https://doi.org/10.33778/kcsa.2019.19.4.115

소셜 네트워크 서비스의 보안 위협요인에 관한 연구★

전 정 훈*

요 약

최근 스마트 기기의 사용이 보편화됨에 따라 다양하고 편리한 서비스들이 개발되고 있다. 이러한 서비스들 중, 소셜 네트워크 서비스(SNS: Social Network Service)는 언제, 어디서나 접근이 용이하다. 특히 정보의 공유뿐만 아니라, 사이버 상에서 사회적 관계를 형성하여 새로운 인맥을 확대시켜주고, SNS의 계정은 다른 서비스의 인증수단으로 사용되어 항상 사용자들에게 신속성과 편의성을 제공한다. 그러나 이와 같은 SNS의 여러 장점들에도 불구하고, 다양한 서비스들과의 연동과정에서 발생하는 보안 취약점들로 인해, 개인정보의 유출 사고가 끊임없이 발생하고 있어, 잠재적 위험요인에 대한 대응방안의 마련이 절실히 필요한 상황이다. 따라서 본 논문에서는 향후 SNS의 사용이 급격히 증가할 것으로 전망되고 있는 가운데, 소셜 네트워크 서비스의 보안 위협요인들에 따른 대응기술들을 알아봄으로써, 대응기술 개발의 기초 자료로 활용될 것으로 기대한다.

Study on the Security Threat Factors of Social Network Services

Jeon Jeong Hoon*

ABSTRACT

Recently, as the use of smart devices is becoming more common, various and convenient services are being developed. Among these services, the Social Network Service(SNS) is easily accessible anywhere, anytime. In particular, as well as sharing information, it forms a social relationship in cyberspace to expand new connections, and the SNS account is used as an authentication means of other services to provide users with speed and convenience at all times. However, despite the many advantages of SNS, due to security vulnerabilities occurring in the interworking process with various services, accidents of personal information are constantly occurring, and it is urgent to prepare countermeasures against potential risk factors. It is a necessary situation. Therefore, in this paper, the use of SNS is expected to increase rapidly in the future, and it is expected that it will be used as the basic data for developing the countermeasures by learning the countermeasures according to the security threats of the SNS.

Key words : SNS, OAuth, OpenID, Threat Factor, CSRF, Covert Redirect, OWASP

접수일(2019년 10월 1일), 게재확정일(2019년 10월 25일)

* 동덕여자대학교/컴퓨터학과

★ 본 논문은 2018년도 동덕여자대학교 학술연구비 지원에 의하여 수행된 것임.

1. 서 론

최근 스마트 기기의 사용과 새로운 서비스의 요구가 증가하면서, 시간과 장소의 제약성을 극복한 서비스의 개발이 활발히 진행되고 있다. 이러한 서비스들 중 소셜 네트워크 서비스(SNS:Social Network Service)는 전 세계로 빠르게 확산되며, 글로벌 서비스로의 영향력이 높아지고 있다. 이와 같은 SNS가 빠르게 확산될 수 있었던 배경에는 스마트폰이라는 전달매체가 있었다[1]. 스마트폰은 일상생활에 없어서는 안 될 필수용품으로 이동성과 편의성, 신속성을 제공하며 SNS의 확산에 촉매제 역할을 하고 있다고 해도 과언이 아니다.

SNS는 정보의 공유와 사회적 인맥 관계를 생성 및 유지, 관리해주며, 다른 서비스를 사용하는데 간단한 확인 절차만으로 인증을 대신하는 서비스를 제공하고 있다. 이와 같은 서비스에 사용되는 프로토콜은 SNS별로 상이할 수 있으며, 이용자에게 간단하고, 편리한 특징을 갖는다. 그러나 사용되는 프로토콜이나 개발방법에 따라 다양한 잠재적 취약점들을 갖고 있어, 지속적인 대응기술의 진화가 요구되고 있는 상황이다.

따라서 본 논문은 SNS의 사용이 일상생활의 일부가 되고, 이용자 또한 계속해서 증가하고 있는 상황에서 보안 위협요인들을 알아봄으로써, 향후 SNS의 서비스 개발뿐만 아니라, 대응기술의 개발에 부합하는 기초 연구 자료로 활용될 수 있을 것으로 기대한다. 그리고 본고의 논리적 구성을 위해 2장은 SNS의 동향에 대해 알아보고, 3장은 SNS의 보안 취약점들을 알아본다. 그리고 4장의 보안 위협요인 및 대응기술과 마지막 5장의 결론 부분으로 이글을 마치도록 한다.

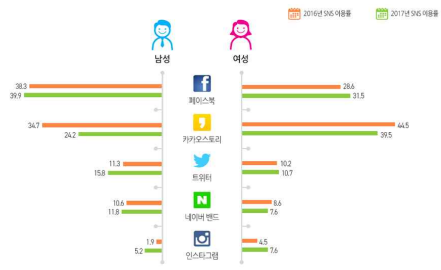
2. 관련 연구

2.1 소셜 네트워크 서비스(SNS)

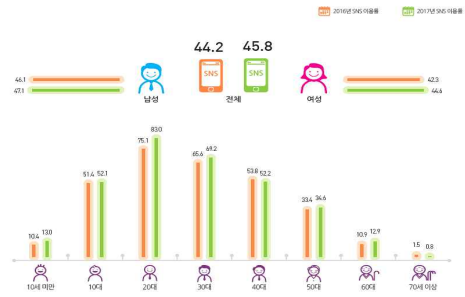
SNS는 온라인상에서 공통의 관심사를 가진 사용자 간의 '관계 맺기' 기능을 지원하고, 축적된 지인 관계를 통해 '인맥 관리', '정보 공유' 등 다양한 커뮤니티 활동을 할 수 있도록 하는 서비스이다. 이와 같은 SNS의 다양한 기능으로는 사진과 신상정보 등의 '프로필'기능과 친구와 지인, 팬 등과의 사회적 관계를 맺는 '관계 맺기' 기능, 이메일, 쪽지, 채팅, 메신저와 같은 '커뮤니케이션' 기능, 사진, 블로그, 동영상 등의 '콘텐츠 생산' 기능, 다른 사용자의 콘텐츠 공유나 배포와 같은 '네트워크의 활용'기능, 인증정보의 제3자 제공 없이도 가능한 '인증 서비스' 기능 등이 있다[2].

국내 SNS의 종류로는 '네이버 밴드'와 '카카오 스토리', '빙글' 등이 있으며, 해외는 '페이스북', '인스타그램', '트위터', '구글플러스', '유튜브', '핀터레스트', '링크트인', '넥소피아(캐나다)', '비보', 'Hi5', '마이페이스', 'dol3day(독일)', 'Tagged', 'XING', 'skyrock', '오르컷(orkut)', '시나웨이보', 'Friendster', 'Multiply', 'Xiaonei' 등이 있다. 이밖에 'Line', 'WHATSA', 'WIBER', 'IMO', 'TELEGRAM', 'WECHAT', 'HANGOUTS', 'ZALO'와 같은 SNS 기반의 메신저 앱들도 있다.

이에 대해 국내 SNS의 성향을 그림1을 통해 알아보면, 남성은 '페이스북'을, 여성은 '카카오스토리'를 선호하는 것으로 나타났으며, 페이스북, 카카오스토리, 트위터, 네이버밴드, 인스타그램 순의 선호도를 알 수 있다[1].



(그림 1) 2016-2017 성별 SNS사 이용률추이[1]



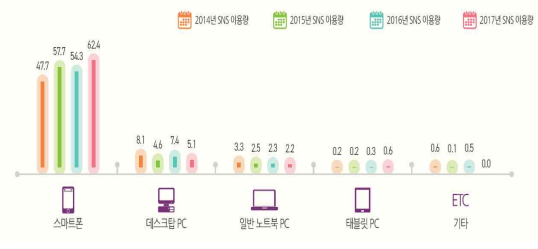
(그림 2) 2016-2017 SNS 이용률 추이[1]

그리고 그림2를 통해 '국내 SNS의 성별 및 연령대별 이용현황'을 살펴보면, 2016년부터 2017년까지 남

성보다는 여성의 이용률이 비교적 높았고, 연령대별로는 20대가 가장 높았으며, 30대, 40대, 10대, 50대, 60대, 10세미만, 70대 순으로 나타났다. 또한 그림3을 통해 '연령별 하루 평균 이용량'을 확인해보면, 다른 연령대에 비해 10대와 20대에서 가장 높은 이용률을 보였으며, 사용시간은 2016년도에 비해 2017년도에는 5.3분의 평균 이용시간이 늘어난 것을 확인할 수 있다.

(그림 3) 2016-2017 SNS 이용자의 하루 평균 이용량 추이[1]

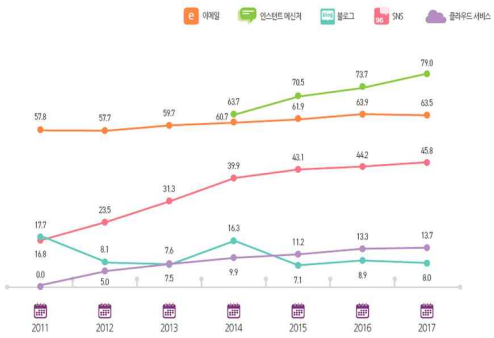
그리고 SNS에 사용된 미디어기기를 알아보기 위해 그림4의 2014년부터 2017년까지 미디어기기 선호도를 살펴보면, 스마트폰의 사용이 가장 높았으며 SNS의 이용률을 높이는데, 스마트폰의 사용이 매우 큰 영향을 미쳤음을 알 수 있다.



(그림 4) 2014-2017 미디어 기기별 SNS 이용량 추이[1]

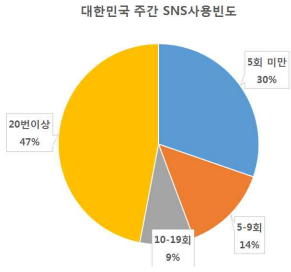
2.2 향후 SNS의 전망

최근 미디어 서비스의 사용이 지속적으로 증가하고 있는 가운데, 인스턴트 메신저나 SNS의 사용이 지속적으로 증가하고 있음을 그림5를 통해 알 수 있다[1].

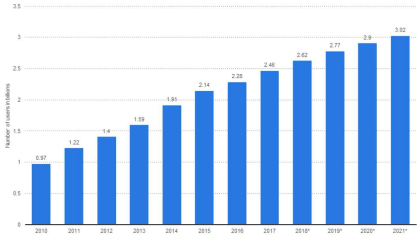


(그림 5) 2011-2017 미디어 서비스 이용률 추이[1]

그리고 그림6의 '국가별 SNS 사용빈도 통계'자료를 확인해보면, 대한민국의 주간 SNS 사용빈도는 '20번 이상'이 47%, '5회 미만'이 30%로 나타났다. 이와 같은 자료들을 종합해볼 때, SNS의 사용빈도와 하루 이용량은 지속적인 증가가 예상되며, 향후 SNS를 이용한 다양한 서비스의 개발 또한 활발해질 것으로 전망된다[3].



(그림 6) 대한민국 주간 SNS 사용빈도[3]



(그림 7) 세계 소셜 네트워크 이용자 추이 및 전망[4]

아울러 SNS의 전 세계 향후 전망에 대해 그림7의 '세계 SNS 이용자 추이 및 전망'을 알아보면, 이용자는 2010년 9억7천만 명에서 2019년 27억7천만 명을 나타냈고, 향후 2021년에는 30억 명을 넘을 것으로 추정하였다[4]. 이러한 결과를 통해, 향후 SNS의 이용량과 이용자의 지속적인 증가에 따른 공격빈도와 피해규모 또한 함께 증가할 것으로 예상된다.

2.4 SNS의 인증 서비스

SNS의 인증 서비스는 이용자에게 인증정보를 제3자에게 제공하지 않고도 가능한 서비스를 제공하며, 이를 위해서는 몇몇 프로토콜들이 사용된다. 프로토콜은 주목적이 허가(authorization)이거나 인증이 주목적인 것과 2가지가 혼합된 형태의 프로토콜이 있다. 다음은 이들 프로토콜들에 대해 알아본다.

2.4.1 OAuth

기존의 인증방식은 웹 사이트에 아이디와 비밀번호를 연동하여 인증하는 방식으로 매우 취약하기 때문에 이와 같은 인증정보의 전달대신 'Access Token'을 사용한다. OAuth는 'Open Authorization', 'Open Authentication'을 의미하며, 다양한 애플리케이션들의 인증 및 인가에 사용되는 사용자의 인증 정보가 제3자에게 제공되지 않고도 가능케 한다. OAuth는 1.0에서 2.0으로 업그레이드되면서, 디지털서명기반에서 HTTPS에 의한 인증으로 절차를 간소화되었고, 개발자의 구현이 용이해졌다. 뿐만 아니라, 리소스(resource) 서버와 허가(authorization) 서버를 분리하였으며, 몇몇 용어가 변경되었다[5].

2.4.2 OpenID

OpenID는 여러 웹 사이트 중 하나의 사이트에서 발급받은 아이디(ID)로 다른 서비스를 사용할 수 있도록 하며, 소위 '간편 로그인'의 기본 개념이 openID로부터 시작되었다. OpenID는 인증(authetication)이 주요 목적이지만 OAuth는 허가 또는 권한부여(authorization)를 목적으로 하는데 차이를 갖는다[6][7].

2.4.3 OpenID Connect

OpenID Connect는 OAuth 2.0을 확장한 형태로 인증 정보는 'ID Token'이라는 암호화된 토큰을 사용하며, JWT(JSON Web Token)로 표현된다[8].

3. 보안 취약점

SNS의 보안 취약점은 이미 잘 알려진 취약점과 근원적으로 해결되지 않은 취약점들을 포함하고 있다. 이에 SNS의 취약점들을 표1의 OWASP와 연관하여 유사 취약점들에 대해 다음과 같이 분류 및 표기해 볼 수 있다[9].

<표 1 > OWASP Top 10 - 2017[10]

A1	인젝션
A2	취약한 인증
A3	민감한 데이터 노출
A4	XML외부 개체(XXE)
A5	취약한 접근통제
A6	잘못된 보안구성
A7	크로스사이트 스크립팅(XSS)
A8	안전하지 않은 역직렬화
A9	알려진 취약점이 있는 구성요소 사용
A10	불출분한 로깅 및 모니터링

3.1 기존 사용자 인증 취약점

SNS 인증은 Authorization 서버에 접근을 시도하는 사용자를 유도하여 아이디와 패스워드를 탈취하는 공격에 취약하며, Authorization Server로부터 인증을 한 후, 사용자의 권한 코드를 전송도중 캡처해 인증을 시도하는 '재사용(Replay) 공격'과 정상적인 사용을 가장한 '위조 또는 위장(Fabrication) 공격'에 취약하다[10]. (OWASP: A2, A3, A5, A9)

3.2 CSRF와 Covert Redirect 취약점

SNS의 이미 알려진 보안 취약점으로는 CSRF(Cross-Site Request Forgery)와 Covert Redirect가 있다. 공격자는 CSRF를 통해 탈취한 사용자 계정을 공격자 계정으로 연동하여 사용이 가능하다[11]. 공격자는 Covert Redirect 공격을 위해 정상적인 사용자로 로그인 성공 후, 발급받은 Authorization code를 사용자에게 전송해야 하는데 공격자는 변조된 Redirect URI를

전송하여 변조된 URL로 로그인을 유도함으로써, Authorization code 값이 공격자 서버로 전달되도록 하여 공격자는 사용자의 계정 탈취가 가능하다[12]. (OWASP: A1, A7, A9)

3.3 OAuth 취약점

OAuth는 베어러 토큰(bearer token)인증 방식의 하나로서 암호화되지 않은 상태로 서비스 요청시마다 발급되는 토큰에 대해 'Intercept'공격에 취약하며[13], SNS의 일종인 소셜 네트워크 게임(SNG)의 경우, 계정탈취와 메모리 공격 및 위변조 공격이 가능하다[14]. 그리고 사용자는 인증코드의 요청 시 인증 토큰은 Token1.Token2형식으로 Token1만이 검증되어 'Access Token'을 수신 받게 되며, 인증코드를 두 번 이상 사용할 경우 인증토큰의 재사용 공격에 취약하다[15].(A2, A3, A5, A9)

결과적으로 SNS의 기존 취약점들은 이미 잘 알려져 있음에도 불구하고, SNS마다 사용 프로토콜이나 개발과정에서 다양한 문제가 발생할 수 있음을 알 수 있다.

4. SNS의 위협요인과 대응방안

SNS의 보안 위협요인들을 OWASP의 주요 요인들로 분류하고 SNS의 위협요인들에 대한 예방과 대응방안을 알아본다.

4.1 위협요인

4.1.1 SNS의 서비스 측면 위협요인

SNS는 사용할수록, 이용자의 업로드 된 콘텐츠 양이 커질수록, 간편 로그인 또는 인증서비스를 다양한 서비스에 사용할수록, 사용자의 SNS 탈퇴를 어렵게 하거나, 불가하도록 하는 잠재적 특징을 갖는다. 따라서 이와 같은 위협요인들의 파급효과는 매우 크며, 반복적이고, 지속적으로 발생하고 있어, 위협요인이 되고 있다.(A2, A9)

4.1.2 SNS의 기술적 측면 위협요인

SNS는 어떤 프로토콜을 사용하고, 어떤 개발환경을 제공받느냐에 따라 대응기술에 차이를 갖는다.

- SNS의 인증서비스에 사용되는 프로토콜에 따라 '가로채기' 공격에 취약한 암호화되지 않은 정보는 프라이버시의 침해를 가능케 하는 위협요인이 되고 있다[16].(A2, A9)
- SNS마다 다른 API 개발과정의 차이에 따른 보안 취약점들은 위협요인이 되고 있다.(A6, A9)
- 다양한 인증수단의 연동과정에서의 보안 취약점의 위험성은 위협요인이 되고 있다.(A2, A6)
- SNS별로 중복된 '인증 서비스'의 등록으로 인한 보안 취약점은 위협요인이 되고 있다.(A2, A5, A8)
- 서비스의 로그아웃과 관련한 취약점(로그아웃 요청에 따른 'Access Token'의 폐기는 가능하나, 리소스 서버의 로그인 상태)은 프라이버시의 침해를 가능케 하는 위협요인이 되고 있다[17].(A2, A6, A9, A10)
- 이밖에도 소셜 네트워크 서비스를 기반으로 하는 소셜 네트워크 게임(SNG) 또한 메모리 및 위·변조, 계정탈취 등의 공격에 취약하며, 애플리케이션과 플랫폼, 네트워크 기반의 위협요인들이 존재하고 있다[14].(A2, A9)

이러한 기술적 위협요인들은 대부분 개발과정에서 발생하고 있으며, 동일 공격이 지속적으로 반복되고 있어 개발환경 및 기술적 요인의 차이를 극복할 수 있는 원천적인 대응이 필요하다.

4.2 대응방안

앞서 SNS의 위협요인들은 SNS별 개발 가이드나 사용 프로토콜의 기존 취약점이나 새로운 취약점에 집중되어 있음을 알 수 있다. 따라서 이러한 위협요인들에 대한 예방 및 대응방안을 알아본다.

4.2.1 예방

SNS의 위협요인들에 대한 예방 방안들을 다음과 같이 나열해 볼 수 있다.

- SNS간의 통합된 API 개발가이드를 제공하고, 보

안테스트를 강화함으로써 예방한다.
- 개발과정에서 OAuth 프로토콜의 보안 취약점을 보완하지 못해 발생하는 문제들을 예방하기 위해 사용자에게 표시하여 즉각적이고 선택적인 조치가 가능하도록 한다.
- SNS와 같은 자격증명 공급자의 개발자에게 보안 권고사항의 준수를 하도록 하며, 'OpenID Connect' 프로토콜의 사용을 권장한다[18].
- '앱'에서의 자격증명 보다는 SNS의 자격증명 서버에서 의존적이도록 하며, 글로벌 식별자 보다는 개인 식별자의 사용을 권장한다[19].

위협요인들에 대한 대부분의 예방조치들이 개발과정에서 다뤄지고 있는 만큼, 개발가이드 및 보안 권고사항의 준수, 안전한 프로토콜의 선별적 사용 등을 통해 위협요인들의 상당부분이 예방될 수 있음을 알 수 있다.

4.2.2 대응

SNS의 위협요인들에 대한 대응 방안들을 다음과 같이 나열해 볼 수 있다.

- '가로채기' 또는 '토큰의 재사용' 등에 대해 토큰 암호화를 사용하거나 재접속 공격에 따른 토큰의 재사용을 검증할 수 있도록 구현한다.
- CSRF 보호에 사용되는 바인딩 값은 추측할 수없는 값을 포함하도록 하며, 사용자 에이전트의 인증된 상태는 클라이언트와 사용자 에이전트만 액세스할 수 있는 위치에 있도록 한다.
- 권한부여 서버는 권한부여 엔드 포인트에 대해 CSRF 보호를 구현해야하며 악의적인 사용자가 리소스 소유자의 인식과 명시적인 동의 없이 권한을 얻을 수 없도록 한다[15].

그리고 앞서 4.1절의 위협요인들의 대응방안을 표1의 OWASP를 통해 알아본다[9].

- A02: 인증과 세션관리, 애플리케이션 기능의 가이드 및 표준에 따른 구현으로 대응한다.
- A05: 인증자에 대한 제한들이 올바르게 적용될 수 있도록 한다.
- A06: 기본으로 제공되는 보안설정을 신뢰할 수 있도록 정의 및 구현하고, 소프트웨어가 최신 상태로 유지가 되도록 대응한다.
- A08: 원격코드 실행이 되지 않도록 안전한 역 직렬화의 구현을 통해 대응한다.
- A09: 알려진 취약점이 있는 컴포넌트와 라이브러리, 프레임워크, 소프트웨어 모듈에 대해 검증을 통해 대응한다.
- A10: 충분한 로깅과 모니터링으로 시스템의 공격에 대응하고, 데이터의 변조 또는 추출 공격에 대응한다.

결과적으로 공격들은 기존의 알려진 취약점을 악용한 공격과 유사 공격들이 대부분으로 프로토콜의 세밀한 분석과 기존 취약점에 대한 보완을 통해 대응할 수 있음을 알 수 있다.

5. 결 론

최근에는 스마트기기를 활용한 다양한 서비스들이 점차 사용자의 편의성과 신속성을 추구하며 개발되고 있는 가운데, SNS는 정보 및 데이터의 공유뿐만 아니라 인맥을 관리하는 대표적인 서비스가 되었다. 그리고 더 나아가 다른 서비스의 인증절차과정을 간소화하고 개인정보를 입력하지 않고도 인증할 수 있는 서비스를 제공하게 되었다. 그러나 SNS의 기존에 존재해 왔던 보안 취약점들과 잠재적인 위협요인들로 인해 이에 따른 대응기술의 마련이 필요함을 알 수 있었다.

따라서 본 논문은 SNS의 보안 위협요인들과 대응기술들에 대해 알아봄으로써, 보다 긍정적인 해결방안 마련과 향후 대응기술 개발에 기여할 수 있을 것으로 기대한다. 그러나 향후, 다양한 분야에 SNS를 활용한 대체 인증체계의 응용이 활발히 진행될 것으로 전망되고 있는 가운데, 지속적인 연구를 통해 취약점의 발굴과 이에 따른 대응 방안을 마련해 나아가야 할 것이다.

참고문헌

[1] 김윤화, "SNS(소셜 네트워크 서비스)이용추이

및 이용행태분석," 정보통신정책연구원(KISDI), 2018.6.15.
[2] 정유진, 배국진, "소셜 네트워크 서비스의 동향과 전망,"한국과학기술연구원, Emerging Issue Report, 2007
[3] https://www.statista.com/statistics/898811/south-korea-social-network-service-weekly-usage-frequency/
[4] 유선실, "해외 소셜 네트워크 서비스 동향," Vol.29, No.19-656, 정보통신정책연구원, 2017
[5] M. McGloin, "OAuth 2.0 Threat Model and Security Considerations," draft-ietf-oauth-v2-threatmodel-06, 2012.6
[6] https://d2.naver.com/helloworld/24942
[7] https://security.stackexchange.com/questions/44797/when-do-you-use-openid-vs-openid-connect
[8] https://connect2id.com/learn/openid-connect
[9] https://ko.wikipedia.org/wiki/OWASP
[10] 박형수, "보안코드를 이용한 OAuth 인증강화방안," 아주대학교 대학원 학위논문(석사), 2016.12
[11] https://meetup.toast.com/posts/105
[12] https://www.hahwul.com/2019/06/oauth-chained - bugs-to-leak-oauth-token.html
[13] 이병천, "OAuth 2.0 MAC 토큰인증의 효율성 개선을 위한 무상태 난수화토큰인증," 한국정보보호학회, Vol.28, No.6, 2018.12
[14] 이상원, "소셜 네트워크 게임(SNG) 서비스의 개인정보 노출 및 보안위협에 대한 연구," 고려대학교, 2014.12
[15] https://habr.com/en/post/449182/
[16] 정미경, "소셜네트워크 OAuth 서비스의 취약점에 관한 연구," 성균관대학교 2012.12
[17] 김진욱 외 3명, "OAuth를 이용한 로그아웃 문제로 인한 취약점 방지기법에 대한 연구," 한국정보보호학회, Vol.27, No.1, 2017.2
[18] https://medium.com/securing/what-is-going-on -with-oauth-2-0-and-why-you-should-not-use-it-for-authentication-5f47597b2611
[19] https://threatpost.com/oauth-2-0-hack-exposes-1-billion-mobile-apps-to-account-hijacking/121889/

〔저자소개〕

전 정 훈 (Jeong-hoon Jeon)
2000년 8월 숭실대학교 일반대학원 컴퓨터학과 공학석사
2008년 2월 숭실대학교 일반대학원 컴퓨터학과 공학박사
2005년 5월~ 현 동덕여자대학교 컴퓨터학과 교수

email : nerdrandy@dongduk.ac.kr