무선랜 장비 관리 미흡 · 무선 랜 사용자의 보안의식 결여
웹 어플리케이션	A1 - 인젝션	· 예상하지 못한 명령에 의한 인젝션
	A2 - 인증 및 세션 관리 취약점	· 데이터베이스에 활용되는 시스템 명령어
	A3 - 크로스 사이트 스크립팅	· 사용자로부터 입력 받은 값의 불확실한 검사
	A4 - 취약한 직접 객체 참조	· 내부 구현 객체의 참조 노출
	A5 - 보안 설정 오류	· 서버 및 플랫폼에 대해 보안 설정
	A6 - 민감 데이터 노출	· 암호화 되지 않은 통신
	A7 - 기능 수준 접근 통제 누락	· 접근 요청에 대해 부적절한 확인
	A8 - 크로스 사이트 요청 변조(CSRF)	· 해커의 악의적 공격
	A9 - 알려진 취약점이 있는 컴포넌트 사용	· 비주기적인 프로그램 업데이트
	A10 - 검증되지 않은 리다이렉트 및 포워드	· 비적절한 검증 절차
서비스 유형	카카오페이	· 키가 유출될 경우 복호화 가능
	애플페이	· 카드등록시 본인확인 절차가 없음
	페이코X티머니	· 결제정보 유출 시 카드복제 가능
	삼성페이	· 기기에 저장된 지문의 정보수집 가능
	안드로이드페이	· 클라우드에 저장된 결제 정보를 USIM이 없는 오프라인단말기에서 접근이 가능

있다. 지금까지 사람을 마주하고 이루어졌던 금융서비스가 사람을 마주하지 않는 비대면으로 가능하다. 최근 금융업계에서는 비대면 금융서비스의 보안 규제 사항에서도 변화가 일어나고 있다. 과거에는 사전규제와 기술종속적인 규제환경 이였다면, 현재는 사후감사 강화와 기술독립적인 자율 보안적인 규제환경으로 바뀌고 있다. 자율 보안적인 규제환경이라는 말에는 보안인증수단과 같은 보안에 관련된 사항을 금융회사가 스스로 결정할 수 있다는 뜻이 담겨져 있다. 특히 2014년 9월부터 공인인증서 의무사용 규정이 폐지되었다. 그에 따라 공인인증서를 대체할 수단이 무엇이 존재하는지에 대해 관심이 커지고 있다[10].

공인인증서를 대체할만한 사용자의 본인인증 방법은 크게 4가지로 분류된다. 알고 있는 것, 가지고 있는 것, 사용자 그 자체, 위치해있는 곳으로 구분할 수 있다.

(1) 알고 있는 것이 가지는 위험 및 취약점

알고 있는 내용은 사회공학 공격으로 인하여 쉽게 누출될 수 있다. 또한 무작위 패스워드 공격이나 패스워드 사전 공격 등을 이용해서도 누출될 수 있는 가능성이 높고, 사기의 일종인 피싱과 같은 공격으로 사용자를 속여 패스워드를 가로챌 수 있는 위험이 있다.

(2) 가지고 있는 것이 가지는 위험 및 취약점

2차적인 인증수단으로 많이 쓰이는 가지고 있는 것은 분실의 위험이 가장 크다. 분실의 위험과 더불어 도난의 위험 또한 배제할 수 없다. 악의적 공격자가 사용자의 인증수단을 갈취 할 수도 있다.

(3) 사용자 그 자체가 가지는 위험 및 취약점

사용자 그 자체로 인증한다는 것은 다른 말로 생체인증 이라고도 한다. 생체인증은 인증장치의 성능에 따라 위험이 결정된다. 생체인증 성능의 기준은 얼마나 정확하게 그 사람의 신분을 탐지할 수 있는지 이다.

FRR(Flase Rejection Rate or Type I Error)은 정확도가 올라감에 따라 에러율도 올라가고, FAR(False Acceptance Rate or Type II Error)은 정확도가 높아짐에 따라 에러율이 내려간다. FRR과 FAR이 그리는 곡선의 교차점인 EER(Error Equal Rate)을 기준으로 범위에 따라 인증장치의 성능이 정해진다.

(4) 위치해 있는 곳이 가지는 위험 및 취약점

위치해 있는 곳이라는 것은 GPS 또는 IP와 같은 것을 이용하는데, 이것은 모바일 기기가 필요하다. 모바일 기기를 분실했거나, 기기의 오작동 시에는 인증을 할 수 없다.

3.2 사용자와 관련된 위험 및 취약점

Pointsec Mobile Technologies에 의해 수행된 모바일 사용에 대한 조사에 따르면 모바일 장치를 이용하는 이용자의 75% 이상이 모바일 기기에 개인정보를 저장하고 있다고 한다. 또한 사용자는 모바일 기기의 보안설정을 허술하게 하여 기업 이메일과 데이터에 접근할 수 있다. 사용자의 보안인식 부족으로 무작위로 무선 랜을 통하여 연결된 기기는 악의적 공격자에 의하여 도청과 같은 공격으로 중요 데이터가 유출당할 수 있다[11]. 물리적 분실/도난으로 인해 사용자는 피해를 입을 수 있다. 만약 사용자가 모바일 기기에 대해 기본적인 잠금 기능을 설정하지 않는다면 공격자는 분실되거나 또는 불법으로 획득한 사용자의 모바일 기기로 핀테크 서비스를 사용할 수 있다. 예를 들어 공격자가 별도의 금융정보가 필요하지 않은 PIN코드를 이용한 송금서비스를 악용한다면, 사용자는 금전적 손실을 입을 것이다[12].

3.3 무선 네트워크와 관련된 위험 및 취약점

핀테크는 모바일 기기의 확산에 따라 더욱 부각되고 있는 서비스이다. 모바일 기기는 휴대하여 이동이 가능하다는 장점을 가지고 있는 반면, 무선네트워크 상에서 연결된다는 특징이 있다. 무선네트워크에서의 위험과 취약점은 크게 3가지로 분류한다. 첫째, 물리적 보안 위험 및 취약점이다. 둘째, 기술적 보안 위험 및 취약점이다. 마지막으로 관리적 위험 및 취약점이 있다.

3.3.1. 무선 랜의 물리적 보안 위험 및 취약점

무선 랜을 구성하는데 있어 중요한 역할을 하는 무선 AP의 경우, 원활한 서비스의 제공을 위해 외부에 노출된 형태로 위치하게 되는 것이 일반적이다. 이러한 무선 AP는 장비의 외부 노출로 인해 비인가자에 의한 장비의 파손 및 장비 리셋을 통한 설정 값 초기화 등의 문제가 발생할 수 있다. 별도의 시설 설치를 통해 외부로부터 접근이 불가능하도록 철저히 보호하여야 한다[13].

3.3.2. 무선 랜의 기술적 보안 위험 및 취약점

무선 랜은 공기를 전송매체로 사용하는 서비스의 특성 상 많은 취약점이 존재하게 된다. 그 중 불특정 다수의 신호수신이 가능함으로 인해 도청이 가능하고, 무선 전파를 전송하는 무선 장비에 대한 공격이 가능하다. 또한 유선 랜에서 존재하는 여러 가지 공격 기법이 무선 랜에서 사용가능하다[13].

3.3.3. 무선 랜의 관리적 보안 위험 및 취약점

무선 랜을 운영하는 대부분의 기관에서는 사용하는 AP의 개수 정도만 파악하고 있어, 실제로 장비가 파손되거나 도난당하여 무선 랜 서비스를 제공하지 못하고 있어도 이를 파악하지 못하는 경우가 발생할 수 있다. 이를 방지하기 위해, 기관에서 사용하는 무선 랜 장비인 AP와 무선랜 카드 등에 대한 장비 운영 현황과 사용자 현황 등을 파악하여야 한다[13].

무선 랜 운영 기관에서 마련한 보안정책과 보안기능을 사용하지 않는 사용자가 있으면, 전체 기관의 정보보호에 허점이 발생하기 마련이다. 무선 랜을 사용하는 기관에서는 관리자뿐만 아니라 사용자도 항상 보안에 관심을 갖고 무선 랜을 사용해야 한다. 아무리 잘 수립된 보안정책과 이를 적용하기 위한 보안장비가 있다하더라고 막상 사용자가 이를 따르지 않으면 무용지물이 되기 때문이다[13].

3.4 웹 어플리케이션과 관련된 위험 및 취약점

사이버상의 공격의 약 75%가 소프트웨어 자체의 보안취약점을 악용한다. 핀테크 역시 소프트웨어를 기반으로 한 서비스이기 때문에 위험이 존재한다. 핀테크 어플리케이션은 불특정 다수에게 서비스를 제공하고, 사용자가 입력한 개인정보를 처리하는 프로그램의 특성상 외부공격에 항상 노출되어 있다[14].

3.4.1 OWASP에 의한 취약점 분석

(1) A1 – 인젝션

예상하지 못하는 명령을 실행시키거나 적절한 권한 없이 데이터에 접근하도록 인터프리터를 속이는 공격자의 악의적인 공격이다.

(2) A2 – 인증 및 세션 관리 취약점

데이터베이스에 저장된 데이터 값을 조회, 열람, 삭제, 추가 할 수 있으며, 인증 절차를 비정상적으로

우회 가능하다.

(3) A3 – 크로스 사이트 스크립팅

공격자가 웹 페이지에 악성 스크립트를 삽입할 수 있는 취약점이다. 사용자로부터 입력 받은 값을 제대로 검사하지 않고 사용할 경우 나타난다. 주로 여러 사용자가 보는 게시판에 활용되며 쿠키, 세션 등 사용자의 정보를 탈취한다.

(4) A4 – 취약한 직접 객체 참조

직접 객체 참조는 개발자가 파일, 디렉토리 데이터베이스 키와 같은 내부 구현 객체를 참조하는 것을 노출시킬 때 발생한다. 접근 통제를 통한 확인하나 다른 보호수단이 없다면 공격자는 노출된 참조를 조작하여 허가 받지 않은 데이터에 접근할 수 있다.

(5) A5 – 보안 설정 오류

훌륭한 보안은 애플리케이션, 프레임 워크, 에플리케이션 서버, 웹서버, 데이터베이스 서버 및 플랫폼에 대해 보안 설정이 정의되고 적용되어 있다. 기본으로 제공되는 값은 종종 안전하지 않기 때문에 보안 설정은 정의, 구현, 유지되어야 하고, 소프트웨어는 최신의 상태이여야 한다.

(6) A6 – 민감 데이터 노출

서버와 클라이언트간 통신 시 암호화 하여 전송을 하지 않아 민감한 정보(신용카드번호, 여권번호, 주민등록번호 등)가 평문으로 전송되는 등 민감한 정보가 노출될 수 있다.

(7) A7 – 기능 수준 접근 통제 누락

대부분의 웹 어플리케이션은 실행 시 기능 수준의 접근권한을 확인한다. 또, 어플리케이션은 각 기능에 접근하는 서버에 동일한 접근통제에 대한 검사를 수행하고, 요청에 대해 적절히 확인하지 않을 경우 공격자는 적절한 권한 없이 기능에 접근하기 위한 요청을 위조 할 수 있다.

(8) A8 – 크로스 사이트 요청 변조(CSRF)

해커가 의도한 행위를 특정 웹 사이트에 요청하는 공격으로 인증 완료된 다른 사람의 권한으로 서버에 부정적인 요청을 한다.

(9) A9 – 알려진 취약점이 있는 컴포넌트 사용

일부 프로그램의 경우 자체적으로 업데이트를 권고하고 또한 업데이트를 하는 것이 쉽지만, 현재 운영 중인 대형 서버와 같이 실시간으로 업데이트를 하기 어려운 경우에 자주 발생하기 쉽다.

(10) A10 – 검증되지 않은 리다이렉트, 포워드

웹 어플리케이션은 종종 사용자들을 다른 페이지로 리다이렉트 하거나 포워드 하고, 대상 페이지를 결정하기 위해 신뢰할 수 없는 데이터를 사용한다. 적절한 검증 절차가 없으면 공격자는 피해자를 피싱 또는 악성코드 사이트로 리다이렉트 하거나 승인되지 않은 페이지에 접근하도록 전달한다.

3.5 핀테크 서비스와 관련된 위험

공통적인 위험과 더불어 각각 핀테크 서비스들은 서비스마다 각각의 위험이 존재한다. 카카오페이는 암호화한 결제정보의 키가 공격에 의해 유출될 경우 복호화가 가능하다는 위험이 있다. 또, 애플페이는 애플의 정책상 카드등록시 본인확인 절차가 없다는 위험이 있고, 페이코 X 티머니는 결제정보가 유출될 경우 카드복제 등의 문제가 발생할 수 있다. 삼성의 삼성페이의 경우 기기에 저장된 지문의 정보수집이 가능하다. 마지막으로 안드로이드페이는 클라우드에 저

장된 결제 정보를 USIM이 없는 오프라인 단말기에서 접근이 가능하다[15]. 핀테크 서비스들의 위험을 정리하면 <표 4>과 같다.

<표 4> 핀테크 서비스가 갖는 위험의 예

서비스 명	결제인증	위험
카카오페이	PIN	· 키가 유출될 경우 복호화 가능
애플페이	지문인식, PIN	· 카드등록 시 본인확인 절차 없음
페이코X 티머니	PIN	· 결제정보 유출 시 카드복제 가능
삼성페이	지문인식, PIN	· 지문의 정보수집 가능
안드로이드 페이	지문인식, PIN	· 클라우드에 저장된 결제 정보를 USIM이 없는 단말기에서 접근이 가능

Ⅳ. 핀테크의 보안고려사항

4.1 보안 의식동향 분석

핀테크에서는 모든 금융활동에 이용되는 정보 자체가 매우 중요한 원천이다. 하지만 악의적인 공격으로 인하여 많은 피해가 있었고, 사용자들은 핀테크 서비스를 이용함으로써 편리함을 제공받은 동시에 정보유출과 같은 위험을 느끼게 되었다.

일반인을 대상으로 핀테크 서비스에 대한 보안 의식을 조사하기 위하여 핀테크 서비스의 분류, 핀테크 서비스의 위험, 핀테크의 보안고려사항 등의 변수에 대한 조작적 정의를 통해 설문을 구성하였다. 질문형식은 폐쇄형 질문을 사용하였으며, 자료에 대한 설문조사는 2015년 9월 초부터 10월 중순까지 약 2개월 정도 소요되었다. 설문지는 집단조사방법을 이용해 직접 방문하여 설문을 진행하였으며, 설문자료의 회수율과 설문 응답의 정확도를 높였다. 전체 200명을 조사 대상으로 하였으나 186개(93%)를 회수하였다.

핀테크 서비스 사용 시 강조되어야 하는 보안에 관한 다중응답이 가능한 질문에서는 개인정보보안이 강조되어야 한다는 응답이 총 응답 208개 중 72개(34%)로 가장 많았고, 이어서 결제 과정 중의 보안이 고려되어야 한다는 것이 총 208개 중 56개(26%)로 뒤를 이었다. 사용자들은 개인정보보안이 결여되고 보안이 내재되지 않은 결제과정을 염려한다는 사실을 알 수 있었다.

4.2 보안고려사항

개인 또는 단체의 금융과 관련된 서비스인 만큼 철저한 보안이 요구되는 핀테크 서비스는 기업의 기술적인 보안 뿐 아니라 법적인 규제 또한 필요하다. 개인정보보호법과 같은 법적인 규제아래 개인정보를 취급해야 하고, 핀테크 기업 내에서 보안에 필요한 정책과 기술을 적용하는 형태로 발전해야한다.

4.2.1 법적 이슈

핀테크 서비스는 모바일 혁명과 더불어 세계적으로 영향을 주고 있다. 하지만 국내에서는 금융당국의 규제로 인해 발전이 더디게 진행되고 있다. 진입 규제 장벽으로는 개인정보보호법, 전자금융 거래법 등이 있다. 금융 산업의 경쟁력 확보와

핀테크 서비스의 발전을 위해서는 정책적인 지원이 필요하다[16-17].

(1) 개인정보 보호법

핀테크 서비스는 사용자들의 개인정보를 취급하고 다루기 때문에 사용자들은 민감한 개인정보를 보호받을 권리가 있다. 개인정보 보호법에 따르면 고유식별 정보를 처리하는 경우 훼손되지 않도록 암호화 등 안전성 확보에 필요한 조치를 해야 한다. 이에 더

불어 개인정보 처리자는 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하도록 정해져있다[18]. 개인정보 보호법에 따른 정책과 세부사항을 <표 5>에 나타냈다.

<표 5> 개인정보 보호법에 따른 정책과 세부사항

정책	세부사항
정기적인 자체 감사 실시	· 개인정보 취급 관련 안정성 확보를 위해 정기적으로 자체 감사를 실시 · 개인정보의 안전한 처리를 위하여 내부 관리계획을 수립 및 시행
개인정보의 암호화	· 개인정보는 암호화 되어 저장 및 관리 · 중요한 데이터는 암호화 및 파일 잠금 기능을 사용
기술적 대책	· 개인정보 유출 및 훼손을 막기 위하여 보안프로그램을 설치 · 접근이 통제된 구역에 시스템을 설치 · 기술적/물리적으로 감시 및 차단
개인정보에 대한 접근 제한	· 데이터베이스시스템에 대한 접근권한의 부여, 변경, 말소
보안을 위한 잠금장치 사용	· 개인정보를 잠금장치가 있는 안전한 장소에 보관
비인가자에 대한 출입 통제	· 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 지정 · 출입통제 절차를 수립, 운영

(2) 전자금융거래법

금융서비스를 제공하는 핀테크 서비스에서는 2014년 10월에 개정된 전자금융거래법(제21조 제3항)에 따라 더 이상 인증 방식에 대해 공인인증서만을 이용하도록 강요해서는 안 된다[19]. 전자금융감독 세칙개정안 발효로 공인인증서 의무 사용이 폐지되었지만, 공인인증서 방식만 고집하는 온라인 상거래 사이트가 여전히 존재한다. 그 이유는 신용카드로 물건을 구매하는 경우 보안사고로 인해 물건 값을 돌려받지 못하면 해당 금액만큼 카드사의 손실로 이어지기 때문이다. 결국 고액 결제 시 사고율을 낮춰줄 새로운 수단이 나오기 전까지 공인인증서는 가장 안전한 방법으로 여겨질 것이다.

4.2.2 보안 정책 및 기술

사용자가 핀테크 서비스를 사용하기 위해서는 본인인증, 개인정보입력 등의 단계를 거치게 된다.

이러한 과정을 안전하게 보호하기 위해서는 보안정책과 기술이 필요하다. 여러 가지 보안 정책과 기술이 요구되지만, 그 중 PCI-DSS, IC Tagging, FIDO, 토큰화 그리고 FDS가 부각되고 있다.

(1) PCI-DSS(Payment Card Industry-Data Security Standard)

PCI-DSS는 카드정보 해킹 및 도난·분실 사고로부터 사용자의 신용카드 정보를 보호하기 위해 국제 브랜드사가 공동으로 마련하여 운영하는 카드산업 보안표준이다.

PCI-DSS의 요구항목에는 첫째, 보안네트워크 설치 및 유지하는 것이 있다. 인터넷 방화벽을 구축 및 관리하고 관리하는데 필요한 기본설정 사용자 비밀번호는 사용자가 다른 용도로 사용하는 것을 금지한다. 둘째, 카드소유자 정보보호는 보관된 신용카드 정보를 암호화 하고 철저하게 관리한다. 셋째, 취약점 관리 프로그램 유지는 안티바이러스 소프트웨어 사용 및 주기적인 업데이트를 해야 하고, 안전한 시스템 어플리케이션 개발 및 관리를 해야 한다. 넷째, 강화된 접근 통제 방안을 수립한다. 철저한 정보접속 권한을 부여하고, 컴퓨터 사용자의 개별 ID 및 비밀보호를 사용한다.

그리고 신용카드 정보의 물리적 접근을 통제한다. 다섯째, 정기적 네트워크 모니터링 및 테스트는 네트워크 및 신용카드 정보 접속에 대한 체계적인 모니터링을 하고, 정기적인 보안시스템을 점검한다. 마지막으로 정보보호정책 유지 및 관리를 하기 위하여 신용카드 정보보안에 대한 정책 및 지침을 마련한다[20-21].

(2) IC Tagging

IC카드 내에 안전하게 저장된 인증정보를 통신기능이 포함된 모바일 기기를 통해 서버에 전달하여 인증하는 기법이다. 사용자가 소유하고 있어야하는 소유기반이고, 비설치형 이라는 특징을 가지고 있고, 기존 공인인증서가 가지고 있는 단점을 개선 할 수 있다[20].

(3) FIDO(Fast IDentity Online)

사용자의 고유한 신체구조 및 행위에 기반하여 인증하는 방식이다. 생체・행위 기반이고 비 설치형이다. 사용자의 편의를 개선하였고, 생체정보 유출의 위험이 있다. 등록과 인증에 사용되는 키가 다른 비 대칭키 구조를 가지고 있고, 서버에 분산 저장한다[20, 22].

(4) 토큰화

결제 시 가상의 카드번호를 이용하여 정보의 유출 및 노출에 대응하는 기술이다. 매 거래 시 일회용 검증 값으로 거래를 검증한다. 토큰화는 기존 시스템의 교체 없이도 도입이 가능하고 비용 측면에서도 장점을 가지고 있다[20, 23].

(5) FDS(Fraud Detection System)

FDS는 이상거래탐지 시스템으로 서버단의 보안강화를 위해 사용되는 강력한 보안체계이다. FDS을 통해서 사용자의 평소 거래패턴을 분석한다. 그 후, 패턴의 범위를 벗어난 액션이 취해지면 이상행위로 간주하여 제제를 가한다[6, 24].

4.2.3 취약점에 따른 보안고려사항

(1) 핀테크의 내재적 취약점에 따른 보안고려사항

핀테크는 비대면 서비스라는 특징을 가지고 있다. 비대면 서비스를 이용하는 사용자 인증과정에서 이루어지는 해킹을 근본적으로 방지해야한다. 기존의 다중요소 인증방법이 아닌 서로 다른 채널에서 인증받는 Two-Channel 인증방식[25]을 이용하여 기존 인증방법이 가지고 있는 단점을 개선한다.

(2) 사용자와 관련된 취약점에 따른 보안고려사항

일부 사용자들은 자신의 모바일 기기에 중요정보를 저장한다. 그러나 기본적인 보안설정을 하지 않고, 보안의식이 결여되어 있는 경우가 있다. 따라서 사용자 보안의식 강화를 위한 정보보안교육이나 모바일 기기 보안 설정 가이드라인이 필요하다.

(3) 무선네트워크 취약점에 따른 보안고려사항

무선 랜 보안 안내서[13]에 따르면 무선 AP와 같은 장치는 별도의 시설 설치를 통해 외부로부터 접근이 불가능하도록 철저히 보호하여야 한다. 아울러 기관에서 사용하는 무선 랜 장비와 무선랜 카드 등에 대한 장비 운영현황과 사용자 현황 등을 파악하여야 한다.

(4) 웹 어플리케이션 취약점에 따른 보안고려사항

신뢰할 수 없는 데이터를 명령어로부터 분리해야하고, 개발자들은 시큐어 코딩 가이드라인을 참고하여 개발함으로써 웹 어플리케이션이 가진 취약점을 보완하여야 한다[26].

Ⅴ. 결론

본 논문에서는 금융서비스와 기술의 융합으로 나타난 핀테크 서비스의 정의 및 특징을 알아보고, 핀테크의 서비스 유형을 크게 금융서비스와 ICT기술로 나누어 분류하였다. 아울러 핀테크 서비스의 국내・

외 시장동향을 살펴보고, 핀테크 서비스를 위험에 따라 분류하여 각각의 취약점을 분석하였다. 일반 사용자를 대상으로 설문조사를 하여 보안 의식동향을 파악했고, 핀테크 서비스의 등장으로 변화된 법적 이슈와 보안 정책 및 기술을 연구하였다. 설문조사를 통해 사용자의 보안 의식동향을 분석한 결과, 사용자는 핀테크 서비스 이용 시 개인정보보안과 결제과정과 관련된 보안에 대한 대응 보안기술을 기대한다. 새로운 기술이 도입되고 혁신적인 핀테크 서비스가 제공되더라도 보안이 취약한 핀테크 서비스는 무의미하다. 그러므로 본 논문에서 제시한 핀테크의 취약점 분석에 대한 대응 보안기술이 마련되어야 할 것이다. 아울러 법적인 보안 규제가 명확하지 않아 발생하는 법적 문제들이 해결된다면 핀테크 서비스는 앞으로 일상생활에서 사용자에게 안전한 금융 서비스를 제공할 것이다.

참고문헌

[1] 박정국, “핀테크 (Fintech) 와 정보보안,” 정보과학회지, Vol. 33, No. 5, 2015, pp. 23-32.

[2] 정준호 & 김정숙, “핀테크 (FinTech) 서비스의 주요 사례와 보안 이슈,” 한국멀티미디어학회지, Vol. 19, No. 1, 2015, pp. 9-15.

[3] 이학준, “국내외 금융 보안 기술의 차이를 통해 살펴본 핀테크,” 2015, LGCNS, http://blog.lgcns.com/661.

[4] 박서기, “핀테크 산업 동향과 주요 비즈니스 모델에 대한 연구,” 한국멀티미디어학회지, Vol. 19, No. 1, 2015, pp. 1-8.

[5] 여신금융연구소, “핀테크의 가치창출 요건 및 시사점,” 2015, pp. 1-19.

[6] 장상수, “핀테크가 정보보호산업에 미치는 영향에 대한 고찰,” 한국인터넷진흥원, KISA Report, 2015, pp. 4-22.

[7] 한국인터넷진흥원, “글로벌 핀테크 산업동향- 미국편,” 2015, pp. 1-21.

[8] 박대현, “산업 간 융합 관점에서 본 핀테크의 시사점,” 한국인터넷진흥원, KISA Report, 2014, pp. 5-15.

[9] 통계청, “2015년 7월 소매판매 및 온라인 쇼핑 동향,” 2015, pp. 11-26.

[10] 국가법령센터, “전자금융거래법,” 2015.

[11] 이영숙 & 김지연, “스마트폰 보안 기술 분석,” 디지털산업정보학회 논문지, Vol. 6, No. 2, 2010, pp. 91-105.

[12] 김지연, 전웅렬, 이영숙, 김미주, 정현철, 원동호, “안전한 스마트폰 애플리케이션 개발을 위한 보안고려사항 및 국산암호알고리즘 적용 방안 연구,” 디지털산업정보학회 논문지, Vol. 7, No. 1, 2011, pp. 51-61.

[13] 방송통신위원회 & 한국인터넷진흥원, “무선랜 보안 안내서,” 2010, pp. 12-111.

[14] 안전행정부, “소프트웨어 보안약점 진단 가이드,” 2012, pp. 8-30.

[15] 금융보안원, “주요 간편 결제 서비스의 보안성 비교 분석,” 2015, pp. 4-17.

[16] 국가법령센터, “개인정보 보호법,” 2015.

[17] 강동식, “핀테크 법제도 개선 움직임과 남은 과제,” 한국인터넷진흥원, KISA Report, 2015, pp. 4-12.

[18] 현경민, “왜 지금 핀테크인가,” 도서출판 미래의 창, pp. 8-256.

[19] 유진투자증권, “보안에서 본 핀테크, 결제에서 본 핀테크,” 2015, pp. 8-55.

[20] 금융보안원, “핀테크 시대의 보안기술,” 2015, pp. 4-18.

[21] Baker, W. H., Hylender, A., Pamula, C. D., Porter, J., & Spitler, C. M, "2011 data breach investigations report," 2011.

[22] 김재중, "FIDO (Fast IDentity Online) 를 이용한 비밀번호 없는 공인인증시스템에 관한 연구," 정보과학회지, Vol. 33, No. 5, 2015, pp. 9-12.

[23] 신용녀, 김영진, & 전명근, "바이오 보안 토큰과 PKI 연계방안," 한국정보기술학회논문지, Vol. 9, No. 5, 2011, pp. 207-216.

[24] 이민규, 손효정, 성백민, & 김종배, "핀테크기반 환경에서 GPS 를 적용한 Fraud Detection System," Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology, Vol. 5, No. 4, 2015, pp. 659-666.

[25] 유한나, 이재식, 김정재, 박재표, 전문석, "인터넷 뱅킹 환경에서 사용자 인증 보안을 위한 Two-Channel 인증 방식," 한국통신학회논문지, Vol. 36, No. 8, 2011, pp. 939-946.

[26] 안철수연구소, http://www.ahnlab.co.kr/kr/site/securityinfo/secunews/secuNewsView.do?cmd=scrap&seq=16555&menu_dist=2.

■ 저자소개 ■

이 유 진
Lee Yujin

2013년 3월~현재
호원대학교 사이버수사보안학부
학생

관심분야 : 융합보안, 시스템보안, 네트워크보안
E-mail : yj941207@gmail.com

장 범 환
Chang Beomhwan

2012년 3월~현재
호원대학교 사이버수사보안학부
조교수
2003년 4월~2012년 2월
한국전자통신연구원 보보호연구단
선임연구원
2003년 2월 성균관대학교
컴퓨터공학과(공학박사)
1999년 2월 성균관대학교
컴퓨터공학과(공학석사)
1997년 2월 성균관대학교 전자공학과(공학사)

관심분야 : 네트워크보안, 보안정보시각화, 융합보안, 제어시스템 보안
E-mail : bchang@howon. ac. kr

이 영 숙
Lee Youngsook

2009년 3월~현재
호원대학교 사이버수사보안학부
부교수
2011년 8월 ~현재
호원대학교 사이버수사보안학부
학부장
2008년 8월 성균관대학교 컴퓨터공학과
(공학박사)
2005년 2월 성균관대학교 정보보호학과
(공학석사)
1987년 2월 성균관대학교 정보공학과(공학사)

관심분야 : 암호프로토콜 암호이론, 디지털 포렌식, 스마트폰 보안
E-mail : ysooklee@howon.ac.kr

논문접수일: 2016년 8월 9일
수 정 일: 2016년 8월 30일
게재확정일: 2016년 9월 8일