디지털산업정보학회 논문지 제13권 제4호-2017년 12월
http://dx.doi.org/10.17662/ksdim.2017.13.4.107

은행권 오픈플랫폼 보안취약성 분석과 보안대책

김 상 근*

Banknote Open Platform Security Vulnerability Analysis and Security Measures

Kim Sanggeun

〈Abstract〉

Open platform technology in the banking industry is anticipated to impact the market very positively together with the activation of Fin Tech services. The domestic environment of payment services has been rapidly changing into the mobiles and multiple new payment services have been introduced from a variety of vendors. However, the convenience of payment always causes worsening the security, and the accidents on the security have been continued to occur such as leakage of personal information, hacking and so on upon the expansion of the industry and the market size. This study aims to analyze the status of Fin Tech open platforms and various problems of the related standard technologies, and to suggest the possible solutions. Upon the analysis results, it was confirmed that multiple solutions were required to improve the main security protocols of open platforms and to process the security functions diversely. In conclusion, the results of this study will be helpful to determine the direction of the solution on the security issues in the open platform environment of the current industry.

Key Words : ActiveX, Open Platform, Mobile Apps, Non-ActiveX, Pin-Tech

Ⅰ. 서론

최근 은행권에 핀테크(Pin-Tech) 오픈플랫폼 시장이 활성화되고 있다. 관련 업체와 은행권의 참여를 시작으로 관련 업계 전문가들은 시장 가능성에 대하여 의논하고 있는 실정이다[1]. 장기적으로는 핀테크 이후 새로운 신기술을 통해 금융권 분야로 오픈플랫폼이라는 통합 서비스 체제(공통 API, 인증/관리)가 확대 될 것으로 예상하고 있다[2].

* 성결대학교 컴퓨터공학부 교수

그러나 보안 분야에서는 새로운 플랫폼 등장과 통합은 매우 민감한 문제이다. 기존 플랫폼에서 알려진 다양한 보안 취약성들을 내포하고 있기 때문이다. 이러한 보안 취약성들에 대한 새로운 보안기술 개발은 비용에 큰 부담이 될 수밖에 없다. 그러나 비용적인 문제 보다 특히 금융권 같은 온라인 뱅킹은 보안기술의 수준이 가장 높아야 하고, 지속적으로 유지 및 개선되어야 할 대상으로 인식되어야 한다.

본 논문에서는 국내 은행권의 오픈플랫폼을 중심

으로 상호관계에 있는 기술들의 문제점을 분석하고, 문제점 별 해결과제에 대하여 설명한다. 본 논문은 모두 5장으로 구성된다. 2장 관련연구는 은행권 오픈플랫폼과 보안기술 현황 분석, 3장 문제점 분석, 4장 해결방안, 5장 결론으로 마친다.

Ⅱ. 관련연구

2.1 은행권 오픈플랫폼 현황

2016년 8월 금융권 공동 핀테크 오픈플랫폼이 국내 최초 개통되었고, 현재 업체 및 은행에서 핀테크 기술을 기반으로 다양한 금융 서비스를 제공하고 있다[3]. 표 1은 2017년 하반기 기준 국내 은행권의 오픈플랫폼 현황을 나타낸다.

<표 1> 국내 은행권 오픈플랫폼 적용 현황

Bank	Service	API
WOORI	Wibee Bank	Service API : Transaction history, Account / Balance inquiry, Incoming / Outgoing transfer, Account real name inquiry, etc. Authentication / Management : User Authentication, Management
NongHyup	NH Pin-Tech OpenPlatform	
KDB	-	
SHINHAN	Sunny Bank	
SC	-	
IBK	-	
Kookmin	Liiv	
KEB	Hana 1Q bank	
CITI	Citi Mobile	

각 은행마다 개인 또는 기업을 대상으로 PC 웹(Web) 또는 모바일 앱(App) 서비스를 제공하고 있다. 참여중인 협력기관은 유관기관을 제외한 은행 총 16개로 표 1의 은행권 이외 7개는 수협, 대구, BNK, 광주, 제주, 전북은행이다[4]. 대부분 기존 플랫폼의 서비스를 유지하고, 추가적으로 핀테크 기술 관련 오픈플랫폼 서비스를 제공하는 형태이다. 주요 플랫폼이 PC의 웹 환경보다 모바일 앱 서비스에 집중되어 있지만, 결국 오픈플랫폼 서버를 통해 인증하고 통신하는 구조이다. 사용자와 은행권을 연결하는 과정에서 공통적으로 사용자 인증에 OAuth 2.0 기술을 사용하고 있다[5].

오픈플랫폼은 OAuth 2.0 표준안을 준수하여 개발되었으며, HTTP 프로토콜의 URI 주소를 사용하는 REST API 방식을 사용하고 있다. 금융보안원은 오픈플랫폼 활성화 이전에 알려진 보안취약점(중간자 공격, 웹 서버 해킹, 단말 악성코드 감염 등)을 고려하여 핀테크 서비스 보안취약점 점검항목을 배포하고 있다[6].

2.2 은행권 보안기술 현황

2017년 대선이후 국내 전자정부 사이트의 전면 ActiveX 폐지 정책이 거론되었고, 다시 여론 및 언론의 관심을 집중적으로 받았다. 보안 분야에서 ActiveX 기술은 최근까지 의존성 문제, 보안 취약성, 관련 규제 등 기술적 및 사회적으로 이슈가 되어왔고, 다양한 대체기술에 대해 논의되어왔다[7, 8]. 표 2는 2017년 하반기 기준 국내 은행권의 Non-ActiveX 적용 현황 조사 결과를 나타낸다.

<표 2> 국내 은행권 Non-ActiveX 적용 현황

BANK	Non-ActiveX	Additional Installation
Kookmin	○	Certified Certificates, Integrated Security Program
WOORI	○	Certified Certificates, Personal PC Firewall, Keyboard Security, Security Log

BANK	Non-ActiveX	Additional Installation
NongHyup	○	Certified Certificates, Personal PC Firewall, Keyboard Security, Secure Browser
KDB	○	Integrated Security Program, Certified Certificate
SHINHAN	○	Anti-hacking, Keyboard security, Certified certificates
SC	○	Certified Certificates, PC Firewall, Keyboard Security, IP Tracker
IBK	○	Keyboard Security Extension
KEB	○	Keyboard Security Extension
CITI	○	Certified certificate, Prevent keyboard hacking, Verify user information, Personal PC firewall, Virus spyware scan

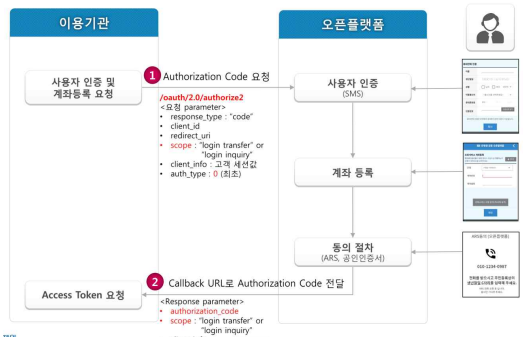
오픈플랫폼 지원 은행권을 대상으로 크로스 브라우징 적용 유무를 조사한 결과 대부분 Non-ActiveX를 지원하는 것으로 나타났다. 그러나 로그인 수행 과정에서 기존 ActiveX 형태로 설치되던 추가 설치 프로그램들이 모두 .exe 형태로 제공되고 있다. 다운 및 설치파일을 실행하는 방식은 또 다른 형태의 ActiveX일 뿐이라고 논란이 되었기 때문에 대체기술로 웹 표준을 준수하는 개발 형태로 변화하고 있다[9].

Ⅲ. 문제점 분석

분석 대상은 첫 번째 오픈플랫폼의 공통 사용자 인증 노드, 두 번째 현재 오픈플랫폼 주요 서비스 환경인 모바일 환경의 웹 표준 기술을 중점적으로 분석한다.

3.1 사용자 인증노드

오픈플랫폼은 결제업체가 오픈플랫폼 센터의 오픈 API를 이용하여 은행 공동망간 상호 통신하는 구조로 설계되어 있다. OAuth 2.0 인증 프로토콜은 HTTPS(Hypertext Transfer Protocol over Secure Socket Layer) 기반으로 API 키와 토큰을 발급하는 보안세션을 생성하지만 중간자 공격, 서버 해킹 등 세션 노출의 가능성이 존재한다[10]. 금융보안원에서는 모바일과 웹에 대한 인증 취약점 리스트 31개 항목에서 인증부분으로 멀티 로그인 탐지 적용 수준, 인증우회 방지 적용 수준을 점검 하도록 권고하고 있다.

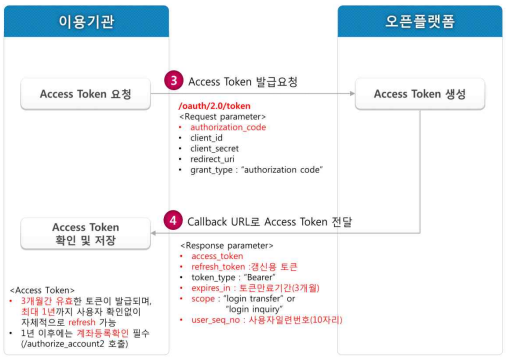


<그림 1> 오픈플랫폼 개발자 가이드 매뉴얼
(사용자 인증과 등록과정)

그림 1과 같이 이용기관의 최초 사용자 인증 및 계좌등록 과정[10]에서 중요정보는 고유 식별 ID, URI(Uniform Resource Identifier), 고객 세션값 등이 있다. 두 구간 사이의 중요 파라미터들을 변조하는 중간자 공격을 가정할 수 있다. 공격자가 ID, URI, 고유세션, 인증코드를 얻을 수 있다. 오픈플랫폼의 SMS(Short Message Service) 인증은 중간자 공격의 유무를 감지할 수 없기 때문에 해결책이 되지 않는다. 이외 SKIP 상태 값을 수정하여 인증을

우회하거나 인증타입 상태 값을 최초(0)로 변조하여 사용자의 새로운 갱신된 중요정보를 재요청할 수 있다.

그림 2와 같이 토큰발급 과정[10]을 살펴보면 인증코드를 통해 권한을 부여받기 때문에 그림 1과정에서 중요 정보들로 토큰정보를 쉽게 얻을 수 있다. 그리고 각 구성요소 자신을 증명하는 제 3자 인증주체가 없다. 개발자가 실제로 매우 복잡한 OAuth 2.0 프로토콜을 직접 강화하여 인증우회를 방지하는 것은 현실적으로 어렵다. 이 때문에 공통 API를 사용하는 모바일 앱의 인증 기능이 오픈플랫폼 인증서버에 전적으로 의존적이게 된다.



<그림 2> 오픈플랫폼 개발자 가이드 매뉴얼(토큰발급 과정)

3.2 웹 표준 기술과 오픈플랫폼

현재 은행권의 .exe는 ActiveX 기반 보안 기능을 대체하기 위한 기술이다. 기존 대부분 은행에서 ActiveX 기반 공인인증서를 지원했지만 Non-ActiveX로의 웹 환경 변화는 현재 오픈플랫폼 환경에도 적지 않은 영향을 주었다고 할 수 있다. 공인인증서 사용의무 폐지[8]와 함께 최근 전자금융거래에 대한 보안성 심의가 전면폐지[11] 되면서 각 업체별로 각 다른 금융 앱을 출시하고 있는 실정이다.

금융보안원은 오픈플랫폼 모바일 보안을 위해 보안 취약점 점검항목을 제공한다. 여기서 모바일 보안 취약점 점검항목[6]을 살펴보면 입력정보 보호적용 수준, 앱 위·변조 탐지 적용 수준, 해킹 운영체제 탐지 적용 수준, 안티디버깅 적용·탐지 수준, 코드 난독화 적용 수준, 안티바이러스 적용 수준 총 6가지를 점검하도록 하고 있다. 2016 모바일 OWASP Mobile TOP 10[12]은 점검 6가지 항목과 부분적으로 일치하는 모바일 보안 취약점에 대하여 설명한다. M1 부적절한 플랫폼 사용, M3 안전하지 않은 통신, M7과 M8 이용자 코드 품질과 코드 변조 등이 있다. M1의 경우 루팅(Rooting)으로 인한 부적절한 코드 실행과 관리자 권한 부여 취약점을 의미한다. M3의 경우 통신 성능 효율성 문제 때문에 HTTPS를 사용하지 않는 앱의 통신 보안 취약점, M7 M8은 시큐어 코딩(Secure Coding) 가이드라인의 부재로 인한 보안 코딩 미적용 문제이다.

M3은 보안통신의 적용 유무는 개발자의 입장에서 성능 효율성에 관련된 매우 민감한 문제이다. 내부 로컬(Local)의 주요 중요 파라미터들은 암호화하지 않는 경우 해킹에 쉽게 정보가 노출될 가능성이 높다. 2017년 후반기 CVE() 기준 애플(Apple) IOS(iPhone OS)[13]는 취약점 344개, 구글(Google) 안드로이드(Android)는 692개[14]로 매년 새로운 취약점이 발견되고 있다. 오픈플랫폼 관련 모바일 앱은 이를 운용하는 은행권에 따라 다르기 때문에 보안 수준에 차이가 있다. 문제는 각 은행권이 공통 API는 활용하지만 모바일 앱을 개발하는데 공통 보안기술이 적용되지 않았음을 의미한다. 가장 최근(2015년)에 발표된 모바일 취약점 점검가이드[15]와 OWASP Mobile Top 10 취약점 항목[12]의 점검항목을 살펴보면 비교적 모바일 자체에 대한 보안 취약점검 항목은 잘 정의되어 있다고 볼 수 있다. 그러나 모바일 보안 가이드라인이 오픈플랫폼의 보안

프로토콜을 개선하거나 플랫폼 자체의 안전성을 제공해주지는 않는다.

분석결과 오픈플랫폼 환경은 기존 제 3자에 의한 상호인증 연계의 부재, 서버 플랫폼의 인증 프로토콜 안전성 문제, 이외 공통 API를 활용하는 모바일 환경을 중심으로 보안 위협에 대해 강력한 안전성을 제공해주지 않는다.

Ⅳ. 해결방안

표 3은 문제점 항목과 해결방안을 나타낸다. 본 관련연구에서 나타난 문제점을 통신노드, 로컬, 서버 3가지 유형으로 분류하고 해결방안에 대하여 설명한다.

<표 3> 문제점 유형 별 해결방안

Type	Problem	Solution
Communication Node	Possibility of bypassing certification due to important information tampering	Third-party verification of URIs
	Do not use HTTPS communication	Validation and application of non-HTTPS communication section
Local	No encryption of input information	Encryption at the user input interface level
	Local hacking of the issued token	Continuous session validation inside the app
Server	Request permission for an abnormal user's resource or token	Third-party server validation for authorization
	Authentication server dependency problem such as open platform server hacking	Establish distributed authentication server for each role

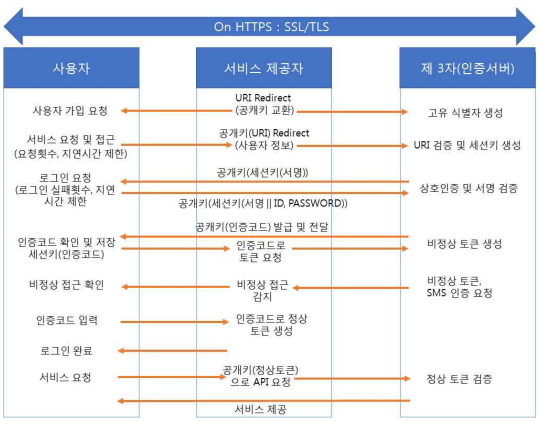
통신노드 보안위협 : 최초 사용자 등록과정 등에서 요청하는 URI에 대한 제 3자 검증을 수행한다. 중간자 공격에 대응하기 위해 URI에 포함된 다양한 통신 정보들을 조합하여 디지털 서명(Digital Signature) 등을 생성하고, 초기 통신과정부터 검증을 수행한다. 이외 분산 서비스 공격(Distributed DoS)이나 불법 URI 요청에 대한 요청 횟수 제한, 요청시간의 지연 방법을 적용할 수 있다.

앱의 통신노드의 경우 각 앱의 웹 보안 표준 안전성(HTTPS)을 지속적으로 검증되어야 한다. 이는 서버보안관리자의 서버 플랫폼의 보안패치 관리가 중요하다는 것을 나타낸다. 그리고 인증 서버 자체에서 HTTPS 통신에 대해 세션을 얼마나 유지할지, 사용자 이벤트에 대해 어떻게 다시 세션들을 갱신할지 주의해야한다. 주요 방법으로는 세션유지 시간을 짧게 설정하고, 모든 이벤트에 대해 세션을 갱신하는 방법을 적용할 수 있다.

로컬 보안위협 : 조사 결과 PC 웹의 경우 대부분 키보드 보안 프로그램이 존재했다. 모바일의 경우 사용자의 모든 입력 인터페이스에 암호화를 적용해야한다. 앱 수준에서의 암호화이기 때문에 암호화 알고리즘 표준 선택에 매우 주의가 요구된다. 반드시 앱 내부 로컬 수준에서 암호화를 적용하도록 해야 한다. 이외 로컬 내에 발급받은 토큰유출로 인해 공격자가 세션을 취득할 수 있는 가능이 존재한다. 앱 내부 수준에서 지속적으로 세션을 검증하도록 적용되어야 한다.

서버 보안위협 : 앞 두 항목에서 설명한 통신 또는 로컬에서 접근하는 모든 공격 형태는 서버에 대한 해킹 가능성 문제의 원인이 된다. 오픈플랫폼에 보안이 매우 의존적인 구조이기 때문에 오픈플랫폼에서 OAuth 2.0 인증 프로토콜 자체도 강화해야 하지만, 서버자체 보안 또한 매우 중요하다. URI 검증, 기본 사용자 인증과 서명 검증, 토큰 발급 및 검증 등 전체 과정이 분산된 인증 서버를 통해서 수행되어야 한다.

그림 3은 본 논문에서 제시한 해결방안들이 적용된 OAuth 2.0 보안 프로토콜에 대한 전체 구조도를 나타낸다. 기존 SSL/TLS 위에서 실행되는 OAuth 2.0 프로토콜 과정에 추가 상호인증을 위한 공개키 기법을 적용한다. 또한 이중토큰을 이용한 비정상 접근 감지 방법을 적용한다. 이외 무차별공격이나 DDOS에 대한 해결방안으로 각 요청 횟수, 시간 지연 설정 등을 포함한다.



<그림 3> 개선된 OAuth 2.0 보안 프로토콜 전체 구조

기본적으로 초기 URI_Redirect 과정에서 SSL/TLS와 다른 공개키를 추가 교환하고 세션키를 이용하여 암호화를 기본으로 수행한다. 외부는 기본 HTTPS로 동작하면서, 내부에서 또다른 공개키 기반 보안채널을 생성하는 것으로 이중 공개키 보안채널을 수행한다. 토큰 발급과정에서 1차적으로 비정상 토큰을 전달하고 SMS 인증과정에서 입력된 인증코드를 활용하여 정상 토큰을 생성한다. 비정상 토큰은 해커의 비정상 접근을 감지하고, 세션을 지속적으로 갱신할 수 있는 효과적인 방법이다. 기존 SMS 인증과정은 OAuth 2.0 보안 프로토콜과 독립적이기 때문에 Two-factor 인증에도 불구하고 제 3자 공격에 안전하지 않았다. 결론적으로 이중 보안 채널 기반으로 프로토콜 수행과정에서 중요한 토큰생성을 SMS 인증과정의 정보들로 조합하여 강력한 보안성을 제공하는 방법이다.

Ⅴ. 결론

본 연구에서 살펴본 오픈플랫폼 환경은 보안 프로토콜의 자체 취약점도 존재하지만, 외부적인 요인으로 모바일 앱 같은 다른 환경에서의 보안 취약점들도 포함한다. 수많은 금융시장과 연계되는 은행권의 오픈플랫폼 은 가장 강력한 보안성을 제공해야 한다. 하지만 기존 웹 환경과 모바일 환경의 빠른 변화에 적응하기 어려운 것이 현실이다.

현황 조사 결과 .exe와 같은 ActiveX 대체 기술은 오랜 기간 동안 문제점으로 남아있다. 또한 환경에 변화에 따른 새로운 취약성들은 아직 정확하게 파악도 하지 못한 실정이다. 분석결과 오픈플랫폼과 각 다른 금융 앱에서 나타나는 보안 취약성은 명확한 검증을 위한 방안이 전무하다. 이는 공통적인 보안 프레임웍이나 환경에 적절한 시큐어 코딩 가이드라인 등 통합 및 표준화가 우선적으로 요구된다. 이외 사건/사고 처리 및 대응과정, 법/제도적인 부분이 반드시 체계적으로 개발/보완되어야 할 것이다.

참고문헌

[1] 박재석, 김민진, 황병일, “핀테크의 발전 배경과 주요 동향,” 한국통신학회지, 제33권, 제2호, 2016, pp. 52-58.

[2] 장상수, “핀테크(Fintech)가 정보보호산업에 미치는 영향에 대한 고찰,” 한국인터넷진흥원, INTERNET & SECURITY FOCUS, 2015.

[3] 한국금융연구원, “경제·금융 관련 주요 정책 및 시장 동향,” 제25권, 제30호, 2016, p. 20.

[4] https://www.open-platform.or.kr/apt/content/openplatform

[5] https://developers.open-platform.or.kr/openapi/oauth

[6] 한국금융연구원, “핀테크서비스 보안 취약점 점검 항목,” 금융보안원 핀테크보안팀, 2017.

[7] 맹영재, 신동오, 김성호, 양대헌, 이문규, “국내 인터넷뱅킹 계좌이체에 대한 MITB 취약점 분석,” 한국인터넷진흥원, 제1권, 제2호, 2010, pp. 101-118.

[8] 이정현, “스마트 환경에서의 공인인증서 활용과 문제점,” 한국인터넷진흥원, Internet & Security Focus, 2013.

[9] 미래창조과학부, “2016년 ICT 융합 신산업을 여는 규제개혁 사례집 – ICT 융합 신산업을 여는 규제개혁,” 2016.

[10] https://www.open-platform.or.kr/apt/content/openapi

[11] 금융위원회, “전자금융감독규정,” 2015-18호, 2015.

[12] https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10

[13] http://www.cvedetails.com/product/15556/Apple-Iphone-Os.html? vendor_id=49

[14] http://www.cvedetails.com/product/19997/Google- Android.html?vendor_id=1224

[15] 행정자치부, 한국인터넷진흥원, “모바일 전자정부 대민서비스 개발자를 위한 모바일 대민서비스 보안취약점 점검 가이드,” 2015.

■ 저자소개 ■

김 상 근
(Kim Sanggeun)

1996년 3월~현재
성결대학교 컴퓨터공학과 교수
2003년 - 2004년
Sydney University 방문교수
1996년 2월
중앙대학교 컴퓨터공학과 (공학박사)

관심분야 : 정보보안, 핀테크, 빅데이터
E-mail : sgkim@sungkyul.edu

논문접수일 : 2017년 10월 24일
수 정 일 : 2017년 11월 20일
게재확정일 : 2017년 11월 22일