

보안 강화를 위한 NFC 기반 전자결제 시스템의 2 팩터 인증 기술의 초안 설계

(Draft Design of 2-Factor Authentication Technique for NFC-based Security-enriched Electronic Payment System)

차병래^{*,**}, 최명수^{**}, 박선^{*}, 김종원^{*}

(ByungRae Cha^{*,**}, MyeongSoo Choi^{**}, Sun Park^{*}, JongWon Kim^{*})

요약

오늘날 IT 기술의 적극적인 활용을 통해 은행을 비롯한 금융 산업 전체에서 거대한 혁명이 진행되고 있으며, 이를 ‘핀테크’라 부른다. 핀테크는 2016년 10대 인터넷 산업 이슈의 하나로 조명 받고 있다. 본 논문에서는 보안 강화를 위하여 FIDO 프레임워크를 이용한 NFC 기반 전자 결제 및 쿠폰 시스템에 2 팩터 인증 기술을 적용하기 위한 초안을 설계한다. 세부적으로 프론트엔드의 단말 디바이스에는 2 팩터 인증과 전자 서명 기술의 적용과 백엔드에는 클라우드 기반의 PG를 위한 분석회피형 악성코드 탐지기술을 을 적용하기 위한 연구를 수행한다.

■ 중심어 : 보안, 2 팩터 인증, NFC, 전자결제 시스템, 핀테크

Abstract

Today, the great revolution in all financial industrial such as bank have been progressing through the utilization of IT technology actively, it is called the fintech. In this paper, we draw the draft design of NFC-based electronic payment and coupon system using FIDO framework to apply the 2 factor authentication technique for strength security. In detailed, we will study that the terminal device in front-end will be applied the 2 factor authentication and electric signature, and cloud-based payment gateway in back-end will be applied malicious code detection technique of distributed avoidance type.

■ keywords : Security, 2 Factor Authentication, NFC, Electronic Payment, FinTech

I. 서론

오늘날 IT 기술의 적극적인 활용을 통해 은행을 비롯한 금융 산업 전체에서 거대한 혁명이 진행되고 있으며, 이를 ‘핀테크’라 부른다. 핀테크는 금융을 뜻하는 파이낸셜(Financial)과 기술(Technology)의 합성어로 스마트 기기로 결제하는 결제 시스템뿐만 아니라 예금, 대출, 그리고 자산 관리 등 각종 금융서비스를 IT기술을 통해 처리하는 금융과 IT가 융합된 산업을 말한다. 일상적인 모바일 banking 서비스나페이팔, 알리페이, 카카오페이 등의 결제 서비스와 전자 지갑도 핀테크의 대표적인 기술이다[1]. 핀테크는 그림 1의 ①과 같이 이미 10대 인터넷 산업 이슈 중의 하나로 조명을 받고 있으며, 국내 핀테크 시장 역시 정부의 규제 완화 및 육성 정책에 따라 급성장할 전망이다[2, 3].



그림 1. KISA의 2016년 인터넷 10대 이슈와 정보보호 10대 이슈

* 정희원, 광주과학기술원 전기전자컴퓨터공학부

** 정희원, 제노테크(주)

이 논문은 2016년도 미래창조과학부의 지원을 받아 수행된 시큐리티 스타트업 R&D 지원 사업의 결과물임 (No. B0717-16-0088).

접수일자 : 2016년 06월 13일

게재확정일 : 2016년 06월 29일

수정일자 : 2016년 06월 29일

교신저자 : 김종원 e-mail : jongwon@smartx.kr

영국에 소재한 국제통상기구 MEF(Mobile Ecosystem Forum, [4])가 발표한 2015년 세계 소비자 신뢰 리포트에서 모바일 결제에 대한 사용자 신뢰도가 낮아진 것으로 분석되었다. MEF는 15개국 모바일 사용자 15,000명을 대상으로 조사한 결과, ‘결제 시스템이 안전하지 않다’고 느끼거나 ‘서비스를 제공하는 대상을 신뢰하기 힘들다’라고 답한 응답자의 수가 증가했다. 전반적인 모바일 시스템에 대한 보안을 믿지 않아 스마트폰에 전자 지갑 앱을 다운받은 적이 없다고 답한 이들은 전체 응답자의 36%였으며, 반대로 모바일 결제 앱을 사용해본 적이 있거나 사용할 의향이 있다고 말한 이들은 15%에 불과했다. 또, 전체 응답자 가운데 22%가 자신의 개인정보가 허락도 없이 업체들에 의해 무단으로 수집, 활용될 것이 걱정된다고 대답했다. 모바일 결제 시스템에 대한 불신은 미국에서만 해도 지난 2013년 26%에서 2014년 35%로 증가했으며, 애널리스트들은 “이번 조사 결과는 향후 애플 페이와 같은 전자 결제 시스템은 물론, 관련 금융 애플리케이션 개발이 난항을 겪을 수 있다는 것을 시사하는 것”이라고 분석했다. 특히, MEF 의장 앤드류 버드는 “모바일 결제 부문의 기업들은 이번 조사 결과를 토대로 서비스 및 제품의 투명성과 안정성을 높이는 한편, 모든 면에서 사용자 프라이버시를 강화해야 한다”고 강조했다[5].

표 1. 모바일 에코시스템의 혜택과 문제점

프레임워크	항목	내용
NFC	혜택	거래 속도, 안전한 카드 데이터 저장, 데이터 망 불필요, 원격으로 초기화 가능
	문제점	복잡한 에코시스템, 일부 시장에서 가맹점 부족
	사례	Isis, 구글 월렛
클라우드	혜택	대부분의 장치와 운영체제 상에서 구동, 다양한 결제 방법(QR/바코드, 위치 정보)
	문제점	데이터 망에 의존, 보안표준 부족, 높은 처리비용으로 가맹점 부족
	사례	페이팔, 레벨업
폐쇄형 카드	혜택	대부분의 장치와 운영체제 상에서 구동, 소비자 위험부담이 적음, 기존 가맹점 POS 장비 사용, 대부분 보상 프로그램과 연계됨
	문제점	지원하는 판매자에 의해서만 가능, 직불/신용카드랑 연계될 경우 보안 위험 있을 수 있음
	사례	스타벅스, 던킨 도너츠

결제 프레임워크에는 보통 3 가지 종류로 NFC, 클라우드, 폐쇄형 카드가 있다[6]. NFC는 높은 수준의 보안과 위험 관리 프

로세스에 대해 선호하는 발행기관과 모바일 망에 의해서 선택된다. 독립된 스타트업 기업들은 클라우드 기반 월렛을 선호하고 그들의 사용자 카드들을 클라우드 기반 서비스와 연동하며 거래에 위치기반, 데이터 연결, QR 코드/바코드를 사용한다. 상인들은 폐쇄형 카드를 선택함으로써 자신이 저장해 놓은 값이나 재충전 선물 카드 시스템 같은 것을 주요 자금조달 수단으로 선택할 수 있는 것을 선호한다. 이 3 가지 에코시스템은 다양한 모바일 월렛의 지원이 가능하도록 같은 월렛에서도 사용할 수도 있다. 표 1은 모바일 상거래의 3 가지 결제 에코시스템과 이들의 사용자 경험상의 혜택과 문제점을 정리하였다.

본 논문의 2장은 관련 연구로서, NFC 기반 모바일 결제의 변화와 보안 인증 기술의 동향과 FIDO에 대해서 간략하게 기술한다. 3장에서는 기존에 개발된 NFC 기반 전자결제 시스템의 개요와 보안 강화를 위한 2 팩터 인증 기술을 적용한 전자결제 시스템의 초안을 설계하며, 마지막으로 결론으로 맺는다.

II. 관련 연구

1. NFC 기반 모바일 결제의 변화

NFC 기술을 기반으로 전자지갑 App 기반 모바일카드, 사용자 휴대단말기를 가맹점 POS로 활용하는 NFC 결제 서비스, 간단한 데이터 교환 및 전자화폐 기반 Money Transfer 등의 차별화된 서비스 제공이 가능하다. NFC는 크게 카드 모드, RFID 리더 모드, 그리고 P2P 모드로 구분되며, 카드모드는 비접촉식 스마트카드 기술 및 보안으로 교통카드와 할인쿠폰 등 다양한 모바일 결제 방식 제공할 수 있다. RFID리더모드는 단말 기기 뿐만 아니라 RFID 태그가 부착되어 있는 스마트포스터 등을 이용한 웹사이트 연결 및 정보 획득이 가능하다. P2P모드는 스마트폰과 PC 및 가전제품 기기 간 데이터 송수신 및 파일공유할 수 있다. 그림 2는 NFC 기반 모바일 결제 기술의 변화를 나타낸 것이다.



그림 2. NFC 기반 Mobile Payment 기술의 변화

2. 보안인증기술의 동향

다양한 무선 네트워크 서비스의 장단점을 상호 보완하기 위하여, 3G/WLAN/ WiBro 등을 포괄하는 통합 무선 네트워크 서비스 체계를 구축하고자 하는 노력이 활발히 이루어지고 있다. 이 때, 각 네트워크 간의 연동은 필연적이며 따라서 기존의 개별 네트워크를 넘어 연동되는 네트워크상에서의 인증, 키 교환 및 데이터 암호화 등을 가능하게 하는 연동 보안 기술이 요구된다. 3GPP TS 33.234 표준 문서에서는 WLAN과 3GPP 연동 환경에서 다음과 같은 보안요소 (security features)들이 제공되어야 한다고 정의하고 있다[7]:

- 가입자와 망간 인증 및 SA(Security Access) 관리
- 기밀성과 무결성 보호
- Immediate Service Termination
- WLAN UE 기능 분할

최근 금융거래 등 온라인결제 이용자들의 불편을 초래하는 동시에 각종 보안이슈의 온상으로 지적되어 왔던 액티브X를 대신해 공인인증서의 보안성을 담보할 새로운 대체기술로 최근 FIDO (Fast Identity Online)가 급부상 하고 있다[8]. 한국 인터넷진흥원에서 점차 사라지고 있는 액티브X 기반의 공인인증서의 한계점을 보완하기 위해 FIDO의 생체인증 기능과 공인인증서를 연계한 기술을 개발하고 있기 때문이며, FIDO가 공인인증서와 결합되면 생체인증기술을 통해 기존 공인인증서의 번거로움과 보안상 한계를 보완하는 동시에 모바일 결제 등에 있어 편리성을 확보할 수 있게 된다. 그림 1의 ②에 나타난 것처럼, FIDO는 2016년 정보보호 10대 이슈중의 하나로 선정되었으며, 그림 3은 FIDO의 UAF(Universal Authentication Framework)와 U2F(Universal Second Factor)의 표준화를 나타낸다.

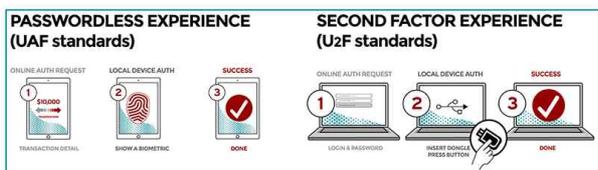


그림 3. FIDO의 UAF와 U2F의 표준화

또한, FIDO Alliance에서 진행하는 관련 기술의 국제표준에도 발맞추어 갈 수 있으며, 특히, FIDO 기술은 패스워드의 피로도가 증가함에 따라 나타나는 기존 ID와 패스워드 체계의 한계를 극복하고, 생체정보 전송 및 저장시 해킹 위험성을 최소화할 수 있는 새로운 인증방식 기술로 주목받고 있는 상황이며, 그림 4는 FIDO의 사용 분야를 간략하게 정리하여 나타냈다.



그림 4. FIDO의 사용분야

III. NFC 기반 모바일 전자 결제 및 쿠폰 시스템의 2 팩터 인증 기술의 초안 설계

기존에 개발된 NFC기반 전자 결제 시스템의 보안을 강화하기 위하여 2 팩터 인증과 전자서명, 그리고 분석회피형 악성코드 탐지기술[9]을 적용하기 위한 설계를 수행한다.

1. 기존의 NFC 기반 모바일 전자 결제 시스템의 개요 및 성능

가. NFC 기반 전자결제 시스템의 개요

기 개발된 NFC 기반 모바일 전자 결제 시스템의 환경은 그림 5와 같이 나타내며, 그림 6은 기 개발된 모바일 전자 결제 앱의 구성도를 나타낸 것이다. 그림 6의 NFC 기반 모바일 전자 결제 앱은 크게 회원 등록, 인증, 정보 수정, 그리고 결제, 구매이력 정보와 검색으로 구성되었다.

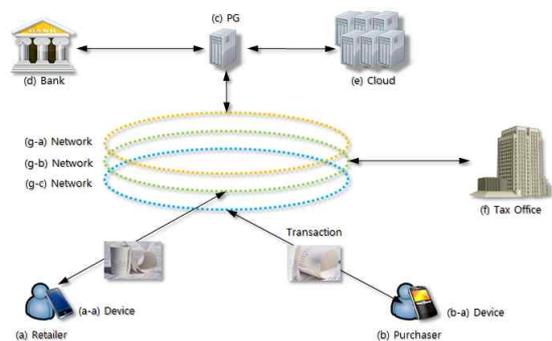


그림 5. 기 개발된 모바일 전자결제의 구성도

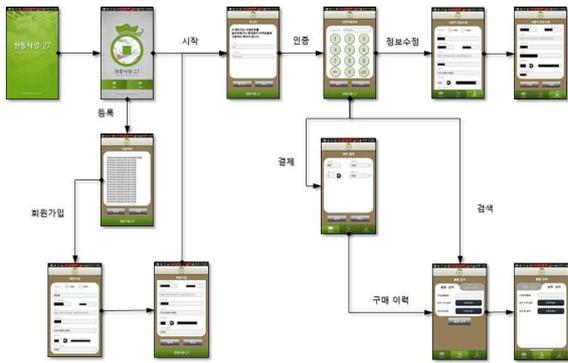


그림 6. 기 개발된 모바일 전자결제 앱의 구성도

나. NFC 기반 전자 쿠폰 시스템의 개요

기 개발된 NFC 기반 모바일 전자 쿠폰 시스템의 환경은 그림 7과 같이 나타내며, 그림 8은 기 개발된 모바일 전자 결제 앱의 구성도를 나타낸 것이다.

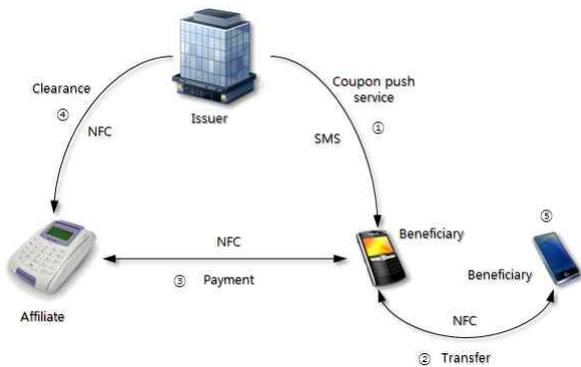


그림 7. 기 개발된 모바일 전자 쿠폰의 구성도

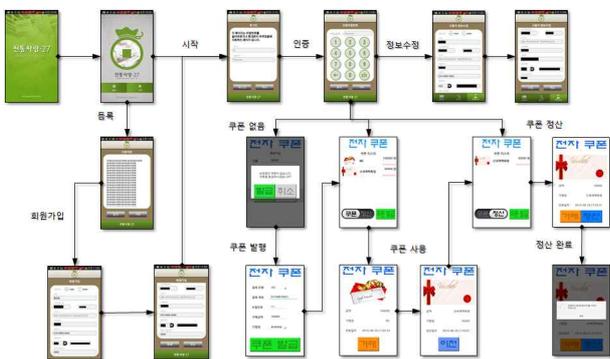


그림 8. 기 개발된 모바일 전자 쿠폰 앱의 프로토타입 구성도

그림 8의 NFC 기반 모바일 전자 쿠폰 앱은 회원 등록, 인증,

정보 수정, 쿠폰의 발행/사용/정산으로 구성되었다.

다. 전자 쿠폰의 시험 시나리오 및 결과

개발된 NFC 기반 전자 쿠폰 시스템의 성능 시험을 위하여 표 1과 같이 전자쿠폰의 시험 시나리오를 이용하였으며, 시험 환경은 성능 진단 프로그램인 Apache JMeter[10]를 이용한 성능을 테스트하였으며, 최대 동시 접속자 500명, 5초 간격 4회 반복 Request를 발생하여 테스트하였다. 그리고 전자쿠폰 시스템의 성능 시험 결과는 표 2와 그림 9에 나타내었다. 그림 9는 NFC 기반 전자 결제 및 쿠폰 시스템의 Payment Gateway 접속자 테스트 결과를 나타낸 것이며, 표 3과 같이 최소 응답 시간은 11 msec이며, 최대 응답 시간은 379 msec, 그리고 평균 응답 시간은 134 msec 이었으며, 처리율은 354.2 TPS 이었다.

표 2. 전자 쿠폰의 시험 시나리오

① 식권 판매대 도착	② 사용자 앱 실행
③ 식권 구매 선택	④ 구매할 식권 선택
⑤ 식권 구매에 대한 팝업 메시지 확인	⑥ 판매자와 태깅을 통한 구매 요청
⑦ 판매자 앱에서 구매 승인 및 결제 요청	⑧ 사용자 앱에서 결제 승인



2. NFC 기반 모바일 전자 결제 및 쿠폰 시스템의 2 팩터 인증 기술의 초안 설계

가. NFC 기반 전자결제 시스템의 설계

2 Factor 기반의 인증이 강화된 NFC 기반 전자결제 시스템은 주로 O2O(Online to Offline, [11]) 환경에서 소상공인을 위한 결제 시스템이며, 보안 측면에서는 2 Factor 인증 기능, 생체정보 인증 기능, 생체정보 보호 기능, 그리고 NFC-P2P결제 기능으로 구성되며, 그림 10과 그림 11에 나타난다. 그림 10과 그림 11에 추가될 보안 기능들을 표현하였다.

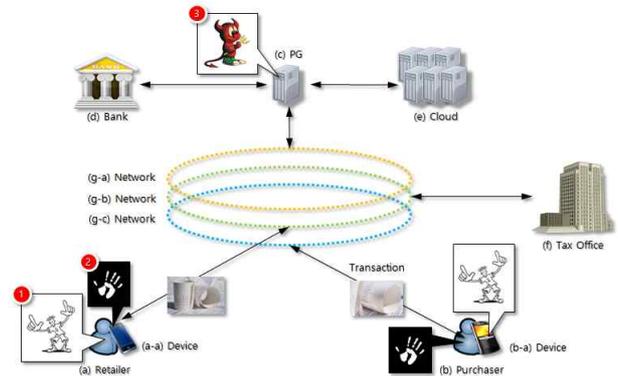


그림 10. 2 팩터 인증 기술에 의한 모바일 전자 결제의 초안 설계

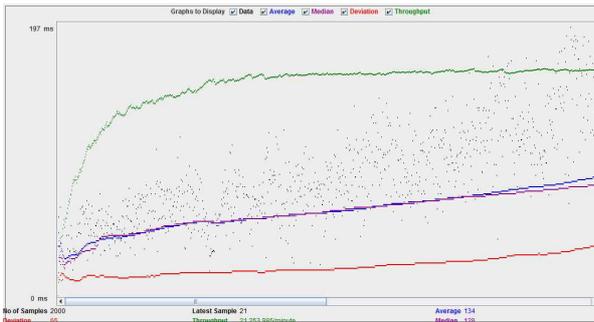


그림 9. NFC 기반 전자 결제 및 쿠폰 시스템의 Payment Gateway의 접속자 테스트 결과

표 3. 성능 시험 결과

총 테스트 횟수	2000 회 (500 * 4)	평균 응답 속도	134 msec
최소 응답 속도	11 msec	최대 응답 속도	379 msec
에러율	0.0%	처리율	354.2 TPS

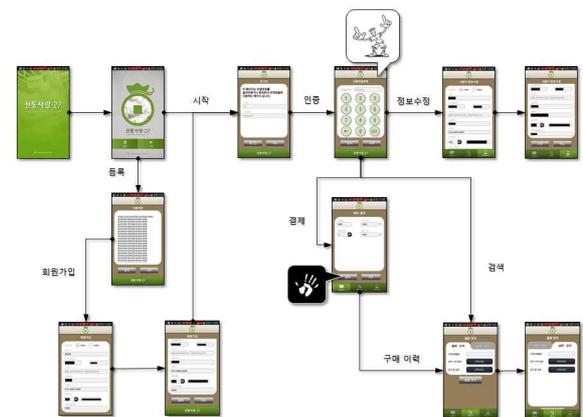


그림 11. 2 팩터 인증 기술에 의한 모바일 전자결제 앱의 구성도 초안

NFC 기반 전자 결제 및 쿠폰을 지원하기 위한 프론트엔드에는 결제 시스템의 단말 디바이스가 존재하며, 단말 디바이스는 멀티 인증을 제공하기 위한 수단으로 기존의 인증 기술에 새로운 인증기술을 결합하여 안전하고 편리한 인증을 제공하

고자 하며, 2 팩터 인증의 요소기술로 FIDO를 적용할 예정이다. FIDO 프레임워크 기반으로 지문을 우선적으로 적용하며, 추가적으로 전자서명 기술을 적용하고자 한다. 전자서명은 NFC 카드에 공인인증서를 저장하고 사용 시에 카드를 터치하여 인증 및 전자서명을 하게 되며, NFC 결제시 사용자의 터치 사인에 의한 인증을 강화한다.

나. NFC 기반 전자 쿠폰 시스템의 설계

2 Factor 기반의 인증이 강화된 NFC 기반 전자쿠폰 시스템은 그림 12와 그림 13에 나타낸다. 그림 12와 그림 13에 추가될 보안 기능들을 표현하였다.

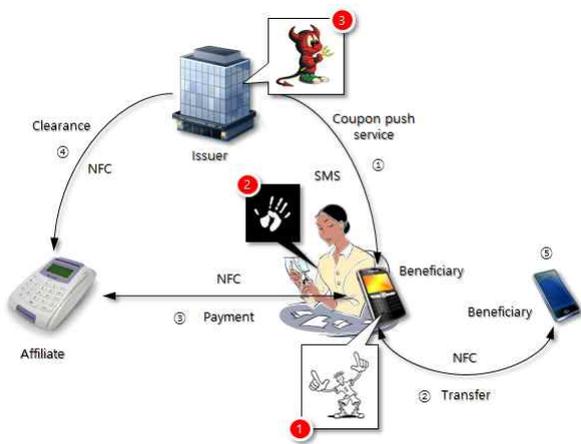


그림 12. 2 팩터 인증 기술에 의한 모바일 전자 쿠폰의 초안 설계

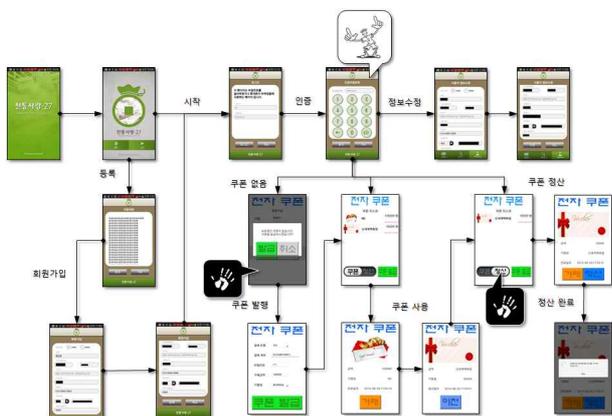


그림 13. 2 팩터 인증 기술에 의한 모바일 전자 쿠폰 앱의 구성도 초안

NFC 기반 전자 결제 및 쿠폰을 지원하기 위한 백엔드에는 Payment Gateway가 존재하며, 일반적인 서버가 아닌 클라우드

드 기술을 이용하며 Payment Gateway를 지원하고자 한다. 클라우드 환경으로의 이전은 가상화 기술에 의한 결제 시스템의 자동 스케일링뿐만 아니라 사이버 탄력성에 의한 다양한 보안 기능을 지원하고자 한다. 특히 클라우드 환경에서의 분석회피형 악성코드 탐지기술은 악성코드가 사전에 가상분석 환경을 조화/검사하는 분석회피 행위 탐지하며, 전자결제의 안전성 제공을 위해 Payment Gateway에서의 악성코드에 의한 부정 결제를 방지할 수 있다.

IV. 결론

NFC 기반의 전자결제 시스템은 전통시장의 활성화를 위하여 소상공인과 소비자들 간의 현금 및 온누리 상품권 등과 같이 편리한 결제수단을 제공하여 매출과 매입의 편리성과 온누리 상품권의 음성적 유용을 차단하는 역할을 수행하고, 그로 인한 부수적으로 사용자의 스마트한 커머스 문화를 만들어 주는 역할을 수행하고 한다. 특히 결제 시스템에서 보안 사고는 매우 치명적이며, 이를 보완하기 위하여 2 팩터 인증을 추가하기 위한 결제 시스템을 설계하였다. 포엔드의 단말 디바이스에는 2 팩터 인증과 전자 서명 기술의 적용과 백엔드에는 클라우드 기반의 PG를 위한 분석회피형 악성코드 탐지기술을 을 적용하기 위한 연구를 수행한다. 향후 다양한 형태 및 비즈니스 모델들의 전자 상품권 및 전자쿠폰, 전자계약 등으로 발전시킬 예정이다.

References

- [1] 강창호, 이정훈, "IT와 금융이 만나는 새로운 세상, 핀테크," 한빛미디어, 2015년 6월5일.
- [2] "2015년 인터넷 및 정보보호 10대 산업 이슈 전망," 한국인터넷진흥원(KISA), 2014년 12월.
- [3] "2016년 인터넷 및 정보보호 10대 이슈 전망," 한국인터넷진흥원(KISA), 2015년 12월.
- [4] MEF, <http://www.mobileecosystemforum.com/>
- [5] Matt Hamblen "모바일 결제 못 믿겠다...사용자 불신 증가,"ITWORLS, 2015년 2월 10일, [Internet] <http://www.itworld.co.kr/news/91836>
- [6] 스킵 알럼스, "모바일 결제 UX 디자인," 비제이퍼블릭, 2015년 7월 7일.
- [7] 3GPP TS 33.234 표준, <http://www.3gpp.org/Dyna-Report/33234.htm>
- [8] FIDO Alliance, <https://fidoalliance.org/>
- [9] 박용수, "(코드 가상화 기법이 적용된) 악성코드 분석방법 연구," 진한엠앤비, 2015년.
- [10] Apache JMeter, <http://jmeter.apache.org/>
- [11] O2O, <http://www.tmogroup.asia/china-online-to-offline/>

 저 자 소 개

차병래



2004년 목포대학교 대학원 컴퓨터공학과 졸업(공학박사)
 2005년 호남대학교 컴퓨터공학과 전임 강사
 2009년 ~ 현재 광주과학기술원 전기전자컴퓨터공학부 연구

조교수

2012년 ~ 현재 제노테크(주) 대표

<주관심분야 : 정보보안, IDS, Neural Network, Cloud Computing, VoIP, NFC 등>

최명수



2009년 목포대학교 전자공학과 공학박사
 2009년 목포대학교 해양텔레매틱스기술개발센터 박사후연구원
 2010년 목포대학교 정보산업연구소 연구전임교수

2015년 ~ 현재 제노테크(주) 기업부설연구소 연구소장
 <주관심분야 : 정보보안, IDS, Neural Network, Cloud Computing, VoIP, NFC>

박 선



2007년 인하대학교 컴퓨터정보공학과 공학박사
 2008년 호남대학교 컴퓨터공학과 전임 강사
 2010년 전북대학교 인력양성사업단 박사후 과정

2010년 목포대학교 정보산업연구소 연구전임교수

2013년 ~ 현재 광주과학기술원 전기전자컴퓨터공학부 연구조교수

<주관심분야 : 정보검색, 데이터마이닝, 해양IT정보융합, 클라우드 컴퓨팅, IoT, 스토리지 시스템>

김종원



1997년 University of Southern California 연구 조교수
 1999년 Technology Consultant for VProtect Systems Inc.
 2000년 Technology Consultant for Southern California Division

of InterVideo Inc.

2001년 광주과학기술원 정보기전공학부 부교수

2008년 ~ 현재 광주과학기술원 전기전자컴퓨터공학부 교수

<주관심분야 : Future Internet, SDN & NFV, SDI>